CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

IN THIS EDITION



Data Breaches:
Beyond Exposing Identities

Why We Need to Rip-off the
Cybersecurity Band-Aids

Why Biometric Data
Use Poses Unique

How to be Workforce Ready
and Standout with
Cybersecurity Hiring Managers

Are the C-suite and Security
teams on the same page?

And much more...

MARCH 2019

MORE INSIDE!

CONTENTS

Data Breaches: Beyond Exposing Identities 22

Why We Need to Rip-off the Cybersecurity Band-Aids 25

Why Biometric Data Use Poses Unique Security Risk 28

How to be Workforce Ready and Standout with Cybersecurity Hiring Managers 32

Are the C-suite and Security teams on the same page? 35

Cross-site Scripting Is an Underrated Vulnerability 38

Cybersecurity in New York City, the Financial Capital of the United States 42

Best Practices for Balancing BYOD with Mobile Security 45

Some Important Developments in the Cyber Insurance Industry 48

Putting Security in Context 51

The Internet of Things Engineering Insights 54

Schrodinger's vulnerability 57

2019 Risks in Focus: Cyber Incidents 60

Why Insider Threats Are One of the Biggest Security Risks 64

Why threat intelligence is the key to defending against Third party risks 67

The US Must Catch Up to Other Prominent Powers in Cyberwarfare Defense 70

Five Steps to Least Privilege Success 73

Security have and have-nots 76

Better, Faster, Cheaper: Changing the Economics of Responding to Cyber Attacks in the Healthcare Sector 79

Want to Secure Your Endpoints? Go Beyond the Endpoint 81

Why Wi-Fi Hacking Will Persist Despite WPA3 86

Operation Eligible Receiver - The Birth Place of Cybersecurity: Configurations 89

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

CONTENTS (cont')

Prioritizing Security in a Multi-Cloud World 93

Overcoming Software Security Issues Caused by the Third-Party Software Procurement Model 96

Phishing in the Dark: Employee Security Gaps Are Growing.....100

Automated STIG "Hardening" Finally Comes to Government IT 103

Software Should Come with a "Nutrition" Label.....106

Shattered! Security in a Fragmented World of Workloads 109

How Organizations Should Choose a Load Balancer for Managing and Securing Application Traffic in the Cloud 112

SaaS DNS Security: Are you Protected? 116

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



@MILIEFSKY

From the

Publisher...

CyberDefenseTV.com and CyberDefenseRadio.com are up. Please check them out!

Dear Friends,

It's March 2019 and the RSA Conference 2019 is days away, March 4-9, 2019 in San Francisco, CA, USA and it will be our 7th year in attendance as a Media Partner.

As promised, we're only a month away of having will have six platforms online and operational. Some of them will be a big surprise to you and we hope you enjoy. Our goal is to be the #1 source of original InfoSec content – 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.

We promise excellent, educational and original content, every month on www.CyberDefenseMagazine.com for free. We promise great interviews on www.CyberDefenseTV.com and on www.CyberDefenseRadio.com. We also offer our own statistics that you are free to reuse anytime, from this page: http://www.cyberdefensemagazine.com/quotables/.

We are days away of announcing our 7th annual RSA Conference InfoSec Awards for 2019 – which will be listed on www.CyberDefenseAwards.com.

The race to win is long and we, after 7 years of growth, are just getting started. With honesty and integrity, we will win the race. *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
CEO, Cyber Defense Media Group
Publisher, Cyber Defense Magazine

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



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

From the Editor…

Do you think CyberWar is real? Do you believe it's happening right now and affecting you and your family? We know it's real. We see new forms of malware, online exploitation, covert data exfiltration and so much more. We'll continue to watch and report on this trend as it evolves as it appears to be the most dramatic cyber security activity of 2019 beyond cybercrime. It affects us all and it needs to be exposed for what it is – with no Cyber Geneva Convention possible, the blowback may reach into the physical realm – with human lives in jeopardy. WannaCry was a tiny example of what's coming and we need to be better prepared with the most advanced cybersecurity products, services, tools and techniques. Let's discuss this and search for them at RSA Conference 2019, together!

Please Enjoy This March Edition of CDM!

To our faithful readers,

Pierluigi Paganini

Editor-in-Chief

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

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

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

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

Copyright © 2019, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (a Steven G. Samuels LLC d/b/a)
PO BOX 8224, NASHUA, NH 03060-8224
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.

PUBLISHER

Gary S. Miliefsky, CISSP®

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

WE'RE CELEBRATING

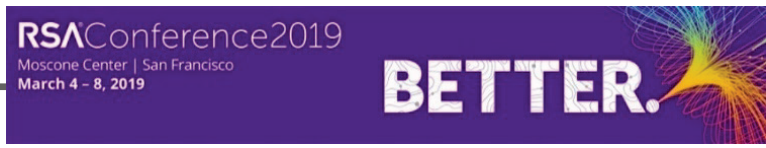
6 YEARS OF EXCELLENCE!

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 AWARDS

SEE US THIS WEEK OF MARCH 4-8 2019 AT…



Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

SPONSORS

RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

Follow your passion—all the way to RSAC 2019.

What makes you tick? Multifactor authentication? Blockchain? No matter what speaks to you, RSA Conference 2019, March 4 – 8, has what you need to stay on top of the topics affecting your organization—and the industry at large.

- Interactive demos from Splunk, Red Canary, Oracle and hundreds more exhibitors
- Hands-on tutorials, trainings and on-point conversations you won't find anywhere else
- Sharp and relevant keynotes from expert speakers such as **Emily Heath**, VP & CISO, United Airlines; **Stuart McClure**, Chairman & Chief Executive Officer, Cylance Inc.; **Bruce Schneier**, Chief Technology Officer, IBM Resilient, IBM Security | Fellow, Harvard Kennedy School; and our closing speaker, actress, writer and producer, **Tina Fey**.
- Over 550 sessions and seminars that address the issues that matter to you

It doesn't get more up your alley than that. Register today to secure your spot at the Conference that's into everything you are. But hurry—Passes and savings will go fast.

Register now: **www.rsaconference.com/cyberdefense-us19**

Follow us: **#RSAC**

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

InfoSec Knowledge is Power
Free Cybersecurity Resources



www.cyberdefense.tv
www.cyberdefensemagazine.com

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.**

Visit us at www.Vaporstream.com/security.

Vaporstream

RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

Follow your passion— all the way to RSAC 2019.

No matter what cybersecurity topics keep you on the edge of your seat, RSA Conference 2019, March 4 – 8, has the information you need to stay on top of the trends affecting your organization, including:

- Thought-provoking keynotes led by top experts, including:

  Emily Heath, Vice President and Chief Information Security Officer, United Airlines
  Ann Johnson, Corporate Vice President, Cybersecurity Solutions Group, Microsoft
  Dave Shackleford, Senior Instructor, SANS Institute
- Interactive demos from Arcon, Cyxtera, Xabyss and hundreds more
- Over 550 sessions and seminars that engage the issues that matter to you, including risk management, cloud protection and authenticated encryption

Register today to secure your spot at the Conference that's into everything you are. But hurry—savings are going fast.

Register now: **www.rsaconference.com/cyberdefense-us19**

Follow us: #RSAC

New Year, New You,
New File Transfer Solution



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**?

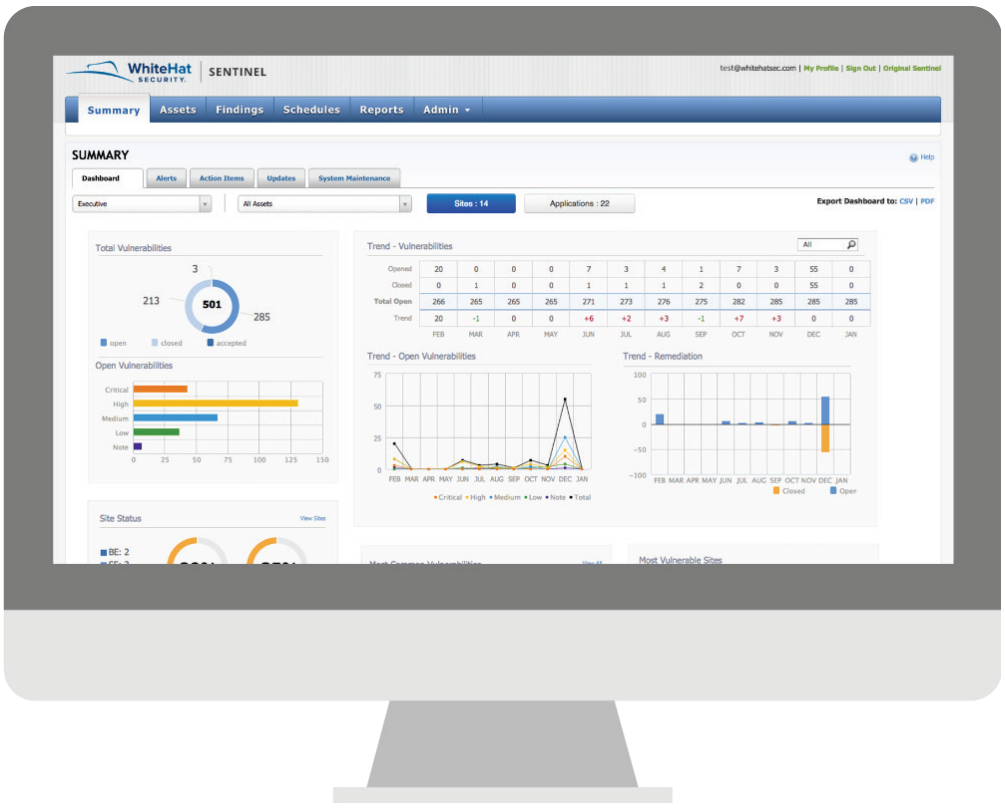
Look no further...

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.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Your peers use managed file transfer to solve key business initiatives - but how?

IT professionals discover innovative uses for their secure file transfer solution every day. From tracking weather patterns in Alaska to eliminating third-shift staffing, MFT makes solving their organizational needs easy.

In The GoAnywhere Book of Secure File Transfer Project Examples, you'll discover 20+ ways your peers use managed file transfer to meet ambitious goals and requirements in their company, including:

- A distribution company that uses MFT to send barcode scans to a file repository.
- A healthcare organization that uses MFT to move faxes into an API for processing.
- A manufacturing business that uses MFT to check a server for firmware updates.



Find the inspiration and know-how for your next file transfer project.

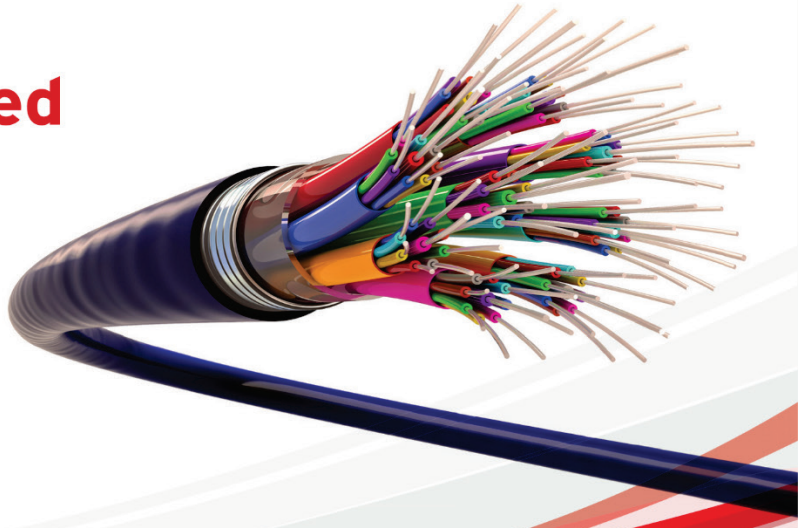
GO ANYWHERE®
Managed File Transfer

Visit ***info.goanywhere.com/use-cases-for-mft*** to get the free guide sent right to your inbox.

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

©2018 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

Hacking Experts

Providing security solutions, training and professional services to enhance cyber security knowledge. We make cyberspace safer for businesses.

TRAINING SERVICES

HACKER HOUSE™

AS SEEN IN

Forbes Bloomberg FOX NEWS CNN

WIRED SKY NEWS The Register MOTHERBOARD

CYBER SECURITY EXPERTS LEADING DEFENCES AGAINST THE DARK ARTS

PENETRATION TESTING SERVICES
view >

RED TEAM AND ADVERSARY SIMULATIONS
view >

INFRASTRUCTURE SECURITY
view >

WEB APPLICATION SECURITY
view >

HARDWARE SECURITY
view >

WIRELESS SECURITY
view >

MALWARE ANALYSIS

MOBILE SECURITY TESTING

BLOCKCHAIN SECURITY


ARTICLES



Data Breaches: Beyond Exposing Identities

Exploring the implications of adversaries or competitors using compromised networks to gain a business advantage under the guise of a data breach

By Kem Gay, Intelligence Analyst, 4iQ

Exposed data breaches are costly and taxing for companies and customers alike. More importantly, breaches are likely to lead to economic espionage as exposed networks may reveal a company's trade secrets, pending mergers and acquisitions, and other proprietary information (PI), threatening a business's overall competitive advantage. This trend isn't unique, and it has become an increasingly common occurrence.

"Studies have calculated that the U.S. loses about 200,000 jobs a year, and Europe loses as many as 150,000 due to cyber theft, including digital theft, piracy, and espionage."

- The Dawn of the Code War, John P. Carlin with Garrett M. Graff

In the past two years, the U.S. Department of Justice has indicted several individuals for cybercrimes related to espionage and stolen personally identifiable information (PII). In December 2018, two Chinese nationals were indicted for conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft. The pair, members of a known advanced persistent threat (APT) group colluding with China's intelligence services, stole sensitive technology-related business information from companies and government agencies across 12 different countries. In addition, more than 40 computers were compromised in order to steal PII belonging to over 100,000 U.S. Navy personnel.

In late 2017, three Chinese hackers were also indicted for similar offenses. In March of the same year, cyber criminals colluding with two Russian intelligence agents were indicted for unauthorized access to a U.S. email service provider resulting in computer hacking, economic espionage, and conspiracy. The perpetrators stole at least 500 million email accounts and trade secrets related to the company. Although we cannot determine, 'Which came first: the chicken or

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

the egg?' for the aforementioned computer intrusions and theft of PII and PI, we can confidently assert that both were targets for cyber criminals and nation state actors. According to a recent report from the National Counterintelligence and Security Center, "Cyberspace remains a preferred operational domain for a wide range of industrial espionage threat actors, from adversarial nation states, to commercial enterprises operating under state influence, to sponsored activities conducted by proxy hacker groups."

At 4iQ, we've continued to observe the flourishing trade of PII in underground communities and the dark web, despite efforts by companies to secure their networks with security protocols and employee cyber security training. In 2018, 4iQ curated 13,000 data breaches, while in 2017, an average of 245 breaches were discovered on a monthly basis.

Compromised networks can be difficult to detect, and some take years to mitigate. Maintaining the integrity or availability of networks is a difficult task for the Chief Information Security Officer or others with that responsibility, as risk mitigation can be difficult to manage. There is no universal remedy to avoid being compromised, but that doesn't mean you should feel powerless. Take, for instance, the infamous 2017 Equifax breach that affected some 148 million consumers worldwide. In the aftermath of the breach, a House Oversight Committee report concluded that the breach was entirely preventable given Equifax's poor and dated cybersecurity practices. This problem isn't unique to Equifax, and therein lies the problem. As a consumer, you expect companies holding your sensitive information to practice proper cyber hygiene, but that just isn't always the case.

A company-wide approach needs to be taken in order to safeguard personal data. Minute details, such as using unique passwords for all your accounts, often get overlooked, leading to detrimental outcomes. If an employee was affected by a third-party breach, and they happened to be using the same password for their work email as they were using for their outside account which was compromised, *your* company could indirectly be impacted. It's cliché, but your organization is truly only as strong as its weakest link. Sitting through mandatory cybersecurity training might be a pain, but it serves a purpose. Additionally, keeping security software up to date and using a breach watch service can help mitigate your organization's vulnerability, in turn reducing the vulnerability of all its stakeholders. Data breaches are an all too common occurrence for businesses in today's global cyber-culture. Why risk adversaries and competitors using compromised networks to gain a business advantage under the guise of a breach?

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

About the Author



Kem Gay is an Intelligence Analyst for 4iQ, a cyber intelligence company that operationalizes the intelligence cycle from open source collection and data fusion to secure collaboration on complex ongoing investigations. Kem brings deep knowledge and expertise as a cyber intelligence analyst, working on investigations and training Intel units on tools and best practices that effectively and efficiently expedite missions. Kem was previously an intelligence analyst for the Federal Bureau of Investigation with over 12 years of dedicated service. She has worked both in strategic and operational capacities supporting various mission priorities to include, cyber, criminal, and counterterrorism. Kem has conducted briefings to diverse audiences who used her assessments to inform cyber operations and policy. She has also worked to identify emerging threats supporting cyber security related matters.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Why We Need to Rip-off the Cybersecurity Band-Aids

By Anne Baker, Vice President of Marketing, Adaptiva

Last year at the Berkshire Hathaway annual shareholders meeting, the Oracle of Omaha, Warren Buffet, proclaimed, "I don't know that much about cyber, but I do think that's the number one problem with mankind." He ranked cyberattacks above the threat of nuclear and biological warfare. The admission endures at a time when cyberattacks continue to spike. Cyberattacks are projected to cost companies $6 trillion annually by 2021, and the market to defend systems, software, and applications is expected to reach $1 trillion within the next three years.

Plenty of vendors have risen up to take advantage. Estimates on the number of companies offering cybersecurity solutions range from 1,500 to well over 2,000. This makes the sea of options very difficult to wade through and differentiate at a time when cyber challenges grow increasingly complex. It also results in companies cobbling together a huge number of products and services that don't necessarily integrate in a desperate bid to protect their networks.

Studies have shown that companies frequently utilize in excess of 70 different security vendors. Not only does this create massively complex IT environments, but it is expensive and very difficult to manage. This leads to problems like the Ponemon Institute found in its 2017 Cost of Data Breach Study in which companies reported that it took an average of 191 days for them to identify a data breach and another 66 days to contain a breach. These delays underscore how IT departments not only struggle to find problems but also have difficulty containing and fixing them once they are detected. Let's reflect for just a minute on all the damage that could occur during those months while an attack goes unrecognized. The costs to companies could easily exceed millions of dollars.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Rip Off the Band-Aid

This leaves us with thousands of vendors selling security solutions and companies spending record amounts on cybersecurity initiatives yet still grappling with identification and remediation of threats and attacks. This would be easier to wave off if attacks were slowing down, but they are not. This year, 46% of U.S. organizations have already experienced a data breach, which is nearly double (24%) what it was in 2017. Attacks continue to accelerate at an unprecedented rate. In fact, Cybersecurity Ventures predicts that by the end of 2019, a ransomware attack will occur every 14 seconds, which is staggering when you consider that in 2016, the average was every two minutes (still pretty bad).

I could throw scary stats out all day long to demonstrate the gravity of the situation, but one fact is clear: What we are currently doing is not working—despite all of the money and technology being thrown at cyberattack problems. Instead of slapping on a Band-Aid, we need to change the entire way we think about cybersecurity. The fact of the matter is that threats are changing so fast in form and function that companies can't keep up today. Not only are the nature of attacks persistently evolving faster than enterprises can adjust, but the sheer volume of attacks leaves companies panicked and underprepared.

Developing Your Cyber Defense Force

The ever-changing security threat landscape has become the number one concern for endpoint security buyers according to Gartner. In this year's Third Annual Study on the Cyber Resilient Organization, 77% of IT professionals reported that their companies do not have a formal cybersecurity response plan. This must change.

Organizations have to accept that attacks will happen, that despite all of their great defenses, issues are bound to slip through. The expectation that something will infiltrate the network, infrastructure, or an employee device must become the norm, and they need to train for what happens when it does. Think of your SecOps team as your very own special forces of sorts, constantly vigilant, set to defend, and ready to respond creatively and rapidly in the event of an attack.

To make identification and remediation of security vulnerabilities and issues as simple as possible, there are three key areas that must be priorities for your defense forces moving forward. While I will dive into each one specifically in subsequent articles, at a high level they are:

- **Peer deep:** Get visibility of all endpoints—and do so at scale. You have to be able to see what's happening all across the network. And, here's the kicker: It needs to be in real time. If data is not current, the potential remains for a system, machine, network, or device to be compromised, and you will lose time fixing it. You also need to view and analyze historical data to identify when issues occurred and how long they impacted your organization.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

- **Act fast:** There must be a plan in place to address an issue at the moment it arises—not days, weeks, or months down the line. Quarantine systems. Shut them down. Contain, contain, contain. Be sure there is a process to take care of any vulnerabilities in real time—one that can instantly scale across all your organization's endpoints if needed without negatively impacting the network or end users.

- **Adapt easily:** Today's environment requires the flexibility to rapidly respond to security issues in seconds. The security products you choose to help you respond shouldn't require time-consuming coding and testing every time you need a new containment or remediation workflow created. They should easily and intuitively enable you to take action against new threats and unexpected attacks. With so many different security solutions at work in your environment, it is also important to identify platforms that are adaptable and that can integrate easily with the security products you already have in place.

These are strange and dangerous times, but they are not insurmountable. As Seattle Seahawks quarterback Russell Wilson likes to say: "The separation is in the preparation." By evaluating and adopting endpoint visibility and control solutions, organizations can discover new ways to mitigate and respond to cyberattacks. Once companies switch from an "if" to a "when" mindset, they can finally mount meaningful defenses that will rip off the Band-Aids and enable them to tackle future security issues head-on.

About the Author



As vice president of marketing at Adaptiva, Anne Baker brings to the company a unique combination of over 15 years of high-tech marketing experience with a technical engineering background. Anne holds a mechanical engineering degree from Cornell University and an MBA from Seattle University. Her work has earned her recognition as one of the "100 Top Women in Seattle Technology" by the Puget Sound Business Journal and one of the "Top 50 Women in Mobile Content" by Mobile Entertainment Magazine. Anne has led the launch strategies for emerging start-up companies as well as created global campaigns for leading technology companies, such as Microsoft and SAP. For more information, please visit https://adaptiva.com/, and follow the company at LinkedIn, Facebook, and Twitter.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Why Biometric Data Use Poses Unique Security Risk

By Morey Haber, CTO, BeyondTrust

We live in sensitive times. One “sensitive”, under-discussed topic that we need to directly confront and have an open conversation about is around the sensitivity of data. Yes, that’s right, what do people today consider “sensitive” data?

The definition of Personally Identifiable Information (PII) often includes your name, email addresses, usernames, passwords, birthdate, address, social security number, credit card information, medical history, etc. I would stipulate that most people can agree that these are all sensitive data sets.

But there is an entire classification of sensitive data in the world that we do not discuss and is going to be a problem in the very near future. The sensitive data we are failing to adequately address is the linkage of our physical, carbon-based human bodies to all the biometric data being stored by IoT devices and services in the cloud. If you think this sounds farfetched, ask yourself if you or any of your loved ones participated in an ancestry DNA kit or received a new notebook, mobile device, or smartwatch that stores health or login data via fingerprints or facial recognition—I am willing to bet, that either you or someone close to you has.

Compromised biometric data poses unique risks

To understand the sensitivity of biometric data and why it should be a part of your conversations, consider the potential risk. You are a person. Typically, you have one single identity. One could argue that, even if you are a spy or have a criminal alias, you still only have one identity since,

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

regardless of your aliases or the names you impersonate, you only have one set of biometric data. You cannot change your fingerprints, voice, face, eyes, EKG, or even veins in your arm.

When information technology uses biometric data for either authorization or authentication (and yes, they are different), it needs to compare the results with a stored profile of your biometric data. The storage is electronic.

While extraordinary safeguards can be placed on the storage and encryption of biometric data, at some point, it needs to be reassembled (at least in parts) to compare to assessed input. If the storage is flawed by design, has vulnerabilities, or the host system is misconfigured, we have a potential exposure of the most sensitive biometric data.

However, the biggest problem with biometric data is not the storage or authentication technology used, rather it is the static nature of biometric data itself. If a password is compromised, you can change it, putting a stop to password re-use attacks that rely on the compromised password. However, if biometric data is compromised, you cannot change it. Your eyes, face, or fingerprints are permanently linked to your identity (excluding bio-hacking which is a topic for another day). Any future hacks that solely rely on compromised biometric data can be an easy target for threat actors.

Biometrics alone should never be used to authenticate or authorize action or commit a transaction. Biometrics should be paired with a password or, better yet, a two-factor or multi-factor authentication solution for a higher degree of confidence.

Assessing how your biometric data is being used and accessed

Some vendors emphasize security for biometric data (Apple Secure Enclave), while others treat biometric data with little safe regard. If you think my latter claim is questionable, consider VTech's My Friend Cayla doll and the ramification for sales, collection of voice fingerprints, and the mischievous potential for a threat actor against you or your children.

The storage of biometric data is quickly increasing, but the implications are just beginning to be understood and well-grasped. We need to begin discussing what we will allow to be stored about our identity and what is just too risky. And, most importantly by whom.

Just consider all the new technology that may now possess your biometric data:

- **Personal Assistants:** Devices from Amazon, Google, and Apple all process voice recognition commands and can be programmed to understand individual voices. Your unique vocal patterns are stored and processed in the cloud. While threat vectors for human voice patterns are still very theoretical, be mindful that this data is being stored.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

- **DNA Kits:** If you purchased or used one of these, your DNA is now on file. And, if you give permission, your data can be used by law enforcement to help solve outstanding criminal cases. You're most private and sensitive data, your DNA, is now in the hands of a third party. You should be aware of everything they can do with it and what the ramifications are if those services are ever breached.
- **Mobile Devices and IoT:** Cellular phones, tablets, and even door cameras capture some form of biometric data and stores it on the device or in the cloud—even if it is not used for authentication or authorization. The risk here is obvious. Some door cameras, based on location, capture photos or video based on movement and may capture your picture just by your walking or driving past it. Your likeness, unknown to you, is now potentially on another end user's device, or in the cloud. And, your mobile phone or tablet now has fingerprints and facial metrics stored within it too. There are plenty of tools and documents on how to bypass these security models if you have the device in hand. You cannot trust these security models based on biometrics alone, and AI may actually make the matter worse by performing the PII linkage for a threat actors.

Opening up a dialogue about biometric data

Now is the time to begin sensitive discussions on biometric data. When you purchase a device, use a new technology, or consider how you are interacting with a new service, ask yourself, and potentially the vendor (especially, if the technology is used for work), the following:

- How are you storing biometric data?
- Where is it being stored? (Especially, what countries, since this may have other legal and compliance ramifications.)
- How is it secured? Who has access?
- Is my biometric data being purged over time?
- Do you sell my biometric data?
- Does law enforcement have access to my biometric data or logs? Even with a warrant?

Biometric data is perhaps the most sensitive information you possess. It is a part of your identity and can never be changed. It is a worthy conversation we need to have in this sensitive world. It affects everyone, does not discriminate, and as new technology emerges, stands to cause potential trouble for everyone unless we understand how our likeness is being captured, stored, processed, and ultimately utilized.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

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 Bachelor's of Science in Electrical Engineering from the State University of New York at Stony Brook.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



How to be Workforce Ready and Standout with Cybersecurity Hiring Managers

Millions of job opportunities are available worldwide for qualified cybersecurity professionals. What's one major must-have for those seeking to fill the vacancies? Academic, technical and leadership skills, together, that set you apart.

Regent University's Institute for Cybersecurity, home to one of the nation's most sophisticated commercial cyber ranges, is uniquely qualified to prepare cybersecurity students to enter the workforce as professionals who are ready to confidently and expertly take on the daunting task of preventing cybercrime, which is predicted to cause more than $6 trillion in damages within the next three years.

The Triple Threat in Cyber Skills: Theory, Hands-On Learning, Communication Skills

Regent's cybersecurity program is built on professionally focused coursework that provides the technical, academic and leadership skills needed to turn the heads of hiring managers. Cheryl Beauchamp, Regent's department chair for engineering and computer science, is one of the world-class educators who shepherded the program from its inception to its designation as a National Center of Academic Excellence in Cyber Defense Education by the National Security Agency and the Department of Homeland Security.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

"The development of professional skills is core to our cybersecurity program. Our courses not only introduce current theory and relevant issues, but they also provide opportunities for students to work on collaborative projects that give them hands-on experience that will be invaluable when they enter the workforce," she said.

The ultimate goal of Regent's cybersecurity program is to graduate well-rounded cybersecurity professionals who are equally as comfortable on the frontline of defending assets and information as they are walking into the boardroom to present jargon-free assessments of vulnerabilities and strategic plans to combat them.

While not required to earn a degree, Regent encourages cybersecurity students to earn professional certifications, such as the Certified Cyber Practitioner™, to get ahead of the game. Many organizations, especially in the government, require them.

A degree, plus those credentials, make Regent graduates the triple threats of the applicant pool in that they have mastered theory, applied it with hands-on learning on the live fire range, and gained practical communication and professional skills.

"Many of our students take advantage of our certification preparation courses to round-out their competitiveness. Graduating with certifications under their belt is another way to make them stand out as professionals," Beauchamp said.

Leveraging Competitions and Access to Experts

Participating in events such as the Mid-Atlantic Collegiate Cyber Defense Competition and the National Cyber League Competition provide Regent's students with another venue to hone their professional skills.

"These are tremendous opportunities for the students to work on communication, collaboration and team-building skills," Beauchamp said. "It also gives them the opportunity to meet students at other universities and network with industry professionals who are looking for recruits," she said.

Regent University is strategically situated in Virginia Beach, Virginia, part of the East Coast's epicenter of military presence and takes advantage of the opportunities afforded by that.

"Given our location, we can draw upon local, private, government and military cybersecurity experts to interface with our students," Beauchamp said. "Through our cybersecurity forums and conferences, we've featured some of the country's leading experts who share their knowledge and offer insights into what it's like to work for entities such as the Space and Naval Warfare Systems Command."

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Maximiliano Gigli, a third-year cybersecurity student and graduate assistant at Regent, said those opportunities have been inspiring. “They give us a personal perspective of the work and their real-world experiences show how theories are put into action,” he said.

Capstones and Clinics: The Secret Sauce beyond Course Credits

Further development of professional skills is gained through the required capstone course that encapsulates their studies including the principals and methodology of information security management, research and project management.

Additionally, Regent recently introduced monthly clinic sessions, offered online and on campus, that cover topics such as the Linux operating system, password cracking, ethical hacking and penetration testing.

“Higher education tends to focus on taking the courses and getting the credits. Our offering of these clinics, outside of the courses, reinforces what they are doing in class and provides them with more hands-on experience,” Beauchamp said.

“These are opportunities are for those who really want to gain experience and learn more. It’s like a bridge. The skills help them with their self-identity, and their career-identity, so they graduate as highly qualified professionals.”

Regent University’s Institute for Cybersecurity is disrupting and transforming the cyber defense industry with a state-of-the-art training platform and world-class trainers. To learn more about how you can stand out as a cybersecurity professional, visit regent.edu/cyber or contact the institute at 757.352.4215.



Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Are the C-suite and security teams on the same page?

By Matt Lock, Director of Sales Engineers at Varonis

With every week seemingly bringing reports of another serious data breach hitting a high-profile organisation, and the EU GDPR ushering in strict new data security laws, cyber security has finally become a major priority for most companies. However, establishing a strong security strategy can still be a difficult prospect.

One of the biggest challenges is aligning the various stakeholders in the business and bridging the gaps between their disparate priorities and perceptions. In particular, the two most important groups influencing the security of a company are the IT and security teams with direct experience in the field, and the C-suite making the overall budgetary and strategic decisions. If these two stakeholder groups are not on the same page, the company's security strategy can become fragmented and ineffective. Our own research has found that the priorities for the C-Suite and IT/security teams can differ drastically in some cases.

The biggest cybersecurity worries

To begin, we wanted to gauge what kinds of cyber threats were causing the most concern, and immediately found that the C-Suite and IT/security teams were in firm agreement that data loss and data theft/exfiltration were the biggest worries. This supports the assertion in Europol's Internet Organised Crime Threat Assessment (IOCTA) that data is the 'lifeblood' for almost all companies; it therefore follows that decisions around its protection, and management are of strategic importance.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Interestingly, the two groups differed heavily when it came to their third choice. The IT and security respondents found ransomware to be the next biggest concern, while the executives were more worried about data alteration, where an attacker changes records or the code in something like an automated assembly line.

Disagreeing on impact

While the two stakeholders generally had the same priorities for cybersecurity, we saw a major difference in opinion when it came to assessing the business impact of a security incident. 31 percent of IT and cyber respondents held brand perception as their main concern, followed closely by intellectual property loss. Costs such as fines and recovery expenses proved to be a much lower priority.

The C-suite on the other hand took the opposite stance, with costs sitting firmly as the main concern. This seems to demonstrate that IT and security practitioners are more focused on trying to protect the company's reputation and operations as a matter of course, while executives see the impact on the businesses' bottom lines as the deciding factor.

A lack of communication?

The biggest difference in opinion seemed to appear when we asked respondents about their security readiness, specially asking if they agreed with the statement "My organisation is making measurable progress when it comes to cybersecurity". IT and security teams were quite optimistic, with 91 percent agreeing with the statement. However, a markedly lower 69 percent of executives felt this way.

The dissimilar perceptions largely stem from a lack of clear communication about the company's security efforts and the impact they have. This was made especially clear when it came to the ever-pressing issue of finances. 88 percent of security and IT teams stated that they could quantify how cybersecurity measures impact the business, but only 68 percent of the C-suite group felt the same.

Taken together, this strongly suggests that executives need more information about their cybersecurity investments and how they are making a quantifiable and justified impact on the company's bottom line. If senior management are not part of the security planning process there is a problem: with more at stake in the event of a data breach, companies can no longer lay the blame solely at the door of the IT security teams if there's a security incident.

Time to speak up, security pros

Clearly, more needs to be done to get the C-suite and IT and security teams on the same page. One of the most telling findings we uncovered from our survey was that the IT and security

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

practitioners appeared to overestimate how well issues were being communicated and understood by their executives. 94 percent of respondents believed their company's leadership acted on their advice about security threats. Juxtaposing this, only 76 percent of executives said that they took input and guidance from their IT and security staff on security issues.

To address this, IT and security teams need to make more effort to speak up and ensure that their concerns are clearly understood by the C-suite. Over the years, many IT heads have focused on the potential damage represented by cyberattacks, but with the threat now more clearly understood, they should ensure they communicate the positive impact of their IT and security investments as well. Whenever possible, they should relate all cyber issues back to the company's operations as a whole.

Finally, IT and security teams should also look to secure more facetime with their leadership groups, giving them time to fully explain their concerns and the necessary investments, rather than just relying on impersonal reports and figures. If they don't already have one, the C-Suite should also be giving the IT team a seat at the executive table to ensure their voice is heard and both groups are on the same page.

About the Author



With 20 years' cyber security experience, Matt is an expert on data security and a regular speaker - and media commentator - on GDPR. An accomplished CISSP Security Consultant, he's worked with world-leading organizations across insurance, pharmaceuticals, legal, health, entertainment, retail and utilities. As Director of Sales Engineers at Varonis, he heads up the team which undertakes risk assessments and data governance projects, helping organizations to secure and manage their unstructured data. Through these assessments, Varonis has found alarming levels of excessive employee access to sensitive files within organizations: its recent report revealed that 58% of organizations have more than 100,000 folders open to every employee.

Matt can share insights, based on this first-hand experience on:

- How failing to lock down access to sensitive files exposes an organization to data breaches
- Why organizations need to take time to identify sensitive data and apply permissions so it's only accessed by the necessary people (known as a model of 'least privilege').

Based in the London office, Matt can be contacted at mlock@varonis.com and at our company website https://www.varonis.com/

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Cross-site Scripting Is an Underrated Vulnerability

Find out Why Cross-site Scripting (XSS) is an underrated vulnerability and how this article will transform your thought.

Cybersecurity attacks are an enormous challenge from the point-of-view of people, organization and nations. Also called cyberattacks, they represent a malicious attempt by an individual or organization to breach the information system of another individual or organization.

For many years, an injection vulnerability has positioned itself in OWASP's TOP 10 vulnerabilities — Cross-site scripting, also known as XSS. These type of attacks work by injecting some piece of code into a benign and trusted web application. It occur when an adversary uses a web application to send malicious code, typically in the form of a browser side script, to different end users.
The flaws that can be exploited by adversaries are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. This article aims to give a lot of things we can do with XSS — an underrated vulnerability.

The Art of XSS

The principle of XSS is always execute malicious JavaScript code in the victim's browser. There are different ways of achieving this goal, and they are often divided into three types, namely:

Persistent XSS: Malicious payload originates from the website's database.

Reflected XSS: Malicious payload originates from the victim's request.

DOM-based XSS: The vulnerability is in the client-side code rather than the server-side code.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

XSS and the Hackers' Inspiration

XSS is and underrated vulnerability. In fact, there are three good reasons for that: (i) it's a client side vulnerability, (ii) many white hats just need that popup for proof-of-concepts, and (iii), most of the black's hats don't know enough JavaScript to make much money with XSS.

XSS is a powerful attack vector to inject malicious payloads and can be used to impersonate something as well. There are a lot of things that we can do with XSS. Next, a list with possible scenarios used by adversaries in real attacks are presented.

Ad-Jacking: Adversaries can inject its own ads in a legitimate website to make money easily and based on a persistent XSS.

Click-Jacking: Hidden overlays can be created in a website to hijack victim clicks and to perform malicious actions such as redirects to login pages and exhibit false payment forms.

Session Hijacking: HTTP cookies can be accessed via JavaScript whenever the *HTTP ONLY* flag is not present in the cookies.

Content Spoofing: JavaScript is very powerful. In this way, an adversary can modify a page with desired content as the JavaScript has full access to client side code.

Credential Harvesting: Victims put their own credentials in a fancy pop-up created by adversaries with the goal of harvest their credentials.

Forced Downloads: There are several application vulnerabilities that hackers are leveraging. One of the most popular example is the Flash Player. Adversaries can force the download from a trusted website that the victim is visiting.

Crypto Mining: Adversaries can use the victim's CPU power to mine cryptocurrency without its consent and knowledge.

Bypassing CSRF protection: Adversaries can make POST requests with JavaScript. They can collect and submit a CSRF token and steal data or even execute critical operations in a third-party service.

Keylogging: Anything that victim's type in their keyboard can be harvested.

Recording Audio: - It requires authorization from the user but adversaries can access microphones. This is possible from HTML5 and JavaScript.

Taking pictures: Adversaries can take pictures from the victim's webcam (this requires authorization from the user).

Geo-location: That requires authorization from the user but adversaries can access victim's geo-location.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Stealing HTML5 web storage data: HTML5 introduced a new feature, web storage. Now a website can store data in the browser for later use and of course, JavaScript can access that storage via window.localStorage() and window.webStorage().

Browser & System Fingerprinting: JavaScript makes it a piece of cake to find browser name, version, installed plugins and their versions, operating system version, architecture, system time, language and screen resolution.

Network Scanning: - Victim's browser can be abused to scan ports and hosts with JavaScript.

Crashing Browsers - Adversaries can crash the browser with flooding them with stuff.

Stealing Information - It's possible to grab information from the webpage and send it to malicious server.

Redirecting: Adversaries can use JavaScript to redirect users to any webpage.

Tab-napping: Just a fancy version of redirection. For example, if no keyboard or mouse events have been received for more than a minute, it could mean that the user is afk and adversaries can sneakily replace the current webpage with a fake one.

Capturing Screenshots - Adversaries can take screenshots of a webpage. Blind XSS detection tools have been doing this before it was cool.

Considerations

JavaScript is a powerful language and can be used to manipulate user's behavior when they are visiting a web page. Many times, it's considered as an underrated vulnerability but the malicious horizon is giant — as observed during this article.

Living in this digital era, you always should suspect something strange.

For developers, there are three brilliant kinds of stuff that I love: (i) escaping, (ii) validating input via a whitelist, and (iii), sanitizing. The use of code-review, automatic static code analysis, and secure code must be always a mandatory procedure implanted in development teams.

Finally, next time you find an XSS vulnerability, report it. If you are not attended at the first time, then change the PoC. Try submitting an exploit to steal data or other critical stuff — surely, it will have another impact.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

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.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Cybersecurity in New York City, the Financial Capital of the United States

NYC Accelerates the Development of a Cybersecurity Cluster to Protect the Financial Capital from Cyberattacks

By Uzi Scheffer, CEO of SOSA

New York City is the financial capital of the United States (and arguably the world) and the cybersecurity space in NYC is mostly populated by firms that are creating solutions for the financial services industry.

New York's position as a financial capital makes the city especially vulnerable to cyberattacks. Although Manhattan is an established gateway for financial services and business in general, it's still developing as a cyber hub. As hackers' tools become increasingly sophisticated, it's no secret that there's room for improvement in cybersecurity in NYC.

To address this urgent need, the New York City Economic Development Corporation (NYCEDC) unveiled Cyber NYC, a huge initiative to transform NYC into a global leader in cybersecurity innovation and talent through collaborations with world-renowned partners in tech, academia and finance. The city has invested $30 million into the initiative, which will accelerate and support the establishment of cybersecurity companies in the city, directly connecting them to NYC-based corporations and developing new talent pipelines to train the cyber workforce of the future.

A key element of Cyber NYC is the launch of a state-of-the-art Global Cyber Center. The NYCEDC selected SOSA to establish the Global Cyber Center to bring together an international community of corporations, investors, startups, and talent to foster collaboration and innovation in NYC's

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

growing cybersecurity ecosystem. The Center offers structured programming aimed at efficiently connecting the

Key stakeholders in this up and coming industry with the goal of creating jobs which are part of this new economy.

In 2019, the size of the global cybersecurity market is expected to reach $167 billion. According to the NYCEDC, cybersecurity is already a $1 billion-plus industry in New York, with more than 100 companies and 6,000 employees. In addition to the overall Cyber NYC initiative and the creation of the Global Cyber Center, here's how Manhattan is going to catch up with world leaders in cybersecurity such as Israel and Singapore this year:

Ongoing regulation will continue to significantly accelerate the development of the cyber security cluster in New York. New regulations demanding New York's banks and financial services companies install specific cybersecurity technologies into their systems could represent opportunities for the space. Proximity to financial institutions creates opportunities for fintech cybersecurity companies to develop targeted solutions that address the requirements issued by the New York Department of Financial Services.

Cybersecurity jobs creation will begin in earnest this year, as Cyber NYC is expected to catalyze the growth of 10,000 good-paying cyber security jobs over the next decade as part of Mayor De Blasio's New York Works jobs creation plan.

Participation of leading financial institutions will grow as the security of the world's largest players in finance face a constantly growing threat. Banking industry leaders will become more involved in the initiative to access cutting edge technologies in this space, and that will help grow the NYC cybersecurity industry: already, Chief Operational Risk Officer Phil Venables and Chief Information Security Officer Andy Ozment from Goldman Sachs have agreed to serve on Cyber NYC's key advisory boards, lending their expertise to advise on the overall direction of the initiative. Top executives and decision-makers from many major financial institutions located in NYC are interested in exploring ways to partner with the initiative and to be part of this new, fast-growing ecosystem.

Innovation hubs will emerge as decision-makers at large financial institutions and corporations increasingly feel the need to keep their fingers on the pulse of global innovation, and they will do so by interacting with talented individuals in the cyber industry. Leaders from large organizations and agile startups will learn from each other and partner to develop new products and services – there will be an increase in event programming and meetups for this purpose in 2019.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

A boom in cybersecurity startups serving finance – the number and size of such startups will increase as the city continues to attract technology-related companies; Amazon selecting Long Island City for HQ2 is a high-profile example. Notable cybersecurity startups currently serving the fintech sector, with headquarters or additional offices in New York, include BioCatch, specialized in behavioral biometric authentication; Illusive Networks, specialized in deception technology; and ThetaRay, which is developing specialized threat analysis and protection technology.

About the Author



Uzi Scheffer, CEO of SOSA. As SOSA's Chief Executive Officer and a member of SOSA's Board of Directors, Uzi leads the day-to-day operations of the company, and is responsible for guiding the company's overall vision and strategy. He is an experienced executive, with a long track record of building operational businesses based on technology. Prior to his role at SOSA, Uzi built a global platform for online marketing of diamond jewelry, based on proprietary technology that was developed in-house. Uzi served as a pilot in the Israeli Air Force and holds a commercial pilot license. He is also a seasoned E-Commerce entrepreneur, specializing in advanced B2C marketing tools and analytics and is passionate about supporting early-stage startups. Uzi is fluent in English, French, and Hebrew.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Best Practices for Balancing BYOD with Mobile Security

Protecting Sensitive Data in a Mobile-First World

By JT Keating, Vice President of Product Strategy, Zimperium

The rapid evolution and advancement of technology has made us almost incapable of separating our devices from the way we conduct our everyday lives, personally and professionally. From the Apple Watch to wearables, tablets and smartphones, bring your own device (BYOD) is no longer something to try to plan for in the future, but something companies have to deal with right now.

The benefits provided by our devices' ability to communicate instantly, exchange files and simplify complex business operations has skyrocketed productivity rates and made collaborating with our colleagues – across offices and borders – practically instant. When computers became essential throughout every work environment, however, cyberattacks weren't far behind. Eventually, the C-Suite woke up to the reality of cybersecurity and the need to take it seriously to stay afloat in today's competitive landscape.

However, the increasing reliance worldwide on smartphones and mobile apps has occurred perhaps more rapidly than any other endpoint. In fact, Gartner predicts that demand for enterprise mobile apps will grow five times against the development capacity in 2017. Amidst this impressive growth, the security of mobile devices has been consistently put on the back burner – and hackers have taken notice.

Mobile Fraud Is Skyrocketing, While Awareness Is Not

In a recent survey, Zimperium found that fifty-one percent of respondents reported an increase in mobile threats in the last 12 months. In fact, according to the RSA Fraud & Risk Intelligence Service, more than 70 percent of fraud is now mobile. In 2018 alone, Zimperium discovered two

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

billion risks and threats among its customers, or about 50 per device. The sophisticated tactics that hackers use to conduct cyberattacks are bypassing office walls to where employees – and thus, their employers – are most vulnerable: mobile. Take phishing, for example. According to Verizon, over 90 percent of breaches started with a phishing attack and Adestra notes that over 60 percent of emails were opened on mobile devices.

The problem is that mobile devices such as smartphones are fundamentally different from other enterprise devices such as desktops and laptops in this vital respect: IT does not administer the advice – the user does. Although modern collaboration techniques often require employees to create and share unstructured company data from their mobile devices, IT does not have the proper amount of visibility into these devices to know what threats the company data may be facing. This explains why, in a recent survey, Zimperium found that 42 percent of organizations were unsure if mobile devices had been involved in past security breaches involving their organization.

Best Practices in BYOD and Mobile Security

There's no denying that personal devices in the workplace aren't going anywhere, given the unparalleled value that they bring to organizations. In fact, Forbes recently reported that enabling the mobile workforce drives 30 percent better processes and 23 percent higher productivity.

However, balancing the use of mobile with recognition of and preparation for the growing number of cyber-risks these devices face needs to become a top priority for IT teams in 2019. Data mandates such as Europe's General Data Protection Regulation (GDPR) have shown that governments and consumers are getting serious about the security of their information. It's essential to keep sensitive company information secured on mobile devices in order to maintain trust from customers and, in turn, maintain a competitive edge.

The bottom line is that organizations need to embrace a healthy mobile security policy that protects the organization and its sensitive IP while promoting productivity on mobile devices both inside and outside of the corporate network. For enterprises who are struggling to adopt mobile security best practices, here are a few key things to consider when balancing BYOD and security:

- **If mobile devices are being used to access corporate data, including from sources such as email and mobile applications, the company has a responsibility to ensure the data is protected.** This applies to corporate devices as well as BYOD devices. Perhaps the most basic and all-encompassing reason for this is that without ensuring data is protected, companies will be out of compliance with one – or multiple – regulations. The modern-day business environment means that every company is now a technology company. The average company in operation today typically processes and stores a large volume of highly sensitive employee, customer and client data that they have an obligation to protect. Regulations such as Europe's General Data Protection Regulation (GDPR) show us that today's consumers and employees are taking the mismanagement of their data more seriously than ever before – and so are their governments. In addition to avoiding millions of dollars in potential fraud and fines, the

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

proper handling of sensitive data is key to keeping consumer trust and, in turn, staying competitive.

- **It's important for all companies to recognize that today's devices contain highly personal information that is private and confidential to the owner of the BYOD device – and every precaution should be taken to not impact that privacy.** In a recent Zimperium research report, 14 percent of companies stated that employee privacy concerns were an inhibitor to adopting BYOD. It's important to keep the security of your company data in mind when adopting a BYOD policy, but it's equally imperative to protect your employees' privacy. BYOD can spike a huge increase in employee productivity, but they'll only capitalize on the opportunities that BYOD brings if they trust that their personal data is being kept private. In the same research report, 53 percent of respondents said BYOD adoption would increase if IT couldn't view or alter personal data and apps.

- **To have the greatest chance of adoption and success, any BYOD security policy must be as easy and as unobtrusive as possible.** Everyone in the security industry already knows that IT resources are more strapped than they've ever been before. To keep both your employees and your IT team happy, the best BYOD policy is a simple BYOD policy. Making an effort to ensure your policy is well-communicated and understood throughout your organization will help boost adoption rates. Find ways to show employees how they can integrate their personal devices into their professional tasks while following your BYOD policy and staying secure. Additionally, making security personal by emphasizing the ways in which following your BYOD policy benefits employees personally as well as the company can help boost adoption.

Technology's rapid evolution has revolutionized the ways in which we communicate both personally and professionally. In addition to corporate-owned devices, today's employees also expect the ability to bring, connect and fully utilize their own personal devices at work. The productivity benefits that BYOD policies bring to the enterprise are well-documented, but in today's era of elevated cyber-risk, sophisticated hackers and high-stakes regulations, it's imperative to balance BYOD with mobile security. By following these best practices, organizations can start on the right path toward creating a satisfied and secure workforce.

About the Author



JT Keating is the vice president of product strategy at Zimperium. He has brought software and mobile communications solutions to market for 25 years. Being passionate about security, he helped define and create multiple innovative approaches including application whitelisting at CoreTrace (acquired by Lumension), integrity verification at SignaCert and the first behavioral malware/phishing solutions at WholeSecurity (Symantec). JT can be reached online at https://www.linkedin.com/in/jtkeating/ and at www.zimperium.com.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Some Important Developments in the Cyber Insurance Industry

Cyber Insurance: The Ultimate Solution to Mitigate Cyber

Swati Tamhankar, Jr-Executive-Digital Marketing, Allied Analytics LLP

Technology has become a part of our lives. It is constantly transforming and improving our lives with innovations such as the internet of things (IoT), health-tech, 3d-printing, artificial intelligence (AI), robotics, and more. However, it also has its share of risks. The expansion of information technology in all spheres via social networks, mobile devices, wireless technologies, and cloud services resulted in more vulnerability. Cyber risks or threat is a growing concern for individuals, institutions, and businesses worldwide. Effective policies are required by organizations to protect themselves against threats. Therefore, several organizations are opting for IT security partners for their protection or depending on their insurers for cyber insurance products and services. Cyber insurance providers basically help companies prepare for cyber threats by contributing to minimizing the said loss or damage and bringing the situation back to normal.

The market for cyber insurance is a rapidly changing and has seen strong growth in the past few years. The increase in demand for cyber insurance arises from new regulations, growing awareness of cyber risks among top-level high executives as well as the rising number of cyber-attacks across the globe. However, lack of standardized policies impedes the market growth. As per the report by Allied Market on the cyber insurance market, the industry is likely to accrue a sum of $14 billion by 2022, registering a CAGR of 28% during the forecast period, 2016-2022. Some of the players operating in the market include American International Group, Inc., The Chubb Corporation, Zurich Insurance Co. Ltd., XL Group Ltd., Berkshire Hathaway, Allianz Global Corporate & Specialty, Munich Re Group, Lloyd's, Lockton Companies, Inc., Bit Sight Technologies, Pivot Point Risk Analytics, and more.

A series of launches and acquisitions took place in the space recently. One of them is the launch of a cyber self-assessment tool by Marsh, a global professional services firm headquartered in New York. Another is the acquisition of E-Risk Services, a liability insurance program manager

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

by Nationwide, an insurance company. Kingsbridge Group, a British specialist insurance services provider, acquired insurrect company Dinghy.

Marsh Introduces Tool for Cyber Insurance

In January '19, a new cyber self-evaluation tool was launched by Marsh that includes the latest insights on cyber security high-quality practices to provide customers with a strong cybersecurity program diagnostic. It also helps smoothen the procurement procedure by serving as a single application for cyber insurance. The innovation makes use of information on organizational cybersecurity controls, technology, and people and figures out the strengths and flag areas of concern for underwriters. Thomas Reagan, US cyber practice leader at Marsh said, "In today's fast-evolving cyber risk landscape, firms want to be able to gain greater insight into their cybersecurity preparedness. Marsh's enhanced online cyber self-assessment provides clients with a comprehensive view of their cybersecurity program maturity, coupled with a streamlined, easy-to-use cyber insurance application process."

Nationwide Buys E-Risk Services

In January 2019, Nationwide completed the acquisition of E-Risk Services with the aim of enhancing its business by expanding its distribution relationships through the latter's wholesale network. E-Risk Services is a company that provides management liability coverages for various organizations such as commercial crime, cyber and technology, employment practices, and more via its Business and Management (BAM) package insurance product. According to Nationwide, the products offered by E-Risk would strengthen its excess and surplus line offerings for small and medium-sized enterprises and enhance its focus on growing both management lines and the program business space. Paul Tomasi, president at E-Risk Services, said that Nationwide has been a great supporter and partner for the growth of their company and the deal shows Nationwide's true commitment to their wholesale broker distribution partners and several current and future policyholders insured through the E-Risk program. He said that they are glad about the acquisition as it brings many great opportunities and possibilities for their company.

Dinghy Acquired by Kingsbridge Group

The acquisition of Dinghy by Kingsbridge Group is aimed at expanding their ability to reach a broader segment of the important creative markets where freelancers demand a different approach to insurance and an enhanced user experience. Dinghy's robust product and technology and Kingsbridge's excellent marketing and commercial power allow the two companies to enhance their product offering to their clients and thereby accelerate their growth opportunities. Dinghy is a company that provides public liability, equipment covers, legal expenses, and cyber liability via their mobile-first website and Kingsbridge provides insurance services contractors, freelancers, the recruitment and utility industries, and others.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

About the Author



Sharmistha Sarkar has always had a keen interest in reading and writing. Though an engineering graduate, she forayed into the field of writing due to her love for words and the urge to do something different. Allied Market Research has given her the chance to gain knowledge about different subjects as a senior content writer.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Putting Security in Context

By Tim Minahan, Executive Vice President of Business Strategy and Chief Marketing Officer at Citrix

Innovation knows no boundaries. It can happen anywhere, anytime. And it doesn't occur in a vacuum. Innovation flows when employees and contractors openly share technology, ideas and information. Smart companies recognize this. But they're also aware of the security risks such a distributed and collaborative innovation model creates. And they're upping their game to manage them. Take Saab, for example. The defense company has a long history of breaking new ground on land, sea and in the air and delivering some of the most innovative products the world has ever seen. At its core, Saab believes that true collaboration leads to better solutions. And to drive it, the company has created an intelligent digital workspace in which its 16,000 employees can share technology, ideas and thinking across more than 80 locations in a secure and reliable way to meet the needs of its customers and give its business a competitive edge.

An Age-Old Problem

"We work every day with classified information. And while we need to be open in one end, we need to be very closed in another to ensure data integrity for those we serve," said Mats Hultin, Group CIO, Saab. "That's the key for us – to balance security and agility."

In the past, when innovation teams were in a single, physical collaboration environment, such a balancing act was a little easier to strike than it is today. Today, innovation teams – from full-time

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

employees to contractors and sub-contractors – are spread around the globe. Design drawings and collaboration must also extend across a multitude of different devices -- from laptops to phones and tablets to connected things. And access business apps and sensitive company information anywhere is there is a Wi-Fi connection or a cellular signal.

This dynamic work environment promises to drive new levels of freedom, productivity and innovation. It also introduces new vulnerabilities and an expanded attack surface that requires a more intelligent and contextual security model that centers on the user rather than the device.

Savvy IT and security teams will combine centralized policy control, user behavior insights, and machine learning and artificial intelligence to administer security policies based on user behaviors and access patterns. When an anomaly or risky behavior is detected, the system will contextually apply appropriate security measures ranging from requiring a second-layer of authentication when logging in from a new device and turning off certain features such as the ability to download or print when accessing from a foreign network to blocking access to select (or all) apps after multiple failed log-in attempts or access from a dangerous location.

A New Solution

This is where things like digital workspace technologies, come into play because they allow companies to provide access to all the applications their employees need and prefer to use in one, unified experience while giving IT a single control plane they can use to onboard and manage application performance without getting in the way of the user experience.

A true digital workspace requires three attributes:

- First, it's unified, giving users single-sign-on access to all the apps and content they need to be productive in one unified experience.
- Second, it's secure, applying contextual security policies to ensure apps and content remain safe
- And third, it's intelligent, using machine learning, micro-apps and bots to surface key insights and guide and automate work.

In creating digital workspaces, companies can serve up personalized access to the systems, information and tools their employees need, when and how they need them while keeping their information and systems secure. And they can do it in a way that provides:

- Standardization and simplification through a single, centralized workspace that unites users and keeps business in sync.
- Deployment efficiencies and cost control, as IT can more easily and cost-effectively stand up and provision servers, workgroups and new projects.
- Greater resilience and security enabled by a flexible, digital perimeter that ensures every user is intrinsically secure.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

It's been said that good things come to those who wait. But innovation happens fast. In embracing tools that enable them to unify their teams and power a more collaborative and intelligent way to work, companies can not only keep pace, but speed ahead and lap the competition.

About the Author



Tim Minahan is the Executive Vice President of Business Strategy and Chief Marketing Officer at Citrix, a leading provider of digital workspace solutions. He has a proactive role in helping to drive focused strategic initiatives and the company's overall business strategy. In addition, he leads global marketing strategy and operations for the company's vision of securely delivering the world's most important apps and data to enable people and businesses to work better. A technology industry veteran who specializes in defining new markets and positioning companies to own them, Minahan has served in a broad range of business leadership roles at leading enterprise software, cloud, and services firms. He most recently spearheaded SAP's successful transition to the cloud as CMO of the company's Cloud and Line of Business unit. Minahan joined SAP when the company acquired Ariba, where he was SVP of Business Network Strategy and global CMO.Minahan is also on the board of Made in a Free World, a non-profit technology company that is using the power of networks and big data to detect and mitigate forced labor from global supply chains. He holds a bachelor's degree from Boston College and completed the CMO Program at Northwestern University, Kellogg School of Management.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



The Internet of Things Engineering Insights

By Milica D. Djekic

The new millennium would bring a lot of challenges with itself. The main concern of nowadays would be some security matters that should provide us an opportunity to proceed with our progress and prosperity. It would appear that today's world would develop at the quite fast pace, but the security concerns would always seek from us to re-think our decisions and make a deep insight before we make a decision to take any step further. The technology is good as long as it's in the hands of reasonable and responsible people and once it gets into hands of bad guys – it can become our nightmare. The period of time that we live at this stage is quite well-known as the 4th industrial revolution.

That era has brought to us so many technological advancements that could impress anyone believing the technology is some kind of unbelievable. The fact is the engineering systems would rely on the strict laws of mathematics and physics and if we see our nature as something being the miracle – we would perhaps experience the emerging technologies as something being so sophisticated as well. One of the most known advancements of the industry 4.0 is the Internet of Things (IoT) being something so new and so old at the same glance. So many experts would agree that the IoT from its engineering perspective is nothing else, but the digital transformation of technology we already know from before.

So, what is the trick with the IoT? The IoT is the application of the existing technological solutions and the only new thing is that those improvements got the internet connectivity with themselves. This would sound so simple. Basically, it is once it got resolved, but there is a long walk through the discovery and development of such a solution. From a today's point of view, it may appear that the IoT is so easy, but the fact is that if you rule over some new technology, it could seem there got no complications at all. The point is the way to obtain so was not that simple, in any fashion.

The IoT engineering would demonstrate that those systems would mainly rely on digital, mechatronics and embedded solutions and those advancements would deal with some sort of the web access. From a technological perspective, it's the challenge to make such a solution and there would be a lot of attempts and failures that would get taken in order to meet so high requirements. Any engineering project would start with so smart market's research and the members of the engineering team would conduct so careful expert's investigation that would suggest them the main directions they need to follow in order to design the new product. More than two decades back, we would talk about the Internet of People (IoP) and everyone would see

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

the web as so convenient place to offer a chance to the folks to communicate with each other. From the current point of view, it's so obvious if we could use the internet to make the people talk to each other, we could also apply such a technology to make our devices being connected with each other using that signal. This could appear as quite simple, right? The fact is you should come to such an idea in the past and make such a dramatic change as the 4th industrial revolution is. So many engineering teams would work hard on their projects and just like the security professionals – they would cope with some procedures and put a lot of effort on in order to document every single step of their task. In the area of science and technology, it's not important to get the good idea only – you need to lead your project from its beginning to its end and consequently offer some results on.

So, we would get the secret formula how to develop and deploy the IoT solutions, but any project of that kind would seek a lot of hard work and ingenious thinking as well. In our opinion, the good preparation and strategic planning could get the appropriate basis in the entire project's approach and conduction. Using the internet signal to make devices communicate with each other is not the easy task. In such a case, you need to think so hard how to configure your hardware and software and above all; how to produce the next generation solutions. If anyone believes, the IoT engineering is about connecting the hardware and waiting for so to begin to exchange the information on, he is fully mistaken.

Any good hardware needs the program that would bring some activity to its operation. In other words, the role of the developers in the IoT projects is from a crucial importance. The programmers are not necessarily familiar with the engineering, because they would deal with so abstract mathematical thinking. In addition, if you want your developer codes something being useful – you need the strong engineering team that would get capable to transfer its knowledge and ideas to that guy who would lately understand the entire concept and make something that would work in the practice.

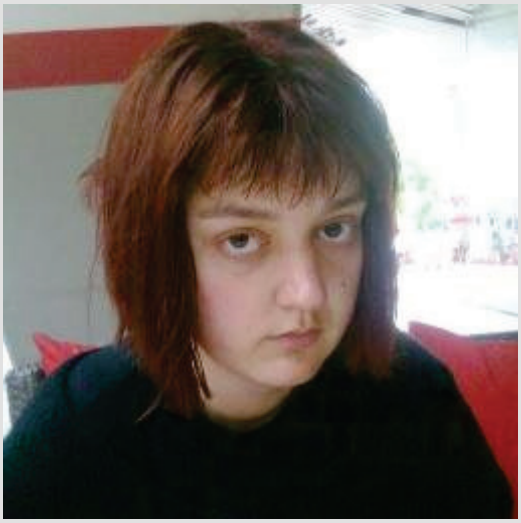
Any IoT projects would bring a plenty of engineering challenges with itself and there would be needed the hours and hours of brainstorming and project meetings that would provide the chance to the entire team to catch up with all the ideas, comments and demands on. The developers are commonly the great mathematicians who would think in programming languages as so many people worldwide speak the foreign languages.

The next open question to the IoT engineering solutions is their security. This is not the challenge to the defense community, because its members would usually be the end users of those solutions. Basically, the IoT security is the big concern to the research and development teams for a reason those guys would get required to make something that would work well and find its place in some practical applications.

Finally, it's significant to mention that maybe some innovation in the field of cyber defense could bring us the new wave in terms of technological revolutions. For instance, if we make a revolutionary new approach to the encryption – we could make the new big boom in the arena of science and technology. As many experts would suggest the only certain stuff in the future is the change, so let it gets like so!

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

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 Bright TALK expert's channel and Cyber Security Summit Europe being held in 2016 as well as Cyber Central 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. Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Schrodinger's vulnerability

Using exploitability to avoid chasing phantom risk

By Alex Haynes, Head of Information Security, CDL

I recently laid eyes on a pentesting report which had the gravest of warnings. '*The host may be vulnerable to remote code execution*'. Dear lord, did they get system access on a host? Nope. Was there a public exploit available for that version of software that enabled remote code execution? No again. Well why would someone make such a vague alarmist recommendation? When I queried this, their logic was that even though there was no public exploit available for that version of software, someone somewhere might have developed one but was keeping it secret. Also, since it's a secret exploit that no one knows about, it could also be remote code execution because that's the most common exploit right?

This is a tongue in cheek analysis of what has reached critical mass in the pentesting industry and is now dubbed '*Pentester syndrome*', the act of making things worse than they appear. You are now delivered reports full of junk risk without any kind of proof of concept with far-fetched contrived scenarios that will never occur (and have never befallen any company at all). Among other things this has led to the rise of crowdsourced security, with many of the world's biggest brands ditching pentesting entirely – as it only delivers actionable vulnerabilities with proof of concept due to the nature of their reward models (researchers are only paid if they can exploit a working vulnerability and deliver a proof of concept).

But back to the original issue. Is out of date software automatically vulnerable? Hardly. Many software version upgrades stem from functionality changes, not security updates. Even those that are for security reasons are for patching specific flaws in the code, or a readily available public exploit. When you trawl through an exploit database, the exploits often refer to very specific vectors that can only be delivered if the configuration of the asset in question is of a particular

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

kind. Many of them require some kind of privileged access already and as I alluded to earlier, remote code execution is exceedingly rare.

This brings us to Schrodinger's vulnerability, a play on the oft used trope of Schrodinger's cat, which to paraphrase implies that until you look in the box, the cat is both alive and dead. A more contemporary reference would be the response that former Secretary of Defense Donald Rumsfeld once blurted out in reference to 'known knowns', 'known unknowns' and 'unknown unknowns' with the latter being the riskiest.

Let's map this to an information asset today and call-back the alarmist reference I started this article with on. This information asset that is out of date but *might* have a vulnerability even there are none publicly available is going into the region of 'unknown unknowns'. We know there are no publicly available vulnerabilities but there may be a vulnerability that exists that we just don't know about. So how probable is this. Fortunately there's no need to speculate since there's plenty of research to draw conclusions from. '*Zero days, Thousands of Nights: The Life and Times of Zero-Day vulnerabilities and their Exploits*' is a piece of research by Lillian Ablon and Andy Bogart that focuses on this very issue. They found that if a zero-day existed and was hoarded by an entity but kept from public view, it would stay that way for an average of 7 years.

What this means for us is that regardless of what version of software you are on, there may be a zero-day that exist (however improbable) but no one will know about it and it will stay that way for an average of 7 years. What's worse is that if you update your software to the latest version, then that version too may also contain this zero-day, even though you are 'fully patched', simply because the code refactoring in the new version has not taken into the account the zero-day by virtue of the fact that it's still an unknown. The research does make a distinction for end of life software, since this will never be patched again, so if a new zero-day is discovered then it effectively becomes 'immortal' since the vendor will never release a new patch to cover this.

Using exploitability for defense

Combining a few approaches can stave off junk risk and avoid you chasing contrived scenarios that will never materialize:

- Switch from pentesting to crowdsourced security for external assets: Pentesting methodology is starting to be considered a legacy approach to offensive security testing. It does not emulate a hacker in any way – it only gives you a frozen snapshot of security posture at a specific point in time, nothing more. Crucially, crowdsourced also gives you actionable threats with proof of concept and their methodology maps more realistically to how attackers behave (for example, no time limit on testing), while pentesting focuses on theoretical threats.
- Having out of date software doesn't mean you're automatically vulnerable! While this may shock some individuals, if the specific threat vector that your version of software is vulnerable to isn't exposed in its current configuration, then you are safe.
- Practically all attacks focus on known vulnerabilities so updating your software to the latest version to protect against 'zero-day' attacks is irrelevant. The new version is as likely to be vulnerable since no code has been refactored to account for the zero-day, hence its unknown status. Updating software is for known threats, not unknown ones.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

- Even if you are exposed to a vulnerability, what are the steps needed for it to materialize. The likelihood of many vulnerabilities drops to almost zero once you factor in the first two variables required: Someone has to want to hurt you and someone has the skill level to exploit that vulnerability. The former is more common than the latter, as an offensive security skillset is still so rare nowadays even in professionals who work within information security.
- Examine your threat model and know who your bad actors are. Are you protecting against nation-state attackers or script kiddies with slap? Many vulnerabilities that focused on a contrived chain of attacks or any kind of physical proximity (think Bluetooth and Wi-Fi vulnerabilities for example) will never materialize unless you are subjected to a specific targeted attack that requires the physical deployment of malicious attackers to your geographical location. Aside from nation state attackers this has never occurred so chase things that are likely to occur (remote attacks on your assets exposed to the internet) rather than those that won't (Someone taking over your Alexa with a Bluetooth vulnerability to pivot into your network).

Naturally I'm not advocating not updating your systems. It's a good practice to get into but for many operational and human reasons many systems are just left behind in the scrum. When you have limited resources a view on 'exploitability' rather than 'vulnerability' can help manage risk far better than chasing down every single vulnerability that exists on your assets. If you take into consideration your threat model, and then sift through your external assets first viewing vulnerabilities through the lens of 'exploitability' you will be able to make your infrastructure far safer than chasing Schrodinger's vulnerability.

About the Author



Alex Haynes is CISO at CDL. He has a background in offensive security and is credited for discovering vulnerabilities in products by Microsoft, Adobe, Pinterest, Amazon Web Services, IBM and many more. He is a former top 10 ranked researcher on Bugcrowd - a vulnerability disclosure platform with over 400 vulnerabilities to his name.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



2019 Risks in Focus: Cyber Incidents

Cyber Risk a core business concern according to 2019 Allianz Risk Barometer

By Emy Donavan, Global Head - Cyber, Tech and Media PI at Allianz Global Corporate & Specialty

In the wake of mega data breaches and privacy scandals, major IT outages and the introduction of tighter data protection rules in the European Union and other countries, cyber risk is now a core business concern in 2019 and beyond, according to the Allianz Risk Barometer 2019. This annual survey of global business risks from Allianz Global Corporate & Specialty (AGCS) incorporates the views of a record 2,415 experts from 86 countries, including CEOs, risk managers, brokers and insurance experts.

For the first time, cyber incidents is neck-and-neck with business interruption (BI) at the top of the Allianz Risk Barometer– with the two risks increasingly interlinked, reflecting the magnitude of the threat now posed by a growing dependence on technology and the malicious actions of nation states and criminals.

Incidents, such as cybercrime, privacy breaches, BI (including ransomware and distributed denial of service (DDoS) attacks) can trigger extensive losses. Cybercrime generates the headlines, but often it is more mundane technical failures, IT glitches or human error, which frequently cause system outages or data losses for business. The fall-out can be costly.

According to AGCS analysis of insurance industry claims, over the past five years, even the average insured loss from a cyber incident is now in excess of €2mn ($2.3mn) compared with almost €1.5mn from the average claim for a fire/explosion incident, with losses from the largest events in the hundreds of millions or higher.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Increasing concern about cyber incidents follows a watershed year. In the wake of the highly disruptive global WannaCry and NotPetya malware attacks, 2018 witnessed a stream of major IT outages, mega data breaches and privacy scandals, as well as landmark data protection rules in the EU's General Data Protection Regulation (GDPR).

Mega Data Breaches and Attacks Soar

As organizations hold more and more personal data, breaches are increasing in size and cost. Recent mega data breaches include Equifax (143 million individuals), Facebook (50 million) and Uber (57 million). Meanwhile, the data breach which impacted around 380 million customers of Marriott hotels at the end of 2018 is one of the largest on record.

The number of cyber-attacks worldwide doubled in 2017 to 160,000, although endemic underreporting means the true figure could be as high as 350,000, according to the Online Trust Alliance. At the same time, the average cost of a cyber-attack has increased 62% over the past five years, according to Ponemon Institute and Accenture. A typical data breach now costs a company $4mn, according to Ponemon, but very large breaches can cost hundreds of millions – the cost of the Marriott breach is estimated between $200mn and $600mn by AIR Worldwide.

Rising Regulation and Litigation

An important factor driving the cost of data breaches is regulation and litigation. In May 2018, the GDPR entered force, introducing greater privacy rights for consumers and greater enforcement powers for regulators, backed by the threat of large fines. Other jurisdictions have since announced plans to introduce tougher privacy laws inspired by the GDPR ranging from California to Brazil to India. Canada and Australia have also established mandatory breach notification regimes, in line with the GDPR and similar requirements in the US.

Cyber incidents are also increasingly likely to spark litigation, including securities and consumer class actions. Data breaches, IT outages and cyber security incidents can generate large third party liabilities, as data subjects, shareholders and supply chain partners seek to recoup losses from companies and in some cases their directors.

Already a feature of US data breaches, class actions have spread to Europe, giving consumers the right to claim non-financial damages, such as for distress. A number of recent data breaches, including that of British Airways, one of the first significant breaches under the GDPR, have triggered class actions in the UK while a landmark case against Morrison's has seen the retailer held vicariously liable for a breach in the UK's first successful data breach class action.

Evolving Threats

Cybercrime has become pervasive as criminals use more innovative methods to steal data, commit fraud or extort money. Worldwide, cybercrime costs an estimated $600bn a year, according to the Center for Strategic and International Studies (CSIS), up from $445bn in 2014. This compares with a 10-year average economic loss from natural catastrophes of around $208bn – three times as much.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

However, the past year has also witnessed a growing threat from nation states, which increasingly use technology to play out rivalries and conflicts, with implications for businesses. Nation states and affiliated hacker groups have targeted universities and public sector agencies, looking to steal valuable data and trade secrets, as well as the networks and industrial control systems (ICS) of critical infrastructure companies. NotPetya was attributed to Russian-backed hackers targeting Ukraine while energy companies in the Middle East have been hit with destructive malware attacks.

Iot and New Tech

Advancements in technology are also generating new cyber threats and vulnerabilities. Organizations are concerned about the effect of increasing interconnectivity and developments such as automation and artificial intelligence.

Vulnerability is also growing with the increase in connected devices, with the Internet of Things (IoT), Industry 4.0 and digitalization of supply chains, which create new attack fronts for criminals and nation states to exploit.

According to cyber security firm Kaspersky, over three quarters of the companies it surveyed expect to become a target of a cyber security attack in the ICS space. However, only 23% are compliant with minimal cybersecurity guidance or regulations of ICS. In 2016, a DDoS attack against internet company Dyn used a botnet army of corrupted IoT devices, while December 2018 saw hackers take control of 50,000 connected printers around the world to create posters supporting vlogger PewDiePie.

"Silent Cyber" Becomes More Noisy

The WannaCry and NotPetya malware attacks highlight the growing risk of BI and even physical damage from malware and other cyber incidents. They also have accelerated discussions around cyber insurance and in particular the need for affirmative cover.

The NotPetya attack is expected to generate around $3bn in losses for insurers, according to Property Claims Services. However, some 90% of this total can be attributed to so-called "silent cyber" exposure, with only 10% covered by affirmative cover. Non-affirmative cover is where cover for cyber incidents may exist in traditional property/casualty (P&C) policies, even though this was not the intention of the underwriter.

"Silent" or non-affirmative cyber exposures lead to inadequate protection for businesses with a lack of certainty and transparency for all parties involved. As part of a group-wide project, Allianz has reviewed cyber risks in its P&C policies in the commercial, corporate and specialty insurance segments and developed a new underwriting strategy to address "silent cyber" exposures.

It is clear from these findings that every company needs to adopt an IT security position which is adequate to its size, operations and risk profile and invest in technological security solutions, proper backup mechanisms and staff training. Companies need to think about all of their employees as members of the cyber security team and provide them with proper training and empowerment to transform their staff from the 'weakest link' to the 'first line of defense'.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

About the Author



Emy Donavan is currently serving as Global Head and CUO of Cyber, Tech & Media PI for Allianz Global Corporate and Specialty (AGCS). In July of 2018, she was also tasked to head Allianz SE's Cyber Center of Competence, which provides support and expertise on Cyber products for all Operating Entities of Allianz.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Why Insider Threats Are One of the Biggest Security Risks

By Yuri Martsinovsky, CEO, SoftActivity

Many people think that all of the biggest security threats come from outside sources such as hackers. However, the truth is that one of the most damaging threats to a company comes from inside the company itself. These insider threats are also becoming increasingly common now with a majority of companies having dealt with an insider attack at least once.

For these reasons, many companies are starting to put more of a focus on preventing insider threats before they can inflict any damage. But what exactly is an insider threat and what makes them so dangerous?

A Threat from Within

The term “insider threat” is generally pretty self-explanatory. But an insider threat is any person already associated with an organization who then acts in a malicious manner to damage the organization. In most cases, this entails things like fraud and theft.

Although that is the broad definition, there are different kinds of insider threats that should be specified.

Not all insider threats act against their organization on purpose. Some of them are unwilling actors who are either tricked or coerced into acting maliciously. For example, perhaps an employee in a company that handles financial information is tricked into entering customers’ information into an online form, leaking the information to a hacker who will use it for nefarious purposes.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Some cases of insider attacks are also the result of state-sponsored attacks. In these cases, a government has either compelled a current member of the organization into acting maliciously or hired someone to infiltrate the company with the intention of stealing information or otherwise harming the organization. These kinds of insider threats are often very sophisticated and coordinated, making them especially dangerous.

A famous example of this happened in 2009 when a Boeing engineer named Dongfan "Greg" Chung stole trade secrets from Boeing and gave them to the Chinese government.

When an individual becomes an insider threat of their own accord, it is often an act of greed for they feel that they may benefit from it in some way, whether this be from selling sensitive information, committing fraud, or directly stealing from the organization.

The Costs and Damages

Insider threats can be one of the costliest security breaches an organization could ever have to deal with. Not only can the damage control required after an insider attack be an expensive procedure but, depending on what the attacker was able to access, the attack itself could end up costing the organization a large amount of money.

The average total cost for a data breach in the US is $7.91 million and this amount is increasing with every year.

But money isn't the only thing that an insider threat can cost an organization. Depending on what they end up gaining access to, they could steal valuable and sensitive information such as customer data, trade secrets, employee account information, and much more.

Moreover, if they do end up accessing customer data, such an attack could end up being a PR nightmare for the organization and hurt the trust that customers place in them. And this, of course, could lead to a loss in business which itself may end up costing the company a large amount of money.

On the Defense

Since there is so much at risk regarding insider threats, it should be no surprise that many companies are now focusing a lot of their efforts on preventing them from happening. These prevention methods include both early detection as well as prediction.

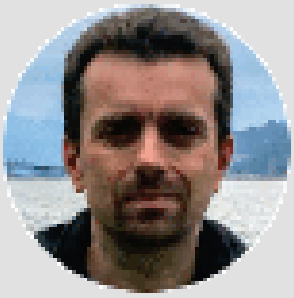
A few of the most common ways organizations attempt to prevent insider threats includes using employee monitoring software to track employee behavior, employee awareness training programs, and a more extensive screening process for new hires.

However, no prevention measure is ever going to be 100% secure. Mistakes happen and humans are always the weakest part of any organization's security, which makes insider threats all the more dangerous.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Unlike with outside security threats that largely depend on exploiting known security flaws in software, insider threats are much more unpredictable and can still happen even when an organization's security is otherwise flawless. This makes them especially difficult to defend against and contributes to them being one of the biggest security threats.

About the Author



Yuri Martsinovsky is the CEO of the SoftActivity Company. He covers insider threats, computer monitoring, and other enterprise security topics. Yuri can be reached online at Twitter @SoftActivity and at company website https://www.softactivity.com/

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Why threat intelligence is the key to defending against Third party risks

By Karen Levy, Senior Director of Product and Client Marketing at Recorded Future

As the march of digitalization continues at an increasingly rapid pace, the business world has become steadily more complex and interconnected. Organizations now routinely rely on a widening web of suppliers and partners, often trusting them with sensitive data and mission critical systems.

The advent of cloud-based services in particular has had a powerful effect on the way businesses operate, with an endless array of cloud-based service providers now available to meet practically any requirement. The adoption of IoT devices and mobile-centric working practices have likewise simultaneously created both more opportunity and more complexity.

While this new interconnected world has unlocked powerful new strategies and business models, it can also drastically increase an organization's exposure to security risks. Cybercriminals often use third-party service providers as a stepping stone to attack larger companies, exploiting their connections to evade the ultimate target's security measures.

The growing third-party risk

Marking the scale of the problem, leading analyst group Forrester reports that third parties were the cause of 21 percent of confirmed breaches in 2018, up from 17 percent the year before. This figure is only likely to increase as organizations continue their digital transformation journey and incorporate yet more third-party elements into their operations.

Some of the most notable security incidents of the last year were the result of third-party connections. The data breach reported by Ticketmaster in June for example was made possible by exploiting a flaw in JavaScript supplied by a third-party developer. Credit card details belonging to more than 40,000 customers were exposed as a result.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Organizations will also frequently inherit third-party risks through M&A activity, as seen with the data breach reported by Marriott International in November 2018. The incident is one of the largest in history, with the information of more than 500m customers being stolen. However, the breach originated with Starwood Hotels in 2014 and went unnoticed when the firm was acquired by Marriott in 2016.

Balancing risk and opportunity

While the increased reliance on digital third-party providers can quickly elevate a company's exposure to risk, firms cannot afford to shun digitalization. The flexibility and efficiency created by digital strategies are essential for retaining a competitive advantage, and is all but impossible to achieve without the use of third-party providers for cloud, IoT and mobile technology.

This means organizations must be able to balance the opportunities presented by third parties against the potential threats they may introduce. While companies are well-used to performing similar analysis for calculating ROI and assessing financial risks, evaluating cyber risks is still a relatively new and unfamiliar school of thought.

Companies need to ensure that a thorough cyber risk assessment is completed for any new partner or service provider they take on as a matter of course. More than this however, they also need to have real-time intelligence on the companies already in their ecosystem. The world of cyber threats moves so quickly that a previously secure partner could become a potential risk at any moment. Organizations need to spot potential threats against their connections before they can come to fruition and lead to an attack.

By analyzing real-time threat activity targeting third parties alongside third-party infrastructure and vulnerability data, organizations can achieve a more accurate and complete view of risk, enabling them to understand current weaknesses and evaluate potential impact against the organization.

Searching for risk indicators

To be truly accurate and reliable, threat intelligence must gather data from a number of different sources, both open and hidden.

One of the most obvious open risks is the use of vulnerable technology. Third parties that rely on web technology that is often exploited by attackers present an increased risk of compromise for their partners, particularly if they are failing to keep them patched and updated. Threat intelligence can also determine if real threat actors are actively targeting vulnerabilities present in a partner's technology.

Another clear indicator of risk is the presence of IT infrastructure misuse or abuse. The use of an IP address hosting a command and control server would present a very clear threat to the firm and any of its connections.

Domain abuse presents an additional and powerful example that a company is being actively targeted by cybercriminals and is a potential threat. The existence of lookalike "typo squat" domains registered to impersonate an organization indicate that it is being involved in a phishing campaign or targeted attack.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Alongside more openly available sources of information, threat intelligence should also account for a third party's hidden dark web footprint. By monitoring for the presence of corporate emails, credentials, and company mentions on dark web forums, it is possible to determine if a company is being actively targeted by criminal groups. The more frequently a firm is mentioned, the more likely it is to be the victim of an attack in the future. If stolen data is available on underground markets, the firm will present a greater risk of being exploited by attacks like credential stuffing, phishing and account impersonation, which will in turn present a threat to any connections.

The elevated cyber risk presented by third parties is an inherent part of today's interconnected, Digitally-driven business world. Organizations which are able to identify potential dangers in their suppliers and partners in real time will be much better equipped to mitigate any risks and confidently pursue the full benefits of their digitalization journey.

About the Author



Karen Levy, Senior Director of Product and Client Marketing at Recorded Future.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



The US Must Catch Up to Other Prominent Powers in Cyberwarfare Defense

By Bryan Becker, DAST Product Manager, White Hat Security

The terms cyberattack and cyberwar have similar meanings, but there are differences to how we should characterize and regard them. Typically, a cyberattack is a single instance attack that may or may not be part of a larger "war" between parties. Conversely, a cyberwar - or cyberwarfare - usually encompasses a strategy that drives long-term offensive *and* defensive operations and is likely waged by a nation-state backer. Cyberwarfare is an ongoing event that encompasses many aspects of information security.

When we look at the state of cybercrime in the U.S., attackers continue to demonstrate an ability to penetrate the perimeter, steal sensitive data and intellectual property, and disrupt operations of large and small corporations and private business, as well as federal, state and local government entities. Attacks are widespread, and as we've seen during recent elections, exacerbated by an unpredictable political climate.

Given how prevalent cyberattacks are in the U.S., it's exponentially more complex to consider what's necessary to defend the entire country against a full-blown cyberwar – and it quickly becomes apparent how woefully behind the rest of the developed world the U.S. remains, with regard to preparedness and ability to defend against a sustained and coordinated cyberwarfare campaign. Based on today's climate, it will easily take at least a decade for the U.S. to catch up with its allies and competitors in terms of nation-state attack protection.

It may or may not come as a surprise that North Korea is near the top of the U.S. cyber adversary list, with Russia posing the largest threat - both immediate and long term. The reason for this is that Russia and North Korea have invested in and continually grown their respective cyber operations dating back as far as the Cold War. Therefore, their experience is decades ahead of

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

the rest of the world. The biggest differences between these two countries is that North Korea tends to focus its efforts on stealing money to enrich the current regime, while the broader Russian strategy is clearly about destabilizing a country by amplifying existing divisions.

China is near the top of the list, as well. Their main goals in cyberwarfare are separate from those of Russia and North Korea – they are more interested in technology theft and obtaining personally identifying information on citizens to target for espionage efforts. On the first topic, China's "Five-year plan" (currently from 2016 – 2020) can be viewed as a shopping-list for targeted cyberattacks attempting to steal information. If you are in an industry that aligns with a goal in their plan, expect to see activity coming from China's direction.

On the topic of targeting individuals to further China's espionage efforts: How do you pick a target who is likely to commit a crime for money? You start by making a list of people who both have the access you need and *need* the money. You may not be willing to copy a few documents in exchange for a new car, but you might be willing to do it to pay for your sister's chemo therapy – this is one reason why healthcare is such a big target.

Cybercrime is international or transnational – meaning, there are no 'cyber-borders' separating countries. For this reason, international cybercrimes often challenge the effectiveness of domestic and international law and law enforcement. It's important to make a distinction between defense and offense here. The United States Cyber Command can put on a formidable offense based upon previous operations (with the assumption that its full capabilities are protected as highly classified). Despite this, U.S. *defensive* capabilities are near the worst when compared to the rest of the world.

Presently, the greatest asset for the U.S. is its cybersecurity industry, which is somewhat fitting for a capitalist nation – but, the challenge is procuring support from organizations that may not be aware that they need strong cybersecurity measures to protect against foreign powers. For example, there is a troublesome hole in the security postures for infrastructure and industrial control systems (ICS) that run our utilities. The old adage, "you're only as strong as your weakest link" can be applied here – this vulnerability presents great danger to our country. Of course, more and more companies are trying to eliminate the vacuum that exists in this landscape - but generally, it has yet to be fully addressed. To understand just how dangerous this type of attack could be, consider this: Russia has already infiltrated the control rooms of multiple power plants across the U.S. The full extent of these intrusions does not seem to be public information, but this is the same thing Russia did to Ukraine in 2015 and 2016, before Crimea was annexed and tensions escalated to armed conflict.

It's important to consider that threats in the cyber realm can easily evolve to the physical realm and therefore, U.S. cyberwarfare defenses are best left to the military, and perhaps some very specialized contractors, as opposed to relying on the technical expertise of those in the cybersecurity industry. In the InfoSec world, there is little relationship between offense and defense - that is to say, "the best defense has nothing to do with offense."

Challenges are looming in the rest of the world, too. Brexit is poised to cause a weakened national security posture for both the UK and the whole of the EU, including cybersecurity. Pushing the UK away from Europe only decreases information sharing and trust, while increasing skepticism towards "motives" when sharing or cooperating on intelligence operations.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

The fact is, the wider international community understands and manages physical conflicts, how to provide recovery efforts and humanitarian aid. But cyberwars remain somewhat unknown, even though they can sometimes be as damaging, and there is a scarcity of international laws to regulate the incidents. The digital world we have come to know is something akin to American western frontier days; the difference is that now, the outlaws are state-sponsored black hats, available to champion any malicious cause for a price. It will take a careful collaboration of resources and very many summits to elevate international cybersecurity to the necessary level of priority and urgency, so that the U.S. and each ally country can achieve more careful collaboration and protection for citizens and global interests.

About the Author



Bryan Becker is the DAST Product Manager at White Hat Security. Bryan has been working in application development and security since the startup scene in 2003. Before working at White Hat Security, he worked as a contractor in the startup hub of Asia, Shenzhen, China. There, he helped multiple startups develop internal and external facing applications, as well as developed strong security policies that are realistically achievable with strapped resources. He has also been heavily involved in the block chain startup industry in Hong Kong, where he helped small teams get proof-of-concept block chain apps up and running to present to venture capitalists.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Five Steps to Least Privilege Success

Getting Organizations Started on a Least Privilege Journey to Reduce Risk

By Joseph Carson, Chief Security Scientist,Thycotic

Organizations today typically face major challenges when seeking to implement least privilege because built-in limits on access can impact employee productivity. If users can't get access to an account, a service, or a device such as a printer, they have to spend time calling the IT helpdesk for a "fix." In many cases, busy IT helpdesk workers may give users more privileges than needed to expedite resolution of user problems. Least privilege is meant to prevent "over privileged access" by users, applications, and services to help reduce the risk of exploitation without impacting productivity.

Let's get organizations started on the right path to a successful least privilege implementation journey. These steps highlight the key stages of activity and are meant to spur further research so you can be fully prepared with the tools you need to make least privilege cybersecurity a reality.

Inventory Devices and Software

Produce a comprehensive inventory of your corporate devices, installed software, and software licenses. You also need to determine where applications typically are being installed from, as well as the software vendors that are approved to be used within your organization.

During the inventory process, create a list of trusted vendors, including signed certificate and trusted software sources for approved applications. These could include a software delivery solution, a software catalogue, a network location, or Microsoft SharePoint. You also need to list the places you don't want software being installed from that could include downloaded program files, email attachments, or any download locations on various devices.

With a complete device inventory, you can develop policies that incorporate trusted and untrusted privilege elevation requests. This process ensures employees can use a least privileged account to perform privileged actions based on approved policies.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Integrate Compliance and Regulations

Almost every organization faces some kind of compliance mandate or regulatory requirement. There have, for example, been major recent updates to regulations such as the Payment Card Industry Data Security Standard, National Institute of Standards and Technology, Cyber Essentials, EU General Data Protection Regulation, and the California Consumer Privacy Act. They all include requirements for data privacy meant to rein in over privileged access by users. Therefore, you must integrate compliance and regulations that apply to your organization into your data impact assessment, risk-based assessment, and privileged access management (PAM).

Combine PAM and Least Privilege to Control Access and Actions

A PAM solution helps with defining policies, discovering privileged accounts, applying security controls, auditing usage, and alerting abuse. Combining PAM with least privilege security allows an organization to elevate privilege On Demand, offer onetime passwords, and increase and decrease privileges based on dynamic risk and threats. PAM helps control privileges, so they're available when needed, and end-users aren't over privileged all the time.

Incorporate Application Control

Application control is technology that enables an organization to elevate application privileges so trusted and approved applications can execute even if users don't inherently have access. On the flip side, application control prevents untrusted applications from executing even if the user has the privileges that permit them to install applications. If an application is unknown, it can be "quarantined" and prevented from executing until further analysis determines whether the application is malicious or authentic.

Manage/Protect Privileges Granted to Users

Separating least privileged users from privileged accounts allows an organization much more control and security over how privileges are granted to users and determines a risk-based approach to what's an accepted risk. This step allows the organization to adopt a zero-trust security posture that's enforced by a least privilege strategy, reducing the risk from cyberattacks but maintaining empowered employees and productivity without the pain.

Applying the core principles of least privilege is a foundational element of your cybersecurity strategy. By removing local administrative privileges on endpoints, you reduce your attack surface and block the primary attack vector, preventing the vast majority of attacks from occurring.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Before you start implementing next-generation Endpoint Protection Platforms (EPP) or complex Endpoint Discovery and Remediation solutions (EDRs), you should consider a least privilege strategy with application control solution. Proactive protection based on least privilege means less time and resources spent detecting an infection, chasing down hackers once they've already entered your network, and remediating the damage.

About the Author



Joseph Carson is the Chief Security Scientist at Thycotic. Joseph is responsible for cybersecurity research in the privileged access management industry accelerating Thycotic innovation and leadership positions. He is a cyber security professional and ethical hacker with more than 25 years' experience in enterprise security specializing in block chain, endpoint security, application security & virtualization and privileged access management. Prior to joining Thycotic Joseph worked on innovative block chain solutions at Guard time and spent more than 10 years in leadership roles at both Altiris and Symantec and Arellia. He is a Certified Information Systems Security Professional (CISSP) and an active member of the cyber security community frequently speaking at cybersecurity conferences globally.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Security have and have-nots

How organizations can stay above "The Security Poverty Line"

By Javvad Malik, security advocate, Alien Vault

Way back in around the 2010 / 2011 timeframe Wendy Nether coined the phrase "The Security Poverty Line" in which she hypothesized that organizations, for one reason or another (usually lack of funds), can't afford to reach an effective level of information security.

Nearly a decade on, and while the term has suck into frequent usage within the information security community, are we any better at solving the issue now that we've identified it?

I asked Wendy on her thoughts, to which she said, "*I don't think we've even come close to understanding it yet. And I think solving it will take an effort on the level of US health care reform*."

It's a morbid thought, and can leave one with a feeling of helplessness. So, I thought I'd try to scratch beneath the surface to see what we can understand about the security poverty line.

Technical Debt

The term technical debt has become more prevalent within information security over the years. Whereby a company will accrue technical debt, or information security risk over time due to decisions they've made. For example, if a service is launched before undertaking a full penetration test or code review, it adds to the debt of fixing any subsequent issues in a live environment.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Exponential losses

One of the challenges with technical debt is that it doesn't occur in a linear manner, rather the debt, or fall below the poverty line occurs at an exponential rate.

Speaking to people who run small businesses, things become a bit clearer as to some of the challenges they face.

Cyber security needs investment in different areas, initially that is to hire expertise, or invest in technologies. Neither of which are necessarily the smallest of investments. But when there are ongoing costs, the cost to maintain security, to undertake ongoing testing. Then, when wanting to do business with larger companies, the smaller company is usually subject to a 3rd party assurance process where they need to demonstrate they meet all the cyber security requirements of the larger company, even in instances where the controls may not be directly applicable. Finally, in the event of an incident, a company that has already under-invested in security is faced with loss of business, or even legal action from partners, regulatory fines, as well as the cost of incident recovery and PR management.

How much Information security is enough?

With such a seemingly endless laundry list of things to consider in the security world, the question on the minds of most businesses is, 'how much is enough'? Unfortunately, if you're looking for a hard number, you'll be disappointed. Because the threats and challenges present in the cyber world represent a moving target.

But this doesn't mean all effort is futile, it's more a case of looking at the world differently.

One way to look at this could be through the lens of finite and infinite games, as coined by James Carse in his 1986 book of the same name.

The idea is that there are two kinds of games, finite, and infinite games. Finite games are those which have rules such as number of participants, boundaries, time duration, and so forth. After a certain period of time, a winner is declared in accordance with the agreed upon rules.

If you try to look at cyber security as a finite game, you will inevitably pull your hair out in frustration and turn into precisely how urban dictionary describes InfoSec.

Cyber Security is more of an infinite game - one where there is no set rules or boundaries or even a winner or loser as defined in the classical sense. Rather the purpose of an infinite game is to always be in a position to continue the game.

Continuing the game

Asking companies to continue the game when resources are scarce and they're living on the security poverty line. But once you understand the game, the players, the pieces, and the moves, it becomes easier to plan your strategy. For that, it's useful to consider the following points.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

1. People

Having the right people can be the difference between making it or not. It doesn't necessarily mean hiring an entire security department. Sometimes, all it needs is a consultant to help provide guidance and steer towards best security practices to ensure security is built right from the beginning.

2. Technology

IT Security technologies have come a long way in the last decade. While the constant news cycle may feel like things are getting worse, we actually see more attacks that focus on attacking humans through phishing, or compromises through third parties.

Therefore, it makes sense to invest broadly in technologies that offer a broader set of capabilities. These be more affordable, not just to buy, but to maintain on an ongoing basis.

3. Outsourcing

In today's age of the cloud and service providers, for many cases it doesn't make sense keeping everything in-house. Securing the services of a reputable MSSP can take away the need to run your own security operation center. Or having a PR agency on a retainer can help smooth over any incidents that need reporting.

4. Insurance

Finally, where risk can't be mitigated or accepted, consider transferring it to an insurance provider. Not only can insurance help alleviate the financial cost of a breach, but it can a long way in demonstrating to customers, shareholders, or partners that insurance was part of a broad cyber security plan to keep data secure.

About the Author



Javvad Malik is a security advocate at AlienVault and a London-based IT security professional. Prior to joining AlienVault, Javvad was a senior analyst with 451 Research providing technology vendors, investors and end users with strategic advisory services, including competitive research and go-to-market positioning. He can be reached on Twitter, YouTube or through his website or AlienVault's website.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Better, Faster, Cheaper: Changing the Economics of Responding to Cyber Attacks in the Healthcare Sector

By John Attala, Director, North America, Endace

The healthcare sector has been and continues to be under attack. As long as malicious criminals and hackers have the upper hand in agility, healthcare organizations, frequently under-resourced, face a never-ending struggle to defend themselves and their data.

Hardware appliances constitute the majority of security solutions required to defend healthcare companies from cyber-attacks. They are expensive to buy and maintain—and can become obsolete before being fully depreciated. The result is that NetOps and SecOps teams are habitually stuck with outdated security solutions during what is often a time-intensive upgrade or replacement process. Getting approval, raising budget, evaluating vendors, running proof-of-concept tests, deploying and configuring new solutions can often take months or years. Cyber thieves don't have the same constraints, often using their victims' own infrastructure to attack them.

For a healthcare organization to be truly agile and able to respond more quickly and more effectively to attacks, it must be able to move beyond hardware-based security solutions. A common platform that allows security analytics solutions to be deployed as virtualized applications removes dependence on specific hardware and allows agile deployment of new functionality as needs evolve.

Virtualizing security functions has the potential to deliver the same benefits that virtualization has delivered in the data center, removing the overhead of managing huge numbers of individual, hardware-based servers and making deployment inexpensive, fast, and relatively easy.
Healthcare security teams face another challenge: the challenge of dealing with a flood of security alerts that their security tools raise. The sheer number of security alerts, and the time it takes to triage, prioritize and investigate each alert is overwhelming. Research from McAfee states that 93% organizations can't adequately triage relevant threats and are unable to sufficiently investigate 23% of the alerts that are raised.

The fact is, investigations simply take too long. Traditional investigation methods involve a slow, cumbersome, and often inconclusive, process of collecting and collating evidence from multiple

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

sources (such as syslog's, Net Flow data, authentication logs, and application logs) and trying to reconstruct what happened.

Leading US healthcare organizations' security teams are turning to continuous packet capture to give them an edge in dealing with the flood of alerts and helping them accelerate the investigation and response process. Recording what happens on their network lets SecOps teams go from a security alert in their monitoring tools directly to definitive, packet-level evidence. Real-life examples include:

A hospital group in the Northeastern US is preventing malware attacks by extracting and reconstructing executable email attachments from recorded traffic and running them in a sandbox to validate whether they are malware or not. It also uses recorded network history to successfully thwart phishing attacks and identify potentially compromised credentials before attackers have an opportunity to use them to access systems. It can also identify when hospital staff have had their personal credentials compromised while on the hospital's network (e.g. banking logins compromised through phishing) and as a result can warn them to change their passwords immediately.

A large healthcare organization based in the Southern US uses recorded network history to accelerate the investigation of security alerts raised by their security monitoring software tools, such as Darktrace, and collected by their Spelunk SIEM. The security team can swiftly retrieve the packets relating to an alert to see precisely what has occurred, and immediately go into analysis mode to know how to respond and what the scope of the threat is.

Virtualizing and streamlining security functions on a common platform can enable organizations to continually evolve their defenses and keep ahead of security threats. With access to a packet-level history of network activity, analysts can examine the actual packets relating to a security alert to make sure they have the definitive evidence they need to quickly and conclusively investigate and respond to security threats and reduce the backlog of unexamined alerts.

About the Author



John Attala is the Director, North America for Endace, a world leader in high-speed network monitoring and recording technology. As the North American sales leader, John has played a pivotal role in launching and building Endace's network monitoring business within the North America. He has more than 20 years' experience in selling networking and security solutions to Fortune 1000 companies and government accounts—bringing a deep understanding of the market, delivering a consultative, solution selling approach to solve complex problems and improving network security across the globe. John can be Reached at Twitter (https://twitter.com/endace) and LinkedIn (https://www.linkedin.com/in/john-attala-8408a9a/) and at our company website (http://www.endace.com) and LinkedIn (https://www.linkedin.com/company/endace/).

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Want to Secure Your Endpoints? Go Beyond the Endpoint

By Jai Balasubramaniyan, Director of Product Management, ColorTokens Inc.

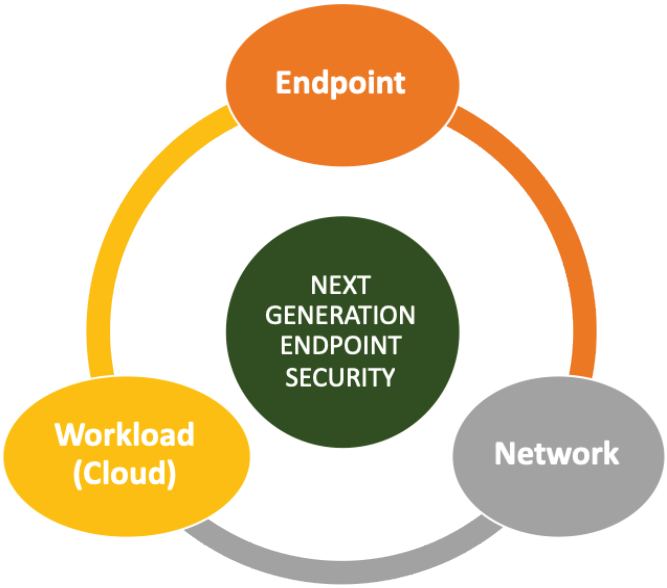
Traditional endpoint security control has always been about malware, threat analysis, and remediation. However, it is useless for an endpoint to be pristine and clear when it is unaware of the environment it is in as it will continue to get polluted even after cleanup. An endpoint protection solution myopically focused on files, sequences and malware residing on the endpoint without understanding the network it is part of, the user who sits behind the endpoint or the application they are trying to access from their endpoint, simply put, is missing the point.

The Endpoint security market is now at the cusp of a significant innovation and change. A next-generation endpoint security solution needs to be able to recognize the user behind the endpoint and what his/her behavior should be. Likewise, it would need to have a deep understanding of applications the user is trying to access, to ensure they have the right roles and access.

Traditionally some of these functions have been done by network security vendors. Unfortunately, they do not work well today's scenario. The disappearing network perimeter and workloads migrating to the cloud has made perimeter security controls, like on premise firewalls, limited in usefulness as they are simply not in the path of a lot of these communications. Similarly, the rising use of encryption will continue to make the network increasingly dark, as they cannot effectively decrypt traffic at high speeds.

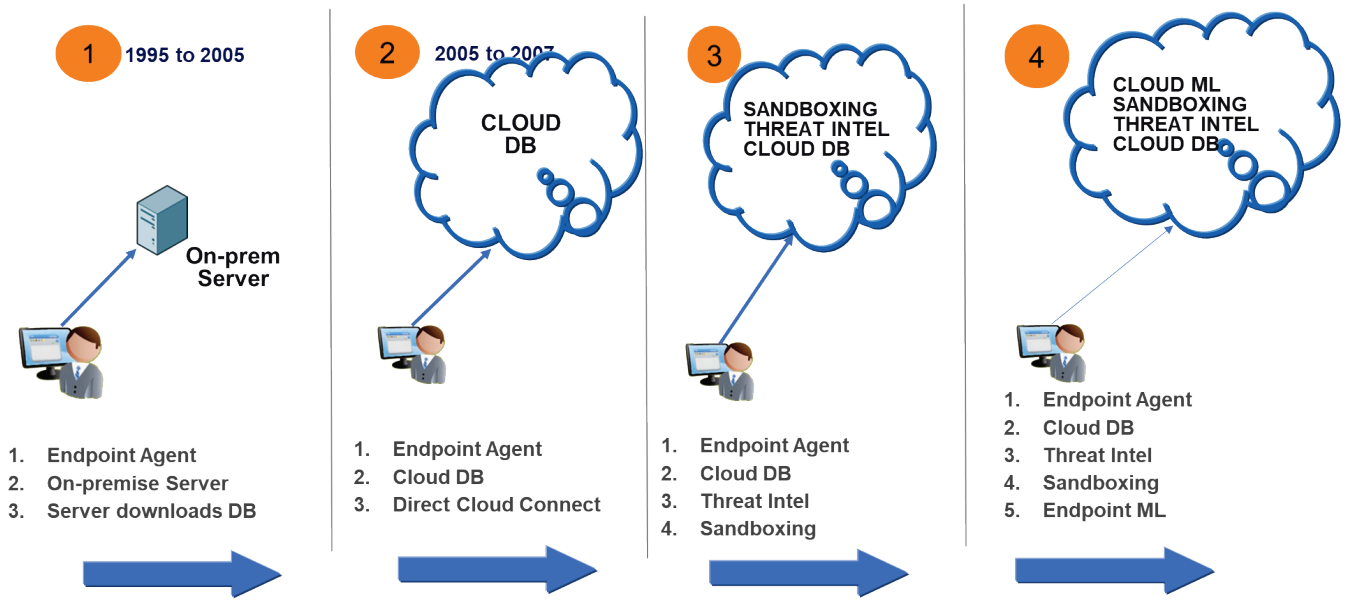
Security vendors have tried to bridge this gap between the network, endpoint, user and application by bringing in a multitude of boxes in the network layer and a multitude of agents at the endpoint with the hope that they will talk to each other and solve the problem. But this has not happened till date.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Limitations of Current Endpoint Security Approaches

Endpoint security has traditionally been about comparing an endpoint with a signature in a database. The signature database was initially downloaded from a central server to a local server in the organization. Every endpoint would then check with this database to compare file-hashes on their system with signatures to determine if a file was malicious or not. As the signatures went into billions of hashes, databases started growing bigger and bigger and started moving to the cloud where a central database served as a repository to all known good and bad file hashes.



This did not solve the problem of zero-day malware which by-definition was a malicious file that has not been seen before, and hence does not have a hash in the cloud. To solve this problem, organizations started deploying machine learning and sandboxing solutions. Sandboxing

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

solutions simply played or executed this zero-day-file that was not seen before in a safe environment where its behavior was analyzed to see if it displayed malicious behavior. Likewise, machine learning was used to look at files that have taken source code from a known exploit but changed the code a bit to create a new executable and hence a new hash. This form of attack, where you changed a known malware slightly to create a brand-new malware with a new hash value, but the source code was essentially the same, was called polymorphism.

The Birth of Endpoint Detection and Response (EDR)

The security industry changed with Operation Aurora, a series of cyber-attacks conducted against well-known technology companies by a nation state. Operation Aurora exploited a well-known vulnerability in Internet Explorer to spawn a PowerShell that could be used to execute commands on the target system. The earlier approach of checking file hashes would not have worked as Internet Explorer and PowerShell are legitimate commands; it is the sequence that is illegitimate. A browser could spawn another browser, it could spawn a music player but should not be



spawning a power-shell under normal circumstances.

The rise of nation state attackers who kept infiltrating each other's private enterprise and critical sectors such as finance and energy contributed to this trend.

Endpoint detection and response tools work by monitoring endpoint and network events and recording the information in a central database where further analysis, detection, investigation, reporting, and alerting take place. Endpoint Detection and Response solutions had four components:

1. Detection
2. Threat hunting
3. Response & Remediation
4. Managed Services

It all starts by recording everything at the endpoint – every file access, every registry call and every network connection was recorded from the endpoint and sent to the cloud. These actions were stitched together and scanned to see if there were malicious or suspicious sequences of activities, such as an internet browser spawning a PowerShell. Likewise, an attacker running port scans and scanning systems laterally using known windows utilities would evade signature defenses but be caught by an endpoint detection and response system as his behavior would trigger an alarm.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

For effective detection, most EDR solutions provide threat hunting tools to scan all the endpoint data coming from millions of endpoints to see the spread of the infection or malicious intruder activity. They allow the administrator to then remediate the infected endpoint by providing tools such as a remote shell where the administrator can login to the infected endpoint and remove the malicious files.

However, EDR solutions also have certain limitations. Customers and solutions can get overwhelmed with the amount of data that needs to be recorded and analyzed to see malicious behavior. Remediation becomes increasingly hard. The volume of data will only increase as a company keeps adding headcount with more employees who generate more data. This is the reason why EDR solutions often package managed security services along with their product as regular customers are not able to handle the complexity of managing a Security Operations Center and personnel who can analyze this data.

Whitelisting, Blacklisting and Process Controls

A doctor rarely tells you to eat everything and then runs a series of tests to tell you what is wrong and prescribes medicines to control your ailment. Rather, (s) he asks you to avoid certain types of food which could make you sick. It is no different with security. Rather than allow the user to run every possible application and every possible sequence of commands and then check in the cloud whether a sequence was malicious or not, an alternate approach would be to simply stop the user from doing certain sequences of actions or running certain applications.

Whitelisting and Blacklisting techniques are extremely effective in fixed function devices and environments with limited change to the endpoints. Here, it would be much easier to simply analyze all the running processes, create a set of process controls and then lock the device down. With this approach, rather than scan the universe for all possible bad sequences, vendors prefer to lock down systems to known good behavior. In such an approach, any new process created outside the known list of allowed processes would trigger an alert or be blocked before execution. Likewise, any process which triggers a network connection other than the well-known utilities like a browser or a file transfer utility will trigger an alert or be stopped prior to execution.

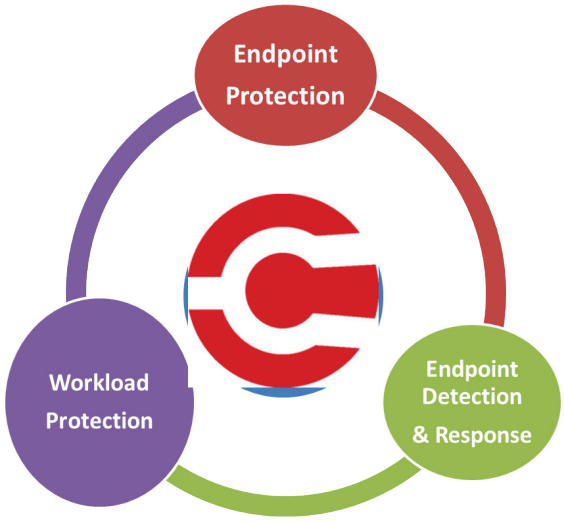
Bringing It All Together - ColorTokens Approach to Security

At ColorTokens we want to bring the power back to endpoint and make it smarter. The endpoint is the start of any communication and therefore the best place to enforce security. We start by sitting at the endpoint, understanding the user who is at the endpoint, understanding his/her access permissions, understanding what applications (s) he uses, and of course all the files (s) he downloads as payload using these applications. The rest of the endpoint security is all about the last part where we focus on analyzing the files (s) he downloads into their endpoint and examining the malicious behavior of the payload.

Color Tokens RADAR360 performs the analysis of the files using traditional Endpoint Protection Controls. We record events to ensure that some malicious sequence is not skipped. However, we

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

also add sophisticated whitelisting, blacklisting, and process controls. If a user is accessing a risky file-sharing application which ends up downloading malware into his system, we do not wait for it to happen and then try to recover like a traditional endpoint security solution. We bring in user and application context to the endpoint so it can quickly recognize this behavior as risky and stop it. We can always revert to the traditional endpoint security behavior of seeing the malware and



cleaning it up or preventing its execution, but we first and foremost try to stop bad behavior from happening.

The ColorTokens platform can be deployed across any endpoint or workload in the cloud (Amazon, Azure and other vendors) and brings the complete network and endpoint context in one simple, easy to use solution.

About the Author



Jai Balasubramaniyan is the Director of Product Management at ColorTokens Inc. He has been instrumental in creating award winning Enterprise Security Products at Cisco, Trend Micro, Check Point, Zscaler, Gigamon, Crowd Strike and ColorTokens. Jai was the architect and developer of the Cisco Router Firewall and led the creation and launch of DMVPN solution winning the Pioneer Award, Cisco's highest technology award. He has also led Product Management of Trend Micro Deep Discovery Solution which won the NSS Lab tests for highest efficacy and Gigamon Security Delivery Platform. Jai has several patents and publications in the security field. He has a Masters in Computer Science from Purdue University and an MBA from the Kellogg School of Management. Jai can be reached online at jai.bala@colortokens.com and at our company website https://colortokens.com/

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Why Wi-Fi Hacking Will Persist Despite WPA3

By Ryan Orsi, Director Product Management, WatchGuard Technologies

In 2017, the famed Key Re-installation Attack or "Krack" attack shocked the world by defeating WPA2 encryption. As a result, the Wi-Fi industry has rallied to release WPA3 with improved security protections. Unfortunately, WPA3 alone will not be enough to stop Wi-Fi attacks; not by a long shot. Before we explore why this is, let's take a step back and examine the appeal of Wi-Fi attacks in the first place.

The Wi-Fi attack surface is one of the most desirable to hackers for a variety of reasons. Just about any Wi-Fi network is highly exposed to vulnerabilities attackers can use to steal sensitive data, eavesdrop, and infiltrate further into the network. Why is it such an easy target? Nearly every cyber security company focuses on layer 7 application attacks (such as zero-day malware and ransomware), while historically very little effort has been made to defend against layer 2 Wi-Fi attacks. In fact, protections for layer 2 have only recently been introduced, leaving 20 years' worth of Wi-Fi access points, routers, and clients wide open to attack.

A primary goal for most Wi-Fi attackers is to gain position as the "man-in-the-middle (MitM)." This involves tricking a victim's device into believing it's connected to the internet through a legitimate Wi-Fi SSID, when in reality, an attacker is broadcasting the SSID and the victim's traffic is flowing directly through to the attacker, allowing them to see everything the victim is doing, typing, watching and more. This type of attack is surprisingly common, and much easier to fall victim to than you might think.

Back to the problem at hand. As I mentioned, the Krack attack roused the industry to develop WPA3, with security enhancements designed to address the shortcomings of its predecessor, WPA2. WPA3 contains a Personal and Enterprise implementation and its security improvements include the forced use of Protected Management Frames (PMF), which protect against

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

eavesdropping on unicast and multicast management frames and the replacement of WPA2's 4-way handshake and Pre-Shared Key (PSK) system with Simultaneous Authentication of Equals (SAE). This essentially eliminates offline dictionary attacks. These security enhancements will help eliminate the various tricks and tools attackers have been using for years to intercept WPA2's 4-way handshake packets, and upload to multiple free services that advertise "recovering your Wi-Fi password".

Open Wi-Fi networks supporting WPA3 also have improvements intended to prevent eavesdropping. Referred to by the Wi-Fi Alliance as "WPA3 Enhanced Open," Wi-Fi networks that don't require passwords will utilize Opportunistic Wireless Encryption (OWE), where each device will receive its own key. This will prevent others on the same open network from sniffing packets out of the air.

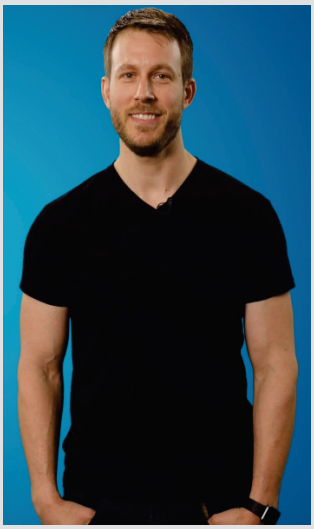
But despite these welcome security improvements, at least one of the six Wi-Fi threat categories – Rogue AP, Rogue Client, Evil Twin AP, Neighbor AP, Ad-Hoc Networks, and Misconfigured APs – can still be used to compromise WPA3 networks. Each of these types of threats represent a unique method attackers can use to either position themselves as a MitM or eavesdrop on network traffic silently. That's why more and more IT departments are creating Trusted Wireless Environments that are capable of automatically detecting and preventing Wi-Fi threats. Relying on WPA3 alone for Wi-Fi security is a mistake.

Take the Evil Twin AP attack, for example. This threat is very likely to be used in Enhanced Open Wi-Fi networks, since OWE can still take place between a victim client and an attacker's Evil Twin AP that is broadcasting the same SSID, and possibly the same BSSID as a legitimate AP nearby. Although OWE would keep the session safe from eavesdropping, the victim's Wi-Fi traffic would flow through the Evil Twin AP and into the hands of an MitM, who can intercept credentials, plant malware, and install remote backdoors. One massive issue with WPA3 it doesn't account for the fact that users and devices connecting to an SSID still have no way to confidently know that the SSID is being broadcasted from a legitimate access point or router. The SSID can still be broadcasted, with WPA3 enabled, from a malicious Evil Twin AP for example.

Don't get me wrong, the emergence of WPA3 is a solid step forward toward addressing today's significant Wi-Fi security issues. That said, it should be looked at as a complimentary security control rather than a cure-all. Any organization operating a Wi-Fi network needs to ensure that they've built a Trusted Wireless Environment that can identify and defend against Wi-Fi threats automatically. This way, the access point deployment itself prevent users and devices from connecting and falling victim to malicious threats. How much trust can you put into your wireless environment?

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

About the Author



Ryan Orsi is Director of Product Management at WatchGuard Technologies, a global leader in network security providing products and services to more than 80,000 customers worldwide. Ryan leads the Secure Wi-Fi solutions for WatchGuard. He has experience bringing disruptive wireless products to the WLAN, IoT, medical and consumer wearable markets. As a VP of Business Development in the RF industry, he led sales and business development teams worldwide to success in direct and channel environments. He holds MBA and Electrical Engineering degrees and is a named inventor on 19 patents and applications. Ryan can be reached via Twitter at @RyanOrsi and at our company website www.watchguard.com/wifi

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Operation Eligible Receiver - The Birth Place of Cybersecurity: Configurations

More than twenty years ago, the National Security Agency conducted an exercise to test the response capabilities of critical Department of Defense information systems in the case of a breach. The exercise was named Operation Eligible Receiver 97, and it concluded with startling results. Utilizing only hacking techniques available publicly, the NSA was able to completely infiltrate the DoD network and gain super user access into high-priority devices; however, one of the only known cases of prevention from the NSA reaching their targets occurred when a marine noticed suspicious traffic on the network and immediately changed configuration settings to lock down permissions.

After a two-year review of the exercise, recommendations were made for an increased focus on configuration management for all entities. Though best practices were not formally codified, the configuration management practices within compliance frameworks reflect the results of the exercise. These frameworks include NIST 800-53 and Security Technical Implementation Guides (STIGs).

Operation Eligible Receiver highlighted the importance of organizations understanding what systems they have, how they are configured, what has changed, and who made changes. With this knowledge security teams are better equipped to meet regulatory compliance and identify configuration drift.

Today's Common Mistakes

In order to improve security posture, organizations must understand what they have, and in doing so, should conduct a reliable asset inventory. It is essential for security teams to know how their network is configured and what has changed over time. When done manually, the process of keeping track of configuration changes can take large amounts of time which many security professionals do not have. A manual approach will typically rely on guesswork when answering

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

questions such as, “Who added a workstation to a domain?” or “When did this user receive administrative privileges?”

These questions pose many potential answers. Configurations may change due to user modifications, settings being misconfigured initially, or machines being turned off when group policies are entered. When configuration changes go unnoticed, organizations are left facing easily exploitable vulnerabilities. These vulnerabilities are one of the main reasons security frameworks recommend that security teams utilize a form of configuration management automation that provides consistent security metrics, as opposed to a manual process.

Setting a Standard

A majority of today’s security frameworks, such as NIST 800-53, include configuration management requirements that reflect the results of Operation Eligible Receiver 97. Guidelines within NIST 800-53 suggest practices such as setting a configuration baseline and limiting systems to only provide essential capabilities in a control known as “least functionality.”[1] Frameworks provide a basis for general requirements but do not provide details on how configuration should be set.

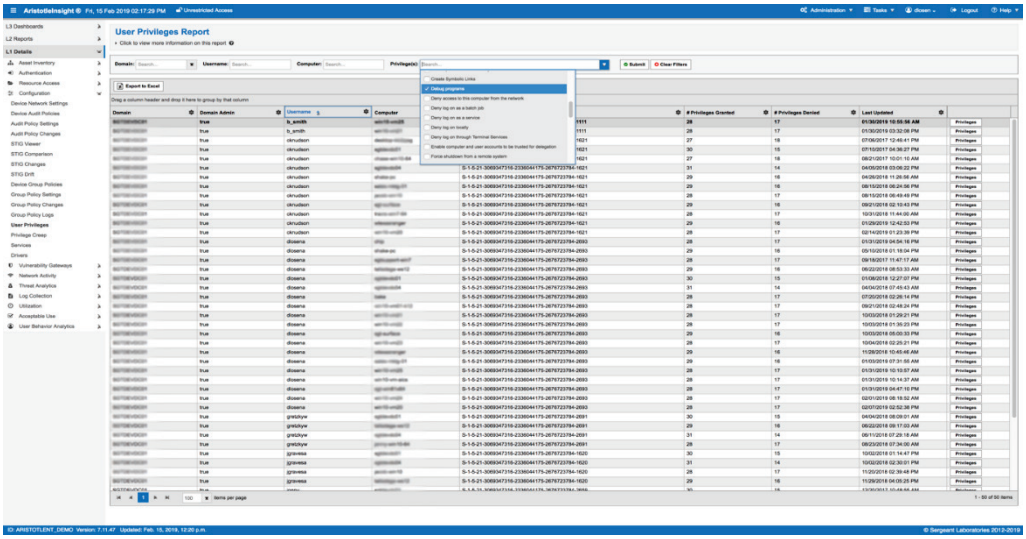
Security teams utilize validated standards, such as Security Technical Implementation Guides (STIGs) from the Defense Information Systems Agency (DISA), for specifics of how configurations should be set. These STIGs are required configuration standards for all Department of Defense devices and systems and have provided a guideline to secure areas of risk within networks since 1998.[2] Following these established standards provides security teams with clear direction in their configuration management process, while ensuring compliance with frameworks and improving the security posture of their organization.

Monitoring Configuration Drift

Even when organizations follow a configuration guideline like STIGs, without a proper monitoring solution, the risk for configuration drift remains. Drift occurs as devices, software, or users are added to a network and can be almost impossible to track manually. An example of drift affecting an organization’s security posture can be seen when looking at user rights assignments, specifically the ability to debug a program. Debug rights are typically only granted to administrative accounts, but misconfigurations and drift lead to regular users receiving them unnecessarily. Another common case is insecure software requiring SeDebugPrivilege to be turned on. When partnered with an inability to properly set permissions, organizations are put in danger of Ransomware. Attackers often use these debug rights assignments to run hash tools against files and collect passwords.

[1] https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf
[2] https://iase.disa.mil/stigs/Pages/index.aspx

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



(The User Privileges Report in Aristotle Insight lists all user privileges across all domains or only specified domains. The report may be filtered by a specific user and/or computer. The image above shows an example of viewing which user accounts have permission to debug programs.)

To overcome configuration drift, organizations require a solution to continuously monitor current configurations, along with a history of changes. Security teams need to be able to immediately determine what changed, when the change occurred, and who made the change. Although the importance of this information was learned over twenty years ago during Operation Eligible Receiver 97, accessing these details is an area in which most organizations still struggle today.

Accessing the Details with Aristotle Insight

Aristotle Insight continuously identifies risk, directs remediation, and documents results from security functions such as Configurations, Vulnerabilities, Privileged User Management, Asset Inventory, and Threat Analytics.

Utilizing the revolutionary UDAPE® technology, Aristotle Insight collects reliable data from the process level from users, devices, applications, and endpoints. A unique Bayesian Inference Engine sorts through the kernel level data highlighting actionable items to help organizations save time and better manage cybersecurity posture.

Aristotle Insight is based on Operation Eligible Receiver 97 and is the solution for cybersecurity teams attempting to implement their security process. Whether completing an audit or addressing internal policies, mature cybersecurity professionals find that Aristotle Insight is a next-generation Cyber Diagnostics solution.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

About the Author



Josh Paape is an Online Marketing Specialist at Sergeant Laboratories, a leader in security and compliance solutions that allow businesses, governments, and healthcare institutions to comply with regulations and stay a step ahead of criminals. As a graduate of the University of Wisconsin - La Crosse, Josh has experience marketing products from a variety of industries. As a contributor to CDM, he hopes to spark new thought and discussion topics in the information security community. Connect with Sergeant Laboratories: https://www.sgtlabs.com
Sergeant Laboratories Blog: https://www.aristotleinsight.com
LinkedIn: https://www.linkedin.com/company/sergeant-laboratories-inc Twitter: @Sergeant_Labs

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Prioritizing Security in a Multi-Cloud World

By Scott Manson, Managing Director, Middle East & Turkey, McAfee

Cloud awareness and adoption continues to grow, as more enterprises take advantage of the benefits that come with multiple cloud platforms. In fact, in a recent *Voice of the Enterprise (VotE): Cloud Hosting and Managed Services* study, conducted by 451 Research, 90% of respondents indicated they have some type of cloud services in place and several are already using multi cloud environments. Closer to home in the Middle East, research by MarketsandMarkets predicts that the cloud market in the region will triple to $2.4 billion by 2020, driven in large part by adoption of multi cloud.

But on the flip side, we're seeing an increase in cloud related security incidents. According to research from the October 2018 McAfee *Cloud Adoption and Risk* report, the average organization generates over 3.2 billion events per month in the cloud, of which 3,217 are anomalous, and 31.3 are actual threat events. This is cause for alarm given that 21% of all files in the cloud contain sensitive data (up17% over the past two years).

Against this backdrop, whether you are switching up your multi-cloud strategy or starting from scratch, here are a few things your organization needs to know first about multi-cloud.

Determine what features will either make or break your multi-cloud strategy

When picking the best multi-cloud structure for your business, be bold. Build a vision for what you need cloud services to do for your company—worry less about "how" and more about the "why" and "what" you need from your providers. The reality is that top cloud providers in IaaS/PaaS and, separately, SaaS spaces, are offering extremely versatile capabilities and compelling value. It is important to understand what features are critical and which ones change the way your organization works when it comes to selecting vendors.

Outside of single requests for a new or different capability, your organization needs to rationalize the different needs for each, down to "collections" of related needs. For example, consider SaaS

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

for well-known, repeatable needs first, then look to move or re-deploy capability into IaaS or build natively in PaaS for efficient applications.

Security measurements are important when architecting a multi-cloud structure

First and foremost, avoid looking at your new cloud infrastructure as a separate environment. It's not merely a new data center, so an organization also needs to consider how switching to a cloud infrastructure will shift how the organization secures assets. Consider looking to resources like the MITRE ATT&CK matrix and the Center for Internet Security's Basic and Foundational Controls list as a guide for answering this question: "In the future, how do I maintain unified visibility and security when I incorporate new cloud providers?"

For a successful multi-cloud migration, use your cloud access security layer and a platform that ultimately unifies your policy and threat identification approaches. Identity is another common challenge area. Moving to the cloud at scale often requires your organization to "clean up" your identity directory to be ready and accommodating of shared sign-on. By using an identity management and/or aggregation platform to expose identity to well-known cloud services, you will be able to ease the cloud implementation burden and threat exposure of any given provider.

Ensure compliance

It's important to know that your organization's compliance requirements are not mitigated or transmuted simply because the data has left your internal environment and entered the one your cloud provider(s) uses. As your organization matures, the way you manage and align your cloud provider's capabilities to your compliance requirements should evolve accordingly.

Initially, ensure that your company requires business unit executives to apply or accept the risk of compliance obligations where service providers may not have every requirement. Your legal team should be a part of the initial purchase decisions, armed with technical knowledge to help identify potential "rogue" cloud services and policy guidelines that dissuade employees from adding services "on a credit card" without appropriate oversight.

As your organization gains more experience with the cloud, request that providers share copies of the SSAE16 attestations / audits. This, together with more formal due diligence processes, should become commonplace. Organizations looking to advance in this space would be well-advised to look at the Cloud Security Alliance's STAR attestation and the associated Cloud Controls Matrix as a ready accelerator to benchmark cloud providers.

Secure buy-in from exec/C-level on a multi-cloud strategy

Use of cloud services should reflect the strategic focus of the business. Technology leaders can leverage the benefits of these services to underpin initiatives in efficiency, bringing innovation to market and controlling costs. To strengthen this message, technology department heads should

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

consider the metrics and operations adjustments that will allow them to demonstrate the enhanced value of the cloud beyond just the bottom line. If you are trying to get exec/C-level buy in, consider the following:
How will you measure the speed of introducing new capabilities?
Are new areas of value or product enhancement made possible through cloud services?
How will the organization measure and control usage to hit your cost targets?
How do you know whether your organization is getting what you have contracted for from cloud providers?
Do you have a mechanism for commercial coverage of the organization when things go wrong?

Protect your organization and secure the cloud

Organizations will often "upgrade" in some areas of basic security (perimeter, basic request hygiene) when making the move to well-known cloud providers. How the overall security posture is affected depends heavily on the level of diligence that goes into onboarding new cloud providers. Implementing critical technical measures like the Cloud Access Security layer and policy around how the cloud is procured and technically implemented should drive basic control requirements.

As the number of cloud providers scales in the environment, your organization needs to assess and document them based on how much your organization depends on a given service and the sensitivity of the data those services will hold. Services that are prioritized higher on these two fronts should have increased organizational scrutiny and technical logging integration in order to maintain the overall defensive posture of the company.

Finally, as with any other technology trend, the missteps in making the transition to business and consumer cloud services have received outsized coverage. Take the time to dive into the "how's" and "whys" of early cloud breaches to avoid becoming a potential victim—after all, when it comes to security, it is better to learn from someone else's (unpleasant) experiences!

About the Author



Scott joins McAfee from his previous role at Cisco, as the Technology and Cybersecurity Director in Middle East and Africa with a proven track record of delivering sales results across the Middle East, Africa and Europe. His technology and solution orientated sales experience spans the last 19 years working ostensibly in this market. Prior to that, 8 years ago, Scott ran cloud sales and operations for BMC software in EMEAR and has always enjoyed working in the leading-edge technology markets to find more optimal ways to take these respective products to market

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Overcoming Software Security Issues Caused by the Third-Party Software Procurement Model

As software becomes more sophisticated, organizations of all sizes continue to harness its capabilities to transform their go-to-market strategies and streamline their operations. Whether the software is developed in-house, through third-party vendors or is of the pre-packaged, off-the-shelf variety; businesses are looking to exploit the latest innovations in order to more effectively compete in the marketplace.

With the rise in the value of intangible software-based services and the data collected through those services, companies have invested heavily in security software and systems in order to protect their most important assets. At the same time, DevOps have been given the mandate to implement more and more innovative functionality, as quickly as possible.

This has put the security and DevOps teams at cross-purposes. Getting software provisioned as quickly as possible has not given the security team's adequate time to ensure full product security. Until recently, ensuring software security has not had the same priority.

That is changing. With new data security and privacy regulations being enacted in some states and the E.U., the C-Suite is pushing hard to have its cake and eat it too. In other words, CEOs, CIOs and CSOs are mandating that software be more capable, developed and provisioned more quickly, while being more hardened against attack.

The current third-party software procurement model makes the previously mentioned C-Suite goals unattainable.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Today's Third-Party Software Procurement Model

By sourcing third-party code instead of developing all software internally, DevOps teams lower their overall development costs and quickly add innovative capabilities to help their businesses remain competitive. Leveraging third-party software components increases efficiency because it saves months or years of originally required development time.

In fact, the majority of the custom software in today's enterprise is sourced externally or contains code from third-party vendors that is built using open source code components. Interestingly, the third-party code is almost always delivered in binary format. Though this delivery method protects the third-party development teams' intellectual property, it makes it almost impossible to accurately account for all open source software (OSS) components in the provided binaries. This problem is compounded when an enterprise platform is updated by different software vendors, over extended periods of time and integrated with off-the-shelf applications.

Why Open Source Components Matter

More than 90 percent of all the software written and in use today integrates some open source code. Such code is used in operating systems, network platforms and applications. This trend will only continue to grow because, by leveraging open source, DevOps can lower integration costs and quickly add new innovations the C-Suite was clamoring to have yesterday.

Whether software is proprietary or open source, it harbors security vulnerabilities. Because of its transparent and collaborative development model, open source code tends to be better engineered than a comparable piece of proprietary code. And thanks to its openness to extension and reuse, open source code is used extensively. This means that a security vulnerability in a piece of open source code is likely to exist across a multitude of applications and platforms.

The open source community is becoming increasingly active in finding and publishing new security vulnerabilities. Consequently, known open source software vulnerabilities become a road-map for hackers to target and attack businesses' systems. Those systems that contain known vulnerabilities that have been left unpatched or unaddressed are likely to fall victim to data loss and theft.

For the past three years, we have seen an escalation in the number and severity of security breaches and data thefts. In many cases, the access point has been hackers leveraging known open source software vulnerabilities. The most costly to date, the 2017 Equifax breach, was due to a vulnerability in Apache Struts that had been known about for months. The Equifax team's failure to patch the vulnerability in their software was catastrophic.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Implementing Security Checks at Strategic Points & Addressing Them

Businesses will continue to rely on third-party vendors to supply their custom software. IT departments will continue to purchase off-the-shelf software and rely on system integrators for customized software components. DevOps teams, custom software providers, system integrators and off-the-shelf software will continue to leverage the collective, innovative power derived from open source.

Given that these trends are likely to accelerate further, businesses can address a significant number of known open source security vulnerabilities by implementing vulnerability checks at strategic points – and then fixing them.

In a typical platform, it is impossible to know what open source code elements exist in the software. Most platforms are an amalgamation of software developed in-house and by third-party contractors. It has likely gone through several upgrades, and key purchasers and contributors are no longer with the business or the custom software vendors.

Exacerbating the issue is that while custom software makers provide their clients with lists of software components in the code they are delivering, they themselves are unlikely to know all of the open source code elements that exist in their code. This is just as true for the in-house development teams.

A solution is to use a binary code scanner to determine open source code components any time new software is procured or developed. This will give the security team the opportunity to understand what exactly the software is composed of, and gives the DevOps team the ability to address known vulnerabilities prior to deployment, while ensuring compliance with all applicable licenses.

Additionally, whether the software development model is waterfall or Agile, it is critical for these scans to be built into the early part of the development cycle. Recognizing the existence of known open source security vulnerabilities in the code is not enough. There must be adequate time to address them through patching and/or other workarounds.

With the constant drive to improve software functionality for every aspect of a business, companies will increasingly rely on third-party software that contains open source code components. Failing to understand and address open source code license issues and known vulnerabilities in newly developed or procured software is a recipe for brand damage and financial loss. Implementing binary scans early in development or procurement and allowing the DevOps teams to have the software corrected will save businesses time and money in the long-run.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

About the Author



Tae Jin "TJ" Kang is a technology industry executive and entrepreneur. He is the president and CEO of Insignary. In addition to founding a number successful technology startups, Mr. Kang has held senior management positions with global technology leaders that include Korea Telecom and Samsung Electronics, among others.Mr. Kang can be reached online at tjkang@insignary.com and at our company website www.insignary.com

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Phishing in the Dark: Employee Security Gaps Are Growing

By Atif Mushtaq, CEO of SlashNext

Phishing is often equated with phishing emails containing malware attachments or links to malicious sites. However, as email security solutions improve and phishing awareness training makes employees more careful about what they click, threat actors are moving to new phishing attack vectors where defenses are not as strong and users' guards may be less vigilant. Most organizations are ill-prepared for these new attack vectors or the growing number of unknown, zero-hour phishing threats lurking on the web.

The phishing threat landscape has already expanded well beyond email and shows no sign of abating. Increasingly, employees are being subjected to targeted phishing attacks directly in their browser and via specialized apps outside their inbox. These targeted attacks are executed with highly legitimate looking sites, ads, search results, pop-ups, social media posts, chat apps, instant messages, as well as rogue browser extensions and free web apps. Users who encounter these threats on the web or embedded in apps can easily make a disastrous click that opens their company up to costly data breaches, ransomware, or other extortion attempts.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

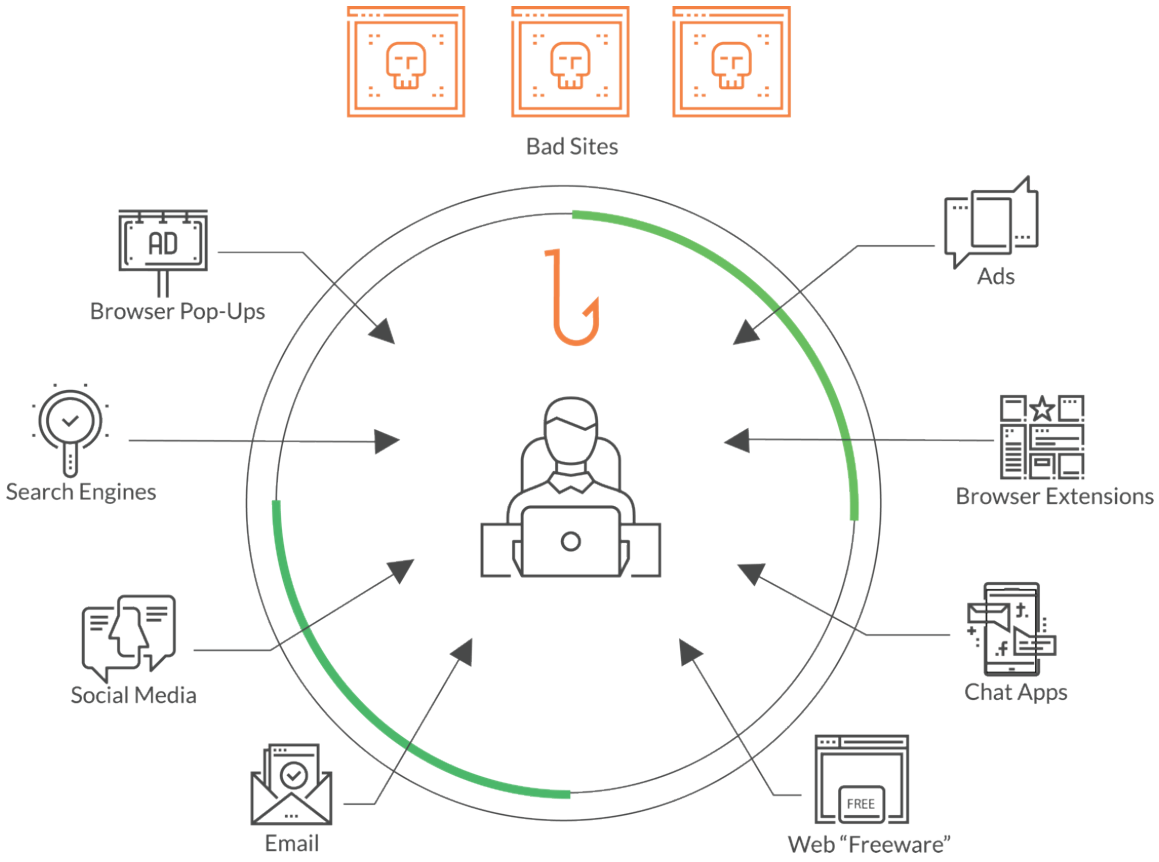


Figure 1: Phishing threat vectors have expanded beyond the inbox

Most companies lack adequate safeguards against this new phishing threat landscape and many IT security leaders do not fully understand how prevalent the dangers are from this growing threat. As a result, organizations are left in the dark when it comes to understanding their exposure to modern phishing risks and how to evaluate needed solutions to protect their employees.

The 2018 Phishing Survey we conducted of 300 IT security decision-makers shows that 95 percent of respondents underestimated how frequently phishing is used to breach enterprise networks. Only 5 percent of survey respondents realized that phishing is involved in over 90 percent of successful breaches. Most also do not realize how fast phishing threats move, typically lasting minutes to just a few hours before sites are taken down and cybercriminals move on to evade existing security controls.

This survey data suggests a dangerous lack of understanding about the implications of new phishing attack vectors and the implications of short-lived, fast-moving phishing threats on the web. Despite layered security controls and phishing awareness training programs for employees, many organizations remain unaware of their increased vulnerability to this threat landscape.

Another data point to note was that nearly two-thirds of respondents cited shortfalls in employee awareness and training as their top concern for protecting workers against social engineering and

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

phishing threats. Furthermore, almost half of respondents (45 percent) said that they experienced 50 or more phishing attacks per month, and 14 percent said that they received more than 500 phishing attacks per month.

In addition, only a third (32 percent) agreed that current threat feeds and blacklists are adequate to protect users from new phishing sites, and 39 percent doubt the ability of their current defenses to reliably detect phishing attacks. So, what can be done?

A Real-Time Shield against Fast-Moving Phishing Threats

According to Webroot, 95 percent of web-based attacks now use social engineering to trick users. The methods are becoming more sophisticated, in large part because users are increasingly trained to recognize security risks, as well as owing to improvements in network, application and browser security. Organizations that are increasingly vulnerable must rethink how they plan their defenses, and a new approach is clearly needed.

A more effective security approach combines solutions for real-time as well as preemptive phishing site detection that can definitively spot malicious sites based on page contents and server behavior rather than relying on URL inspection and domain reputation analysis — methods which are easily fooled by more sophisticated hackers. When combined with automated ingestion of real-time phishing site blacklists by URL filtration or blocking defenses, organizations can better shield their users from fast-moving, zero-hour phishing threats which would typically be unblocked.

Note that not all URL filtration and blocking defenses such as firewalls, web proxies, gateways, and DNS servers are capable of continuous blacklist updates, but the security industry is improving. It is what is needed to close the gap on phishing security measures to better protect employees.

About the Author



Atif Mushtaq has spent most of his career on the front lines of the war against cybercrime. Before founding SlashNext he spent nine years as a senior scientist at FireEye where he was one of the main architects of its core malware detection system. Mushtaq has worked with law enforcement and other global agencies to take down some of the world's biggest malware networks including Rustock, Srizbi, Pushdo and Grum botnets.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Automated STIG "Hardening" Finally Comes to Government IT

For the thousands of hard-working men and women responsible for securing government IT networks to the Defense Information Systems Agency's mandatory "STIG" standards, the task can be daunting and even somewhat thankless.

That is because the STIGs (Security Technical Implementation Guides) outline hundreds of pages of detailed rules that must be followed to properly secure or "harden" the government computer infrastructure.

Given that this work is typically a manual process, it can be extremely tedious and time consuming for IT personnel. In fact, it is estimated that the government spends hundreds of millions annually to remain in compliance with the STIG standards.

So, as new software tools enter the market that automate the process to near push-button simplicity, the first reaction after "sounds too good to be true," is considerable relief.

By automating the process, a task that once took weeks – or even months – can be completed in a few hours across all endpoints. Ongoing security updates are also automatic and can be completed in minutes.

Explaining the STIGs

To be fair, there can be a considerable "fog" surrounding the STIGs.
The STIGs essentially exist because government networks are largely built using commercial operating systems (Windows/Linux), database management systems, web servers and other network devices. The STIGs, therefore, define alterations in operating environment settings so these environments can be configured in the most secure manner possible.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Unfortunately, once an application environment is hardened to the STIG specifications, it can cause installed application to "break," meaning it won't install and/or run properly. This impacts both new and legacy applications installed on the system.

Why do applications break? Because they are rarely designed or tested to operate in STIG environments.

For example, if the STIGs require altering some of the controls of the Windows or Linux operating system the application is built on, the application will break. If an application requires specific capabilities to operate and the STIGs prohibit or blocks those capabilities, the application will fail to load or operate. And so on.

Unfortunately, there are no generic set of STIG "rules" that can be applied to all applications. Instead, server policies must be manually adjusted on an application by application, server by server basis - which can take many weeks and cost in excess of $10,000 annually, per server instance.

"If the same policies and configurations could be implemented on all systems, STIG compliance would be a rather easy exercise," explains Brian Hajost of Steel Cloud and an expert on automated STIG compliance. "Commercial and government applications respond to security policies differently. The controls for each system, therefore, have to be uniquely adapted or tuned to each application environment."

This painstaking task often falls to system administrators, application administrators or information assurance staff.

"There are thousands of IT people across government that are asked to address the STIG compliance manually, but many times are not experienced or trained to do so," says Hajost. "So, they muddle through, but the initial hardening effort can take weeks or even months."

Fortunately, new automated tools are available that automate STIG compliance. Products such as ConfigOS from Steel Cloud harden existing government networks automatically, even across complex and disparate infrastructures with varying security levels.

ConfigOS identifies and hardens all controls considered a potential security risk. As outlined in the STIGs, risks are categorized into three levels (1/2/3) with Category 1 being the most severe and having the highest priority.

The software then produces a domain-independent comprehensive policy "signature" including user-defined documentation and STIG policy waivers. In this step alone, weeks, or months of manual work can be completed in an hour.

The signature and documentation are included in a secure, encrypted signature container that is used to scan endpoints (laptops, desktops, physical/cloud servers) without being installed on any of them. The time it takes to remediate hundreds of STIG controls on each endpoint is typically under 90 seconds and ConfigOS executes multiple remediations at a time.

"The government publishes the [STIG] book and we are just automating the tedious work to get the job done," says Hajost.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

ConfigOS supports over 6,000 standard STIG controls in a wide range of tested content. However, the software is also designed to allow users to tailor controls to respond to an application's requirements.

"We could enforce the STIGs to the letter, but that doesn't work if it means the application will not run," explains Hajost. "So ConfigOS creates an operational policy that is as close to the published STIGs as possible, but still allows the application to function as designed," explains Hajost.

The signature containers can then be transported across large and small networks, classified environments, labs, disconnected networks, and tactical environments with connected and disconnected endpoints. No other changes are required to the network, security and no software is installed on any endpoints.

To date, ConfigOS has been licensed by just about every branch of the Department of Defense, as well as parts of DHS, HHS, and Department of Energy. The product is also used by large defense contractors and in programs for all branches of the military.

Hajost adds that automation is even more important given that STIG compliance is an ongoing process with new security updates introduced periodically

The STIGs, for example, are updated every 90 days to account for newly discovered vulnerabilities as well as changes and updates to by the vendors supplying the major operating environment components.

With ConfigOS that means that within two business days after DISA publishes a new version of the STIGs, new tested production content is made available to customers.

"When it is a manual task, security updates to existing applications and operating systems are typically delayed by months," says Hajost.

The software can also speed implementation of new network applications, servers and appliances by evaluating and hardening each prior to installation.

Hajost estimates automating the process reduces initial hardening time by 90%, while reducing system security policy maintenance expenses by about 70%.

Given the potential cost savings of automating STIG policy compliance exceeds hundreds of millions of dollars annually, IT personnel struggling to secure government networks manually may find this one task they are happy to automate.

About the Author



Jeff Elliott is a Torrance, Calif.-based technical writer. He has researched and written about industrial technologies and issues for the past 20 years.

For more information about ConfigOS from SteelCloud call (703) 674-5500; or visit www.steelcloud.com.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Software Should Come with a "Nutrition" Label

By Tae Jin "TJ" Kang, CEO, Insignary, Inc.

During the latter half of the 18th Century and throughout the 19th Century, the Industrial Revolution fundamentally changed the geographical, political and commercial landscape in Europe and the United States. Citizens that had previously lived in predominantly agrarian, rural societies found themselves in living in urban and industrial ones.

This industrial and decidedly technological shift in the Western economies meant that people became focused on creating, building and selling more specialized products and services. While businesses produced a seemingly endless variety of higher quality products, the sheer amount of choice engendered consumer confusion and some fraud.

By the start of the 20th Century, consumers were often lied to in advertisements and the composition of the food and medicine they were consuming was difficult to determine. In 1906, the United States passed the Food and Drug Acts. Still in effect today, they prohibit interstate commerce in misbranded and adulterated foods, drinks and drugs.

In 1990, the Nutrition Labeling and Education Act was passed. It required all packaged foods to bear nutrition labeling and all health claims for foods to be consistent with terms defined by the U.S. Government. As a result, the food ingredient panel, serving sizes and terms such as "low fat" and "light" were standardized. It is almost inconceivable that a consumer would purchase a product without this information today.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Why should software be any different?

Consumer data and privacy is put at risk daily by the software they use in the PCs, smartphones, tablets and other consumer devices. The software-based services they use are also at risk. Their retailers', banks', credit monitors' and governments' systems are being hacked at a higher frequency and cost.

Open Source Software – Boon & Bain

A great deal of this is due to the increased use of open source code elements in software today. It is estimated that more than 90% of the software in development and use today contains open source. Its use is tied to its ability to be quickly integrated, delivering tremendous levels of innovation. However, this innovation comes with a cost. In 2018, 16,555 known software vulnerabilities were published by National Vulnerability Database (NVD), a new record.

The open source community is now constantly finding and publishing new security vulnerabilities. Consequently, known open source software vulnerabilities become a road-map for hackers to target and attack businesses' systems. Those systems that contain known vulnerabilities that have been left unpatched or unaddressed are likely to fall victim to data loss and theft.

Build Your Own Software Composition "Nutrition" Label

Be it developed in-house, custom-built by a third-party, off-the-shelf or some kind of amalgamation; the level of software sophistication and complexity continues to grow rapidly. Someday, in order to better protect businesses and consumers, governments may mandate, like they have in the food and medicine industries, software composition or "software nutrition" labeling.

Until that day comes, businesses should require their software vendors to provide them with this information. Unfortunately, not all software vendors provide this information citing many reasons, such as protection of proprietary IP, among others. Smart businesses can take a more proactive approach by analyzing third-party software and building a software component list of their own.

While a great deal of the code delivered today to enterprises is accompanied by documentation that lists the software components, many third-party vendors do not provide their clients the list of software components.

Additionally, third-party software products are likely to be a combination of in-house developed and procured code. This makes analyzing and tracking open source software elements incredibly challenging. Given that this code is delivered in binary format, businesses have had to take the composition documentation on faith.

New fingerprint-based binary scanning technologies make building a software "nutrition" composition label relatively easy and straightforward. Additionally, these scanners find small, open source code elements, catalog them and match them against databases of known security

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

vulnerabilities. If they find vulnerabilities, they alert the DevOps and security teams so they can be addressed.

Like the vendors at the turn of the 19th Century, software providers are coming under ever increasing scrutiny by their enterprise, SMB and consumer customers. In order to increase brand trust and reap larger profits, software vendors should look to provide the most accurate software composition documentation with their binary files. Until that time, business software purchasers should look to protect themselves and their downstream customers from potential data theft and privacy loss by leveraging fingerprint scanning technologies to accurately understand the composition of their software, before it is deployed.

About the Author



Tae Jin "TJ" Kang is a technology industry executive and entrepreneur. He is the president and CEO of Insignary. In addition to founding a number successful technology startups, Mr. Kang has held senior management positions with global technology leaders that include Korea Telecom and Samsung Electronics, among others.Mr. Kang can be reached online at tjkang@insignary.com and at our company website www.insignary.com

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Shattered! Security in a Fragmented World of Workloads

By Satyam Tyagi, Director Product Management, ColorTokens Inc.

Look at me, I'm in tatters!

> *Don't you know the crime rate is going up, up, up, up, up?*
>
> *To live in this town you must be tough, tough, tough, tough, tough!*
>
> *You got rats on the West Side*
>
> *Bed bugs uptown*
>
> *What a mess this town's in tatters, I've been shattered*

Enterprise IT and applications have evolved over the last decade with the adoption of virtualization, micro services, hybrid data centres, and dynamic multi-cloud environments. The value of data has increased with extensive digitization of every information and process necessary to run the business.

Maintaining a consistent and comprehensive security posture is a challenge. Security teams have to do a lot of heavy lifting to work in these challenging environments. This fragmented and incomplete picture and always playing the catch-up game with the dynamic infrastructure puts a lot of pressure on the admins, resulting in misconfigurations and inconsistent security posture, paving the way for breaches.

More and more about some useless information

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

I can't get no satisfaction, I can't get no satisfaction

Cause I try and I try and I try and I try

I can't get no, I can't get no

When I'm driving' in my car, and the man come on the radio

He's telling' me more and more about some useless information

Supposed to fire my imagination

Traditional security solutions like firewalls and antivirus are insufficient and incomplete. More firewalls and more antivirus are not going to cut it.

The fact is only 15% of the traffic flows through the perimeter firewalls and no matter how good or sophisticated the firewall is, it can only do so much. And traditional antivirus and signature-based techniques can only catch a small percentage of attacks.

There are multiple vendors who are pushing different security tools in the cloud, from server hardening, vulnerability management, visibility, micro-segmentation, system integrity management, application control whitelisting, EDR etc.

The biggest challenge is that these solutions are fragmented and are artificially put together with a SIEM, which is cumbersome, requires months if not years of tuning and teams of analysts dealing with false positives.

Get what you need, oh yeah!

But if you try sometimes you just might find

You just might find

You get what you need, oh yeah

What the security team needs is a comprehensive and integrated security platform for their endpoints and workloads.

Need 1: Understand the Comprehensive Security Picture

Security teams need a place where they can see the complete picture. A consolidated view where one can understand vulnerabilities in the context of exposure. Malware infections in the context of the threats they pose. And network traffic and application access in the context of the authorization policy. Without a comprehensive picture, security teams can neither understand the situation nor communicate it to the stakeholders.

Need 2: Enforce Business Security Needs

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Once security can see the comprehensive picture, they need the ability to enforce business needs. Which applications are dealing with sensitive data and need to be isolated and protected; which users are privileged or need access to privileged data and applications to perform their business function? This needs to be done in a way such that it can scale. If every environment, cloud, operating system, software, application, and user device needs a separate control, then it does not work. The work of the security teams becomes constantly translating the ever-changing business needs into infrastructure specific technologies which are never the same.

Need 3: Simplified Incident, Investigation and Remediation Centre

Acknowledgement that you need to have the ability to detect and remediate attacks is crucial – no matter how sophisticated our protection maybe. Having a consolidated platform means that no fine tuning of the incident centre for months to integrate all products. No cumbersome and time-consuming false positives because the disjoint products have no context, where one product understands vulnerability but does not understand it is shielded and quarantined, where another understand botnets and malware but does not know the business value of compromised systems.

At ColorTokens we provide a comprehensive security platform that is designed around these key needs of security teams. In fact, we offer a complete managed service around our SaaS cloud based technology. Such that the security teams can say …

Hey, you, get off my cloud

Hey, you, get off my cloud

Don't hang around because two's a crowd

On my cloud, hey, you.

About the Author



Satyam Tyagi is the Director of Product Management at ColorTokens Inc. He is an industry thought leader in security and networking, responsible for significant advances in end-point, mobile and application security. He was awarded four patents in application security and networking, including products sold by Cisco and Avaya. An inaugural director of Samsung Mobile Enterprise Lab, Satyam led the team originating Samsung Knox smartphone security enabling Samsung phones to be certified for US military use. At Zscaler, he led mobile security products protecting sensitive data for some of the world's largest enterprises. Satyam also held roles in product management and engineering at Juniper, Sipera (Avaya) and Cisco. He holds a Master's in Computer Science from University of North Texas and Bachelor's in Computer Science and Engineering from IIT (BHU). Satyam can be reached online at satyam.tyagi@colortokens.com and at our company website https://colortokens.com/

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



How Organizations Should Choose a Load Balancer for Managing and Securing Application Traffic in the Cloud

By Kamal Anand, Vice President and General Manager, Cloud Business Unit at A10 Networks

Load balancing of application traffic has been around for a long time. But, as more organizations move to the private and public cloud, it's undergoing significant changes. Let's look at some of the important considerations of this evolving technology.

Three major requirements underlie IT operations and DevOps today: agile, efficiency and, multi-cloud operations.

- Agile: The movement toward public cloud is arguably driven by an organization's desire to deliver more functionality faster. Public clouds like Microsoft Azure and Amazon Web Services (AWS) allow organizations the capacity and capability necessary to drive that agility.
- Efficiency: Doing more with less puts a great amount of pressure on IT operations. With infrastructure as a Service (IaaS), management is divided into infrastructure management and application management. IaaS addresses availability, elasticity and efficiency of operations, and cost. Application teams then address the efficiency of application delivery.
- Multi-Cloud Operations: Companies prefer to keep their data within their own data centers. Most adopt a multi-cloud infrastructure to balance privacy and efficiency. Less-sensitive data may be stored in public clouds while sensitive data remains in their private cloud.

Current State of Load Balancing in the Cloud

Advanced load balancing has emerged as an important element of modern operations. Load balancing has evolved given these three requirements of DevOps. Load balancing historically only handled distributing the traffic amongst servers and, in some cases, SSL offload.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Load balancers are in the middle of an organization's application traffic. They're place in a critical position to see a tremendous amount of information about the flowing traffic.
Advanced load balancing provides more value and efficiency to the operations team. This is especially true with micro-services architecture and the deployment of datacenter containers or Kubernetes environments.

5 Benefits of Advanced Load Balancers for the Cloud

The advantages of advanced load balancing can be condensed into five main categories:

1. Increased visibility, insights and analytics.
2. Integrated security.
3. Centralized management.
4. Automation and integration.
5. Container and Kubernetes integration.

Let's take a closer look at each benefit and why advanced load balancing plays an important role in promoting team agility, improving security, streamlining workflows and using new technologies.

1. Increased Visibility, Insights and Analytics

Increased visibility, insights and analytics allow organizations to accomplish a number of goals, spanning from basic to cutting-edge.

- Improve network traffic monitoring by including application traffic with traditional infrastructure monitoring. Organizations can learn what traffic is coming and how efficiently it is being served.
- Detailed reports and health statistics, and thus better understand how their infrastructure is performing.
- Operations teams can complete the troubleshooting process more efficiently.
- Analytics and insights become proactive rather than reactive. A company might notice a latency issue and work to fix it before users start sending in support tickets.
- Use the insights to perform actions automatically. Automatically adjust the infrastructure due to a change in application traffic, or block a user identified as an attacker.

2. Integrated Security

Load balancers are placed directly into the flow of all network traffic. That placement presents an ideal opportunity to understand the behavior and differentiate between good and bad traffic. Load balancer can automatically detect anomalies and, as a result, stop malicious traffic.
Infrastructure security is the responsibility of public cloud providers like AWS and Azure. Application-level security is still the responsibility of application owners as per Shared Security Responsibility. It is essential organizations understand the importance of full stack security and look for load balancers with integrated security.
Security products have traditionally been overly complicated and difficult to configure. Modern security products' makes it easy for operations teams to quickly configure and use critical functions. Advanced

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

load balancers capable of integrating with advanced security products can increase efficiency and strengthen defenses.

3. Centralized Management

Centralized management eliminates the need to log in to individual load balancers. There you can see the entire application stack within a single pane of glass. Public clouds allow the application stack to run across multiple regions. Centralized management allows application traffic to be managed across all regions within a single console. This provides both efficiency and easy manageability.

Advanced load balancers integrate with centralized management. Central management of policies is even more valuable when load balancers are deployed across multiple clouds. This power adds centralized visibility and analytics of the environment. The centralized analytics correlates data coming from various sites. This facilitates actionable insights across the entire environment.

Observations from one site, especially related to cyber security attacks, can be used for proactive actions on other sites. For example, a cyber attacker is identified at one site they can be blocked at all sites from a central console.

4. Automation and Multi-Cloud Integration

More than 70 percent of organizations have a multi-cloud environment. Any technology they adopt today must integrate across the entire environment. This includes public clouds, private clouds, data centers, and bare-metal servers. This requirement applies to choosing a load balancer.

It's important that load balancers have APIs for integration. Many enterprises have already implemented continuous integration/continuous delivery pipelines. Load balancers need to integrate with DevOps toolchain and infrastructure platforms.

Full integration is achieved only when API calls are possible in all directions. DevOps tools can call the load balancer API. Load balancer can call the external API in case of an alert or event.

5. Containers and Container-Orchestration Integration

The industry is adopting containers and container orchestration systems. According to a recent survey by 451 Research, 71% of enterprises are either using or evaluating options like Kubernetes and Docker.

Applications are moving from monolithic to a micro service architecture. Deployments are migrating from traditional hardware servers with virtual machines running on the cloud, to containers running on multiple environments.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Kubernetes and Docker have been adopted by many of the industry's top players, including Google, Amazon, Microsoft, VMware, RedHat, IBM and more. Docker and Kubernetes have as a result become de-facto standards.

Data center criteria should include integration with container technologies. It must automatically scale containerized applications as needed while simultaneously maintaining complete visibility. This eliminates the need to manually configure policies or manage scaling.

About the Author



Kamal is responsible for A10 Networks Cloud Business, including the Management and Analytics platform. He joined A10 Networks via its acquisition of Appcito, where he was the co-founder and CEO. Apachito was a venture-funded provider of a SaaS, multi-cloud ADC solution. Kamal has over 25 years' experience in the areas of software, networking and security.

Julia can be reached online at (kanand@a10networks.com) and at our company website http://a10networks.com

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



SaaS DNS Security: Are you Protected?

By Kanaiya Vasani, Executive Vice President, Products and Corporate Development at Infoblox

Are Software as a Service (SaaS) security solutions truly the panacea they are publicized to be?

The answer is, it depends on how the SaaS solution is architected. A majority of SaaS-only security solutions are "overlay" solutions that simply provide an additional layer of security on top of an enterprise's existing network and security infrastructure. These overlay solutions are easy for the vendor to develop, but difficult for the customer to combine with other existing security solutions and derive value from. In contrast, a hybrid approach to security is one that tightly integrates SaaS solutions with an enterprise's existing IT infrastructure and leverages SaaS capabilities to seamlessly extend and scale on-premise solution performance. With a hybrid solution, the vendor does the heavy lifting of seamless integration with existing infrastructure, thus providing a unified solution, which unlocks valuable context available from the on-premises infrastructure. Such context allows the hybrid solution to prioritize threats better. In addition, the unified solution enables sharing of data with broader security ecosystem for an efficient and optimized incident response.

DNS as a Security Tool

As enterprises gear up to handle the barrage of increasingly targeted and sophisticated cyber-attacks, security architects must take advantage of the visibility that each IT asset can provide. DNS is an excellent example of a scalable and pervasive network infrastructure protocol that offers unmatched visibility into network traffic patterns, malicious and otherwise. If used optimally, DNS can provide an affordable and scalable first line of defense for detection and mitigation of the vast majority of known threats. Behavioral analysis of DNS traffic can also serve as an "early warning system," flagging potential zero-day threats in the network.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

When it comes to DNS security, many organizations are interested in cloud-based SaaS-only solutions, which they think will be easier to implement and provide sufficient functionality to identify infected devices and protect against threats like malware and phishing attacks. SaaS for DNS security can be effective, but only when integrated with on premise systems.

Overlay (SaaS-only) solution challenges

The way most SaaS-only DNS security solutions work is to enable businesses to forward their DNS traffic to the cloud, where DNS queries are processed and potential malicious activity is detected and flagged. In order to identify the infected end host, these solutions require the deployment of DNS forwarding proxies (running on virtual machines) deep inside the enterprise network or the use of endpoint agents. As enterprises move their workloads into private and public clouds, deploying and managing these proxies can become even more complicated.

Most enterprise DNS servers support the ability to block access to domains via configuration of response policy zones. By directing all DNS traffic to the cloud, SaaS-only solutions fail to leverage these existing security capabilities, which allow an enterprise to block the most egregious threats at the very first DNS server that detects it.

Further, because overlay solutions do not integrate with the incumbent enterprise DNS architecture, they leave enterprise administrators stuck with operating two separate and siloed management systems and having to manually correlate data between the two. Beyond the inefficiencies of managing two separate DNS systems, an even more significant drawback is that you sacrifice visibility and security context. Specifically, overlay solutions are unable to leverage the rich contextual data available in the enterprise DNS, DHCP, and IP address management systems (DDI). This context can help with prioritization of security threats, a key requirement for security analysts who are swamped with alerts they can't keep up with.

Why a hybrid approach for DNS security

To recap, a hybrid DNS security approach weaves security right into the network control fabric of the enterprise. Tight integration with the incumbent enterprise DNS, DHCP, and IPAM infrastructure simplifies deployment and management brings efficiency and scale and improves overall security efficacy and effectiveness.

Hybrid solutions offer enterprises complete flexibility in terms of deployment options – the best combination of on premise and SaaS. And regardless of the deployment model, enterprises get all the benefits of integration with their DDI infrastructure:

- Reduces complexity: Hybrid solutions take away the hassle of deploying proxies throughout the network. The on premise component of the solution can be configured to forward recursive DNS traffic to the DNS service in the cloud while preserving the ability to identify the end host

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

associated with any security event detected in the cloud. This ability can be seamlessly extended to workloads running in private and public clouds as well.

- Increases flexibility: With a hybrid solution, customers may choose to leverage their on premise DNS servers to block access to domains based on curated low false positive threat intelligence and leverage the cloud for a more comprehensive threat assessment based on a lot more threat data as well as big data analytics.
- Improves visibility: Hybrid solutions offer a single pane of glass for managing security across the enterprise DNS infrastructure.
- Enables threat prioritization: Rich network context data, e.g., where the device sits in the network, who is the user, how critical is the asset from a business standpoint, etc., that was locked up in network control protocols located on premise can be made available in the security dashboards and used to intelligently prioritize threats for remediation.
- Improves intelligence: On-premise network and user context is automatically shared with the SaaS component of the solution, and security events detected in SaaS can be shared back with the security ecosystem on premise, creating a closed intelligence loop across the enterprise. Indicators of compromise can be shared in real time with existing security infrastructure (on premise or in the cloud) including endpoint security, NAC, vulnerability management, and SIEM solutions for an automated incident response such as quarantine, scan, or killing of malicious processes running on suspicious devices.

About the Author



Kanaiya is an executive leader with a proven track record of bringing new technology to market as well as managing large businesses and product P&Ls. He leads product management, product & technical marketing, corporate development and business development for Infoblox. Prior to Infoblox, Kanaiya held several senior leadership roles at Juniper Networks including Corporate VP for Business and Corporate Development and VP of Product Management for Juniper's core routing business. He has extensive experience in software, networking and telecom, and has previously served in senior management positions at Terayon, Lantern Communications, ADC Telecom, and Network Systems Corp. He holds Masters Degrees in Management of Technology and Computer Science from University of Minnesota.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide


EVENTS

connect:ID 2019

TECHNOLOGY · SOLUTIONS · POLICY

Walter E. Washington Convention Center, Washington, DC, USA



THE PREMIER ARENA FOR NEXT GENERATION IDENTITY SOLUTIONS

IDENTITY RE-IMAGINED

- Through a world-class exhibition connect:ID 2019 will bring together identity technology innovators, industry distributors, and solution providers with thought leaders and policy makers in markets where next-generation secure ID is needed.
- At connect:ID 2019 join: **1500 Event Attendees** | **500 Conference Delegates** | **125+ Exhibiting Organizations** | **150 Speakers** | **3 Conference Streams** | **From over 40 countries**

Exhibition
April 30-May 1, 2019

Conference
April 29-May 1, 2019

Event powered by

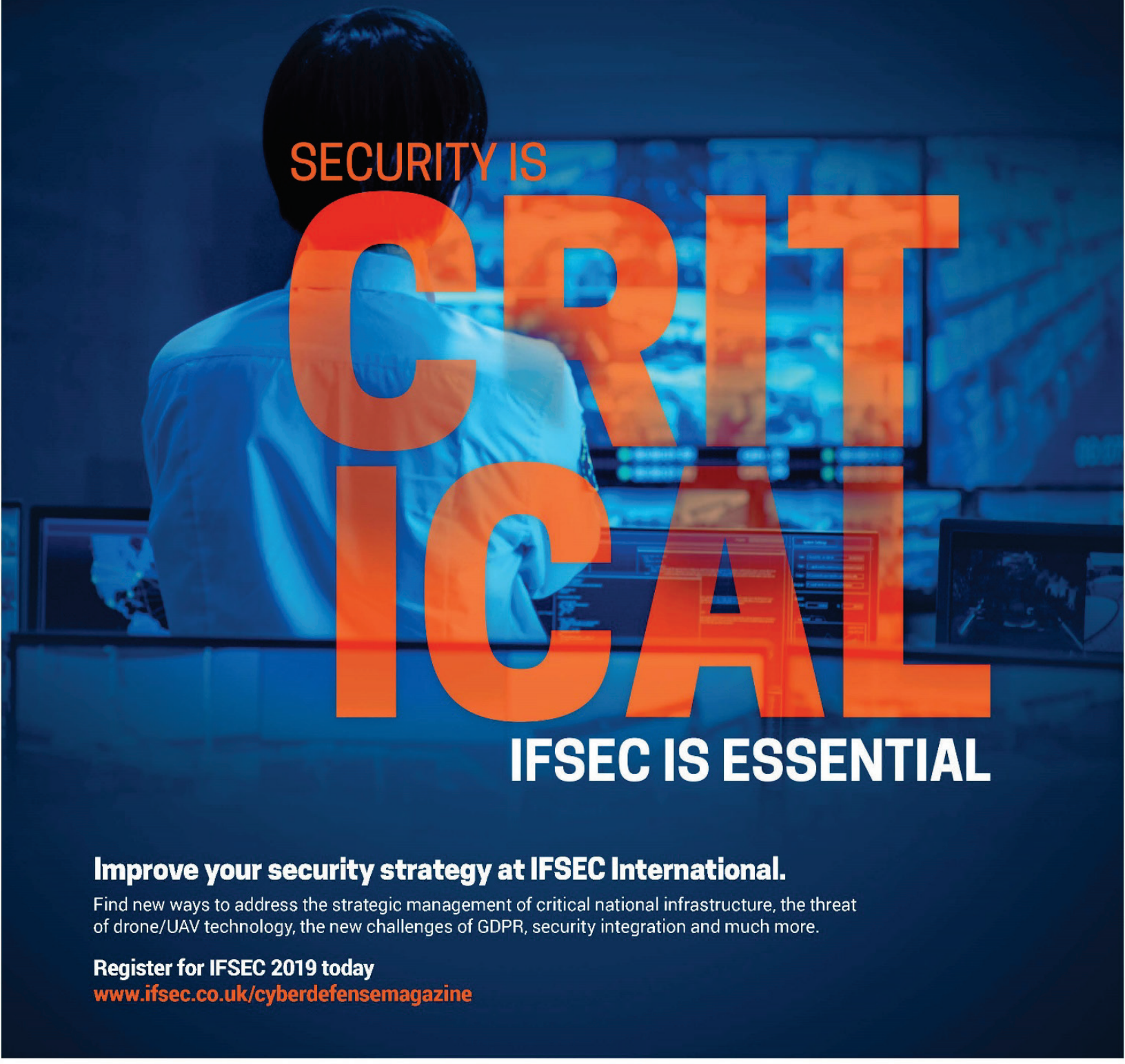
science media partners

IBIA International Biometrics+Identity Association

www.connectidexpo.com

IFSEC INTERNATIONAL

18-20 JUNE 2019
EXCEL LONDON UK



SECURITY IS

CRITICAL

IFSEC IS ESSENTIAL

Improve your security strategy at IFSEC International.

Find new ways to address the strategic management of critical national infrastructure, the threat of drone/UAV technology, the new challenges of GDPR, security integration and much more.

Register for IFSEC 2019 today
www.ifsec.co.uk/cyberdefensemagazine

Proudly in partnership with

ASIS INTERNATIONAL · bsia british security industry association · ECA · IPSA www.ipsa.org.uk · LPCB delivered by bre · NSI Security. Improved · SSAIB · THE SECURITY INSTITUTE

Organised by

UBM

CLOUD & CYBER SECURITY EXPO

12-13 March 2019 ExCeL, London
www.cloudsecurityexpo.com

Hear from over 200 expert speakers covering key topics and meet over 150 providers offering leading cloud and cyber security services and solutions at the UK's largest cloud and cyber security event.

Register for your free ticket today:
www.cloudsecurityexpo.com CyberDefenseMagazine1

SECURING DIGITAL TRANSFORMATION

Security is not just for the IT team: it now impacts everyone, and is an imperative consideration for the entire business. Join us on 12-13 March 2019 to gain knowledge and insight from industry leading security experts on emerging trends, tech deep dives, lessons learned and market forecasts.

Our 2019 speakers include:



JOHN MEAKIN
Group Chief Information Security Officer
GSK



CHI ONWURAH
Shadow Minister of Industrial Strategy, Science and Innovation
UK Parliament



JON TOWNSEND
CIO
National Trust



DAVID DEIGHTON
Chief Architect and CISO
University of Birmingham



EMERIC MISZTI
CISO
Motor Insurers Bureau



RAZVAN TUDOR
Chapter Lead
ING

For more information contact the team today on **+44 (0)207 013 4997**

CO-LOCATED WITH: CLOUD EXPO EUROPE · DEVOPS LIVE · SMART IOT · BIG DATA WORLD · AI TECH WORLD · BLOCKCHAIN TECH WORLD · DATA CENTRE WORLD

CloserStill

THE SUNDAY TIMES INTERNATIONAL TRACK 200 2017 HSBC · THE SUNDAY TIMES 100 BEST COMPANIES TO WORK FOR 2018 · FT 1000 Europe's Fastest Growing Companies

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



OFFICIALLY SUPPORTED BY

STRATEGIC PARTNERS

IOT PARTNER

PLATINUM SPONSOR

DIAMOND SPONSOR

GOLD SPONSORS

POWERED BY

CO-LOCATED WITH

ORGANISED BY

COMEX TECHNOLOGY SHOW 2019

17-19 MARCH 2019
OMAN CONVENTION & EXHIBITION CENTRE, MUSCAT
WWW.COMEX.OM

Strategic Partner
e.oman

DIGITALISING THE FUTURE

COMEX BUSINESS

TRENDING FEATURES

- AR/VR/MR
- 3D PRINTING
- SMART CITY
- CYBER SECURITY
- CLOUD DATA
- ROBOTICS
- INTERNET OF THINGS (IOT)
- ARTIFICIAL INTELLIGENCE (AI)
- MACHINE LEARNING
- BLOCKCHAIN TECHNOLOGY

KEY INDUSTRIES

- MANUFACTURING
- HEALTH CARE
- TOURISM
- RETAIL
- TRANSPORT & LOGISTICS
- EDUCATION
- OIL & GAS
- BANKING & FINANCE

Network with C-Level tech executives at **TECH EXECS VIP CLUB**

Pre-registered meetings at **COMEX MATCHMAKING ZONE**

Focus on 'Industry 4.0' at **SMART CITY CONFERENCE**

Knowledge-sharing seminars & demos at **TECH TALKS WORKSHOPS**

Smart Homes & Lifestyle Products, Gaming Hackathon & Cyber Warfare Zone at **COMEX LIFESTYLE**

Organiser
OITE
www.oite.com

BOOK YOUR SPACE TODAY!

Ahmed Farag
Sales Manager
+968 9411 3434
a.farag@oite.com

Malicia Lal
Sales Manager
+968 9551 7815
malicia@oite.com

Supporter: Omantel

Official Artificial Intelligence Sponsor: Microsoft

Lead Sponsor: FIREWARE KNOWLEDGE PROTECTED

Platinum Sponsor: National Centre for Statistics & Information, Sultanate of Oman

Association Partners: ASSUN MOTOR, WTIA, CCAOI

Digital Media Partner: Business Live ME

Media Partners: Conference Locate, SmartSMB, Carrier Community, thebusinessyear, Cyber Security Review, IndiaTechonline, Expo Rooms, Digital Forensics Magazine, Dossier, Security, APSM, EAITSM, CDM, Oxford Business Group, Haptic

4th CYBER INSURANCE SUMMIT 2019

26 - 29 MARCH 2019, HONG KONG

Leading Exchange of Strategic Insights on How to Better Understand, Underwrite and Price Cyber Risk in an Ever-Changing Cyber Insurance Market.

Key Highlights:

Proven Track Record of Quality: Equip Global' s highly distinguished Cyber Insurance Summit Series has set a proven track record of bringing together some of the best case studies in the Cyber Insurance field, as well as delivering highly targeted discussions to address current market trends and challenges. In this upcoming 4th Cyber Insurance Summit 2019, expect to hear from the best of the Asia's Cyber Insurance industry as they discuss and share on Devising a Strategic Framework to Overcome Challenges Brought about by an Absence of Standard Coverage Language.

Eye Opening Presentations From 16+ Industry Leaders: Hear from 16+ specially curated speakers from across the Asia and beyond, so as to exchange strategic insights on Bridging the Gaps in Incident Data and Advances in Modelling Capacity.

Recipe for Success: Hear from Asia's esteemed Cyber Insurance Leaders as they share Successful Case Studies on how you can Overcome Customer Segmentation & Underwriting Challenges Faced by Cyber Insurance Providers. Learn from only the Best Practices!

Specially Curated and In-depth Workshops: Looking to ELEVATE your summit experience to the next new level? Join us for our 5 highly targeted workshops that are specially curated to address the top challenges facing the Cyber Insurance industry in Asia, so as to accelerate your market infiltration efforts!





LEARN MORE:

PHONE + 65 6376.0908

EMAIL enquiry@equip-global.com

WEB www.equip-global.com

"The conference provided excellent ideas, speakers were extremely dedicated, this definitely exceeded my expectations!"

- Head of Underwriting, Chubb

Researched & Developed by:

EQUIP GLOBAL

RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

Follow your passion— all the way to RSAC 2019.

No matter what cybersecurity topics keep you on the edge of your seat, RSA Conference 2019, March 4 – 8, has the information you need to stay on top of the trends affecting your organization, including:

- Thought-provoking keynotes led by top experts, including:

  Emily Heath, Vice President and Chief Information Security Officer, United Airlines
  Ann Johnson, Corporate Vice President, Cybersecurity Solutions Group, Microsoft
  Dave Shackleford, Senior Instructor, SANS Institute
- Interactive demos from Arcon, Cyxtera, Xabyss and hundreds more
- Over 550 sessions and seminars that engage the issues that matter to you, including risk management, cloud protection and authenticated encryption

Register today to secure your spot at the Conference that's into everything you are. But hurry—savings are going fast.

Register now: **www.rsaconference.com/cyberdefense-us19**

Follow us: #RSAC

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.

PUBLIC SAFETY INDONESIA

GET YOUR FREE PASS NOW!

27 February - 1 March 2019
Jakarta Convention Center, Jakarta - Indonesia

Co-located with:

Police Leadership
FORUM & CONGRESS 2019

Hosted by:

INDONESIAN NATIONAL POLICE









Public Safety is Security: Strengthening Through Collaboration

Indonesia's Leading Conference & Trade Expo on Public Safety & Police Technology

Trade Visitors:
3,000+

Conference & Congress Delegates:
400

Exhibitors:
80+

Online registration: publicsafetyindonesia.com

Title Sponsor: alhua TECHNOLOGY

Platinum Sponsor: SAMSUNG

Silver Sponsor: HIKVISION

Supported By: APTIKNAS, ASIS, ASISINDO, BEA

Media Partners: 21AAR, airmagz, CDM, IndoSecuritySystem, iSAFETY, MAJALAHPROPERTI.COM, Malaysia SAFE, VENUE

Organised By: d-house CLARION

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

Atlanta, GA - Feb. 13
Denver, CO - Apr. 2
Philadelphia, PA - Apr. 25
Dallas, TX - May 16
Seattle, WA - Jun. 25
DC Metro, VA - Jul. 16
Chicago, IL - Aug. 27
Charlotte, NC - Sep. 25
New York, NY - Oct. 3
Scottsdale, AZ - Oct. 17
Boston, MA - Nov. 6
Houston, TX - Nov. 21
Los Angeles, CA - Dec. 5

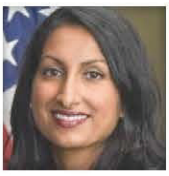
THOUGHT LEADERS HAVE INCLUDED



Sean Roche
Associate Deputy Director of Digital Innovation
The CIA



David Ostertag
Global Investigations, Investigative Response
Verizon



Sanchi Jayaram
Chief, Foreign Investment & Corp
U.S. DOJ, National Security Division



David Cass
Chief Information Security Officer
IBM



Mike Wilusz
Customer Engineer
Google

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 Them

THE DARK WEB
Dealing with a Universe Filled with Threats to Your Enterprise, Society and Beyond

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



معرض مدن المستقبل

FUTURE CITIES SHOW

8 - 10 April 2019

Dubai, United Arab Emirates

Propelling Globalization through Digital Transformation

Key Focus Areas

- Artificial Intelligence
- Blockchain
- Smart Mobility
- Smart Infrastructure
- Sustainability

REGISTER NOW

For early bird discounts

Future Cities Show is an exceptional platform to engage with inspiring experts from leading technological solutions brands and services and a perfect opportunity to network with industry leaders from smart cities, strategic government representatives and creative business influencers.

+971 4 39 23232 info@futurecitiesshow.com

www.futurecitiesshow.com

IoT ASIA | 27-28 March 2019

Hall 1, Singapore EXPO

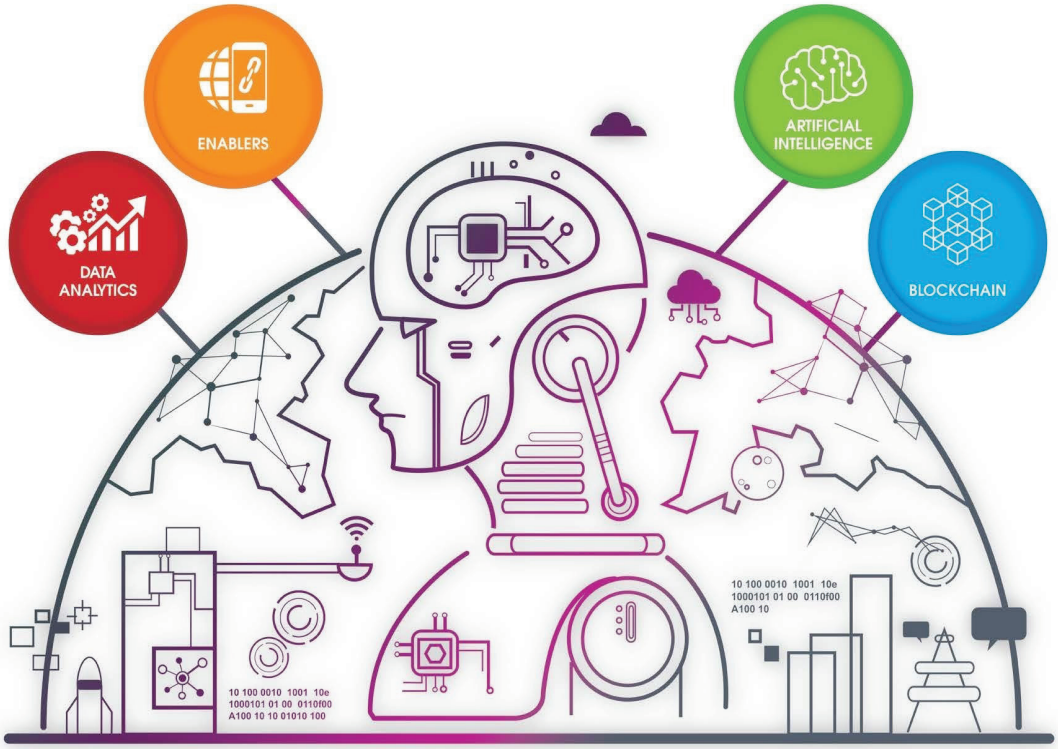
INTERNATIONAL EXHIBITION & CONFERENCE ON THE INTERNET OF THINGS

TRANSFORMING BUSINESSES, GOVERNMENT AND SOCIETIES

SHOWCASE your latest innovations and strengthen your business partnerships

BUILD Value Chains across the IoT Ecosystem

GAIN key insights from best practices and case studies from Industry Leaders



BUILDING VALUE CHAINS

SMART CITIES // INDUSTRIAL IoT

ENABLERS

ARTIFICIAL INTELLIGENCE

DATA ANALYTICS

BLOCKCHAIN

JOIN US AT THE 6TH EDITION OF IoT ASIA 2019

Interested to Exhibit or Sponsor? Contact us at sales.iotasia@singex.com

www.internetofthingsasia.com • #iotasia

Organised by

SiAA

SingEx

Industry Accolades

ufi Winner of the Marketing Award 2016

2015/16 #IoT Awards

Singapore Experience Awards 2015 Recipient

2014/15 Internet of Things Awards

COMEX TECHNOLOGY SHOW 2019

17-19 MARCH 2019
OMAN CONVENTION & EXHIBITION CENTRE, MUSCAT
WWW.COMEX.OM

Strategic Partner
e.oman

DIGITALISING THE FUTURE

COMEX BUSINESS

TRENDING FEATURES

- AR/VR/MR
- 3D PRINTING
- SMART CITY
- CYBER SECURITY
- CLOUD DATA
- ROBOTICS
- INTERNET OF THINGS (IOT)
- ARTIFICIAL INTELLIGENCE (AI)
- MACHINE LEARNING
- BLOCKCHAIN TECHNOLOGY

KEY INDUSTRIES

- MANUFACTURING
- HEALTH CARE
- TOURISM
- RETAIL
- TRANSPORT & LOGISTICS
- EDUCATION
- OIL & GAS
- BANKING & FINANCE

Network with C-Level tech executives at **TECH EXECS VIP CLUB**

Pre-registered meetings at **COMEX MATCHMAKING ZONE**

Focus on 'Industry 4.0' at **SMART CITY CONFERENCE**

Knowledge-sharing seminars & demos at **TECH TALKS WORKSHOPS**

Smart Homes & Lifestyle Products, Gaming Hackathon & Cyber Warfare Zone at **COMEX LIFESTYLE**

Organiser
OITE
www.oite.com

BOOK YOUR SPACE TODAY!

Ahmed Farag
Sales Manager
+968 9411 3434
a.farag@oite.com

Malicia Lal
Sales Manager
+968 9551 7815
malicia@oite.com

Supporter
Omantel

Official Artificial Intelligence Sponsor
Microsoft

Lead Sponsor
FIREWARE
KNOWLEDGE PROTECTED

Platinum Sponsor
NATIONAL CENTRE FOR STATISTICS & INFORMATION
Enhancing Knowledge
SULTANATE OF OMAN

Association Partners
ASSUN MOTOR
WTIA
CCAOI™
Representing the ecosystem of Internet -Bharat Model

Digital Media Partner
Business Live ME

Media Partners
Conference locate.com
SmartSMB
Carrier Community
thebusinessyear
Cyber Security Review
IndiaTechonline
EXPO ROOMS
DIGITAL FORENSICS
Dossier
SECURITY
APSM
EA ITSM
CDM
OXFORD BUSINESS GROUP
HAPTIC

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

It's time to change the way you transfer files.

Manual scripts and free SFTP tools are convenient and budget-friendly, at least until something fails and causes a breach. Then, they're a nightmare.

With security vulnerabilities on the rise, it's time to find a new method for exchanging files with trading partners.

GO ANYWHERE®
Managed File Transfer

GoAnywhere MFT simplifies data exchange while limiting the risks of using homegrown tools and software. With GoAnywhere, you can:

- Automate your transfers with conditional, multi-step workflows.
- Connect to a variety of internal and external file servers.
- Establish, maintain, and generate reports for regulatory compliance.
- Collaborate with teams through a browser-based web client.

Visit info.goanywhere.com/mft to learn how you can streamline AND secure your file transfers once and for all.



helpsystems

ACI
Active Communications International

The 3rd Next Generation Cyber Security for Utilities

Staying a Step Ahead of Increasingly-Sophisticated Cyber Threats

February 13 - 14, 2019
Denver, CO



FEATURING AN EXCLUSIVE TOUR OF
TRI-STATE GENERATION & TRANSMISSION
FEBRUARY 12, 2019

INTRODUCTION

With the value of damages caused by cyber-attacks growing rapidly every year, adopting a new and comprehensive approach to cyber security is more important than ever. Among essential facilities that feel this pressure, few feel it more than our utilities. Cyber incidents have the potential to bring regional economic growth to a grinding halt, especially when they target the lifeblood of our modern civilizations. With threats becoming more sophisticated and gaining better resources, security professionals must continue to adapt and develop their methods of defence and response to ensure the uninterrupted production of our power.

SPECIAL DISCOUNT FOR SUBSCRIBERS

As a supporting partner to 3rd Next Generation Cyber Security for Utilities, ACI are offering Cyber Defense Magazine subscribers a 15% discount on delegate registration until 31st January 2019.

To claim please contact Cheryl Williams on
+44 203 141 0623 • cwilliams@acieu.net

QUOTE DISCOUNT CODE: CYu3MKT

SPONSORS INCLUDE

BURNS McDONNELL

For commercial and sponsorship opportunities please contact Kristina Gyulavári on
+1 929 331 6835 • kvari@acieu.net

BAPCO

The Annual Event 2019

TCCA Critical Communications Europe 2019

12 - 13 MARCH 2019
RICOH ARENA, COVENTRY

TWO EVENTS ONE LOCATION

REGISTER NOW

WWW.BAPCO-SHOW.CO.UK/REGISTER

Reasons to Attend

Bringing together the BAPCO and TCCA events creates an unrivalled opportunity for all those involved in the sector to come together in the UK to network, learn and discuss everything to do with critical communications and public safety solutions.

THE 2019 EVENT IS THE MUST-ATTEND ANNUAL EVENT FOR THOSE INVOLVED IN PUBLIC SAFETY COMMUNICATIONS AND WILL ENABLE THEM TO:

- Network with the communication industry's biggest suppliers
- Compare and source new comms methods, products and services
- Receive free expert advice on the implementation and management of equipment and technologies
- Attend best-practice workshops and pose questions to the experts at the industry's forefront
- Learn how to increase service efficiency and reduce costs
- Do business, make new contacts, and place orders face-to-face

New for 2019

DRONE ZONE



SHOWCASE THEATRE



Our Sponsors

PLATINUM SPONSOR

MOTOROLA SOLUTIONS

GOLD SPONSORS

APD

FREQUENTIS

SILVER SPONSORS

tait communications

3tc SOFTWARE THAT EMPOWERS

@BAPCOEVENT
@CRITCOMMSSERIES

BAPCO ANNUAL CONFERENCE AND EXHIBITION
TCCA CRITICAL COMMUNICATIONS SERIES

WWW.BAPCO-SHOW.CO.UK
WWW.CRITICAL-COMMUNICATIONS-WORLD.COM

automotivecybersecurity.iqpc.com

AUTOMOTIVE CYBERSECURITY

DETROIT

March 27-29 2019

The 9th Automotive Cybersecurity Detroit is a one of a kind networking experience that brings top cyber security experts together with leaders in the automotive industry to discuss challenges in the near and not too distant future.

We will feature key influencers and decision makers from OEMs, Tier 1's, Disruptors, and other external transport industries as we navigate the most critical opportunities and challenges for vehicle cyber security: ECU security, over the air updates (OTAs), V2V/V2I communications, securing embedded systems, and much more!

Attendees Include:

CATERPILLAR

intel

nexteer AUTOMOTIVE

Visteon

LEAR Where Passion Drives Possibilities

MAGNETI MARELLI

APTIV

DELPHI

DURA Automotive Systems

MITSUBISHI MOTORS

veoneer

To learn more, contact Nuria.Frances@iqpc.com or 212-885-2694



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

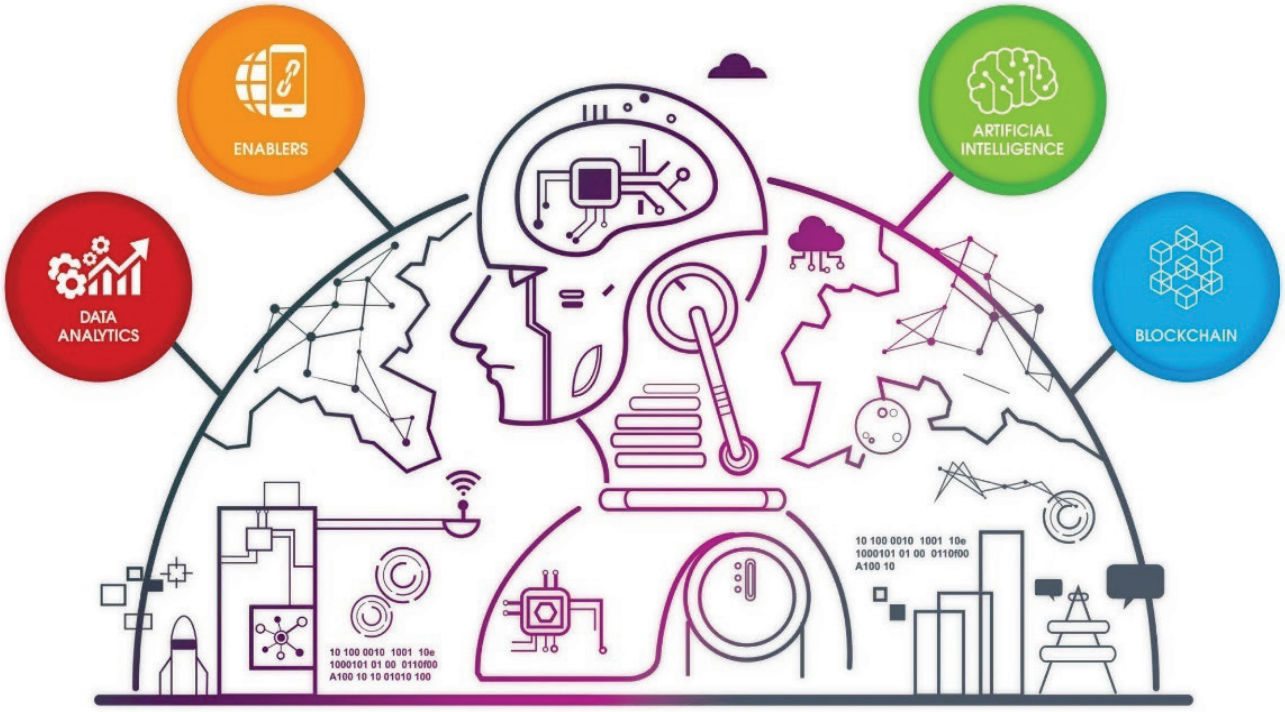
CYBERINVESTINGSUMMIT.COM

IoT ASIA | 27–28 March 2019

Hall 1, Singapore EXPO

INTERNATIONAL EXHIBITION & CONFERENCE ON THE INTERNET OF THINGS

TRANSFORMING BUSINESSES, GOVERNMENT AND SOCIETIES



BUILDING VALUE CHAINS

SMART CITIES // INDUSTRIAL IoT

Artificial Intelligence Blockchain Data Analytics Enablers Data Analytics Blockchain

Enablers Artificial Intelligence Data Analytics Blockchain Artificial Intelligence Data Analytics

ENABLERS Artificial Intelligence Data Analytics Blockchain Data Analytics Blockchain Artificial Intelligence Data Analytics Blockchain Artificial Intelligence Data Analytics Enablers Blockchain Data Analytics Artificial Intelligence Data Analytics Enablers **ARTIFICIAL INTELLIGENCE**

DATA ANALYTICS Data Analytics Blockchain Artificial Intelligence Blockchain Artificial Intelligence Data Analytics Enablers Artificial Intelligence Data Analytics Blockchain Data Analytics Blockchain Artificial Intelligence Data Analytics Enablers Data Analytics **BLOCKCHAIN**

Gain key insights from best practices and case studies from Industry Leaders.

REGISTER NOW!

www.internetofthingsasia.com • #iotasia

Organised by

SiAA SingEx

Industry Accolades

ufi Winner of the Marketing Award 2016

2015/16 #IoT Awards

SINGAPORE EXPERIENCE AWARDS 2015 RECIPIENT

2014/15 Internet of Things AWARDS

RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

Follow your passion—all the way to RSAC 2019.

What makes you tick? Multifactor authentication? Blockchain? No matter what speaks to you, RSA Conference 2019, March 4 – 8, has what you need to stay on top of the topics affecting your organization—and the industry at large.

- Interactive demos from Splunk, Red Canary, Oracle and hundreds more exhibitors
- Hands-on tutorials, trainings and on-point conversations you won't find anywhere else
- Sharp and relevant keynotes from expert speakers such as **Emily Heath**, VP & CISO, United Airlines; **Stuart McClure**, Chairman & Chief Executive Officer, Cylance Inc.; **Bruce Schneier**, Chief Technology Officer, IBM Resilient, IBM Security | Fellow, Harvard Kennedy School; and our closing speaker, actress, writer and producer, **Tina Fey**.
- Over 550 sessions and seminars that address the issues that matter to you

It doesn't get more up your alley than that. Register today to secure your spot at the Conference that's into everything you are. But hurry—Passes and savings will go fast.

Register now: **www.rsaconference.com/cyberdefense-us19**

Follow us: **#RSAC**

Official Partner

NECTEC
a member of NSTDA

CYBER INTELLIGENCE ASIA

NOVOTEL SIAM SQUARE HOTEL | BANGKOK, THAILAND
27 TH – 28 TH FEBRUARY 2019

Esteemed Speaker Line-up:

Allan Cabanlong, Assistant Secretary, Cyber Security and Enabling Technologies, **Department of Information and Communications Technology (DICT), Philippines**

Wasawat Chawalitthamrong, Head of Crime Relating to Submission of Bids to Government Agencies, **Department of Special Investigations, Thailand**

Chalee Vorakulpipat, Head of Cybersecurity Laboratory, **National Electronics and Computer Technology Center (NECTEC), Thailand**

Fazlan Abdullah, Head, Government Engagement, **CyberSecurity Malaysia**

Budi Rahardjo, President, **Indonesia Computer Emergency Response Team (ID- CERT)**

Dr. Haji Mingu bin Haji Jumaan, Director, **Sabah State Computer Services Department, Malaysia**

Rana Shahzad, Forensics Expert, Cybercrime Division, **Federal Investigation Agency, Pakistan**

Martijn van der Heide, Specialist, **Thailand Computer Emergency Response Team (ThaiCERT)**

Kitisak Jirawannakool, Information Security Specialist, **Thai Bankers Association**

Virag Thakker, Senior IT Compliance Officer, **Agoda**

SPONSORSHIP OPPORTUNITIES AVAILABLE!

To book a stand in our exhibitor hall please contact us at events@intelligence-sec.com or +44 (0)1582 346 706

Sponsors & Exhibitors

Resecurity®

For more information visit – www.intelligence-sec.com

Book your place by:
w: www.intelligence-sec.com I e: events@intelligence-sec.com I t: +44(0)1582 346706

INTELLIGENCE-SEC

COMEX
TECHNOLOGY
SHOW 2019



CYBERTECH

THE EVENT FOR THE CYBER INDUSTRY

28-30.1.2019

TEL AVIV



CYBER.

WE LIVE IT. BREATHE IT.

Cybertech Worldwide. Creating Business Opportunities Across Borders.

SAVE THE DATE FOR CYBERTECH TEL AVIV 2019!

Join us on **January 28-30, 2019**, at the Tel Aviv Convention Center for the **BIGGEST CYBER EVENT** of the year!

>> **15,000** Attendees >> **170** Speakers
>> **210** Companies >> **90** Start-Ups
>> **160** Delegations from over **70** countries

Come LEARN, NETWORK, and MAKE BUSINESS with the cyber industry's most prominent players.

Top executives. Government officials. THOUSANDS of great business networking opportunities. All at the forefront of global innovation!

Register today at http://cybertechisrael.com | For more information, please contact cyber@cyberconference.com.

YALE CYBER LEADERSHIP FORUM

THE LAW, TECHNOLOGY, AND BUSINESS OF CYBER SECURITY

February 28–March 2, 2019 • Yale University • New Haven, Connecticut

Learn effective approaches to recognizing, preparing for, preventing, and responding to cyber threats.



"The experience gained from attending the Forum was indispensable and highly effective in understanding and mitigating the overall and ever-emerging cyber security threat landscape!"

— Randall S., Cyber Threat Intelligence Liaison Officer, U.S. Department of Energy

Scholarships and discounts are available for a limited time.
Apply by January 25 to qualify.

WEB *cyber.forum.yale.edu* **EMAIL** *cyber.forum@yale.edu*

DATA PROTECTION WORLD FORUM
PRIVACY | TRUST | RISK | SECURITY

CDM
CYBER DEFENSE MAGAZINE

Rowena Fell
Global and EMEIA Risk Assurance Operations Leader - Ernst & Young

Flavius Plesu
Head of Information Security Bank of Ireland UK

Steve Wright
Data Privacy and Information Security Officer - John Lewis

Marloes Pomp
Head of Blockchain Projects Dutch Government



SEE THESE SPEAKERS FOR FREE

Use our code 'CYBERMAGFREE'



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

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

CYBER DEFENSE TV

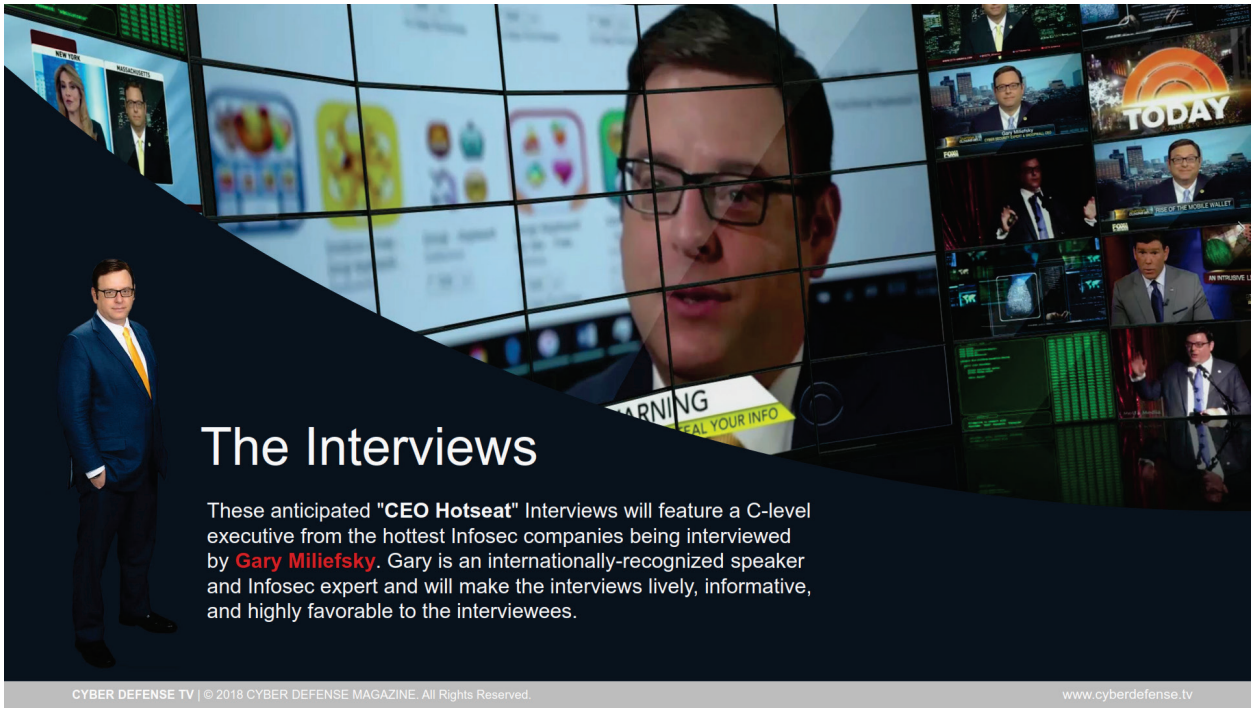
INFOSEC KNOWLEDGE IS POWER

We've launched http://www.CyberDefenseTV.com and http://www.CyberDefenseRadio.com

Over 40 amazing interviews and growing each year. Watch. Listen. Learn.

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

A new division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

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.



Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Marketing and Partnership Opportunities

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



Copyright (C) 2019, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) PO Box 8224, Nashua, NH 03060-8224. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. marketing@cyberdefensemagazine.com Cyber Defense Published by Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC. Cyber Defense Magazine, CDM, Cyber Defense eMagazine, Cyber Defense Test Labs and CDTL are Registered Trademarks of STEVEN G. SAMUELS LLC. All rights reserved worldwide. Copyright © 2019, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them.

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

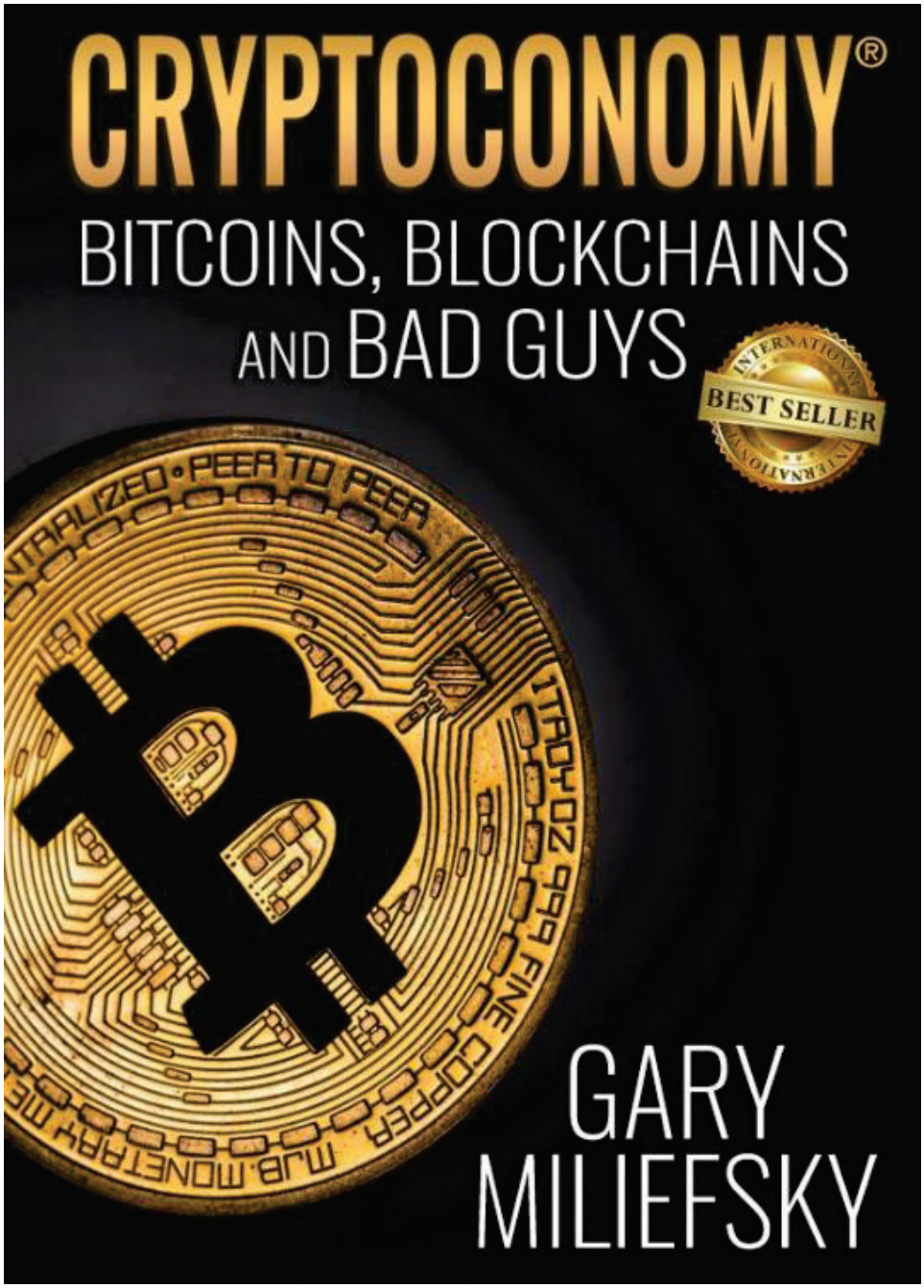
Cyber Defense Magazine

PO Box 8224, Nashua, NH 03060-8224.
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)
Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 03/01/2019

TRILLIONS ARE AT STAKE

No 1 INTERNATIONAL BESTSELLER IN FOUR CATEGORIES



Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



Regent University's Institute for Cybersecurity is disrupting and transforming the Cyber Defense industry with a state-of-the-art training platform and world-class trainers. To learn more about commercial training offerings, visit regent.edu/cyber or contact the institute at 757.352.4215.

Learn more about this program: https://www.regent.edu/institutes/cybersecurity/industry-training/

Space is limited, so register today: https://regent.emf360.com/explore/search



Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

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