

# CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

## INSIDE THIS EDITION:

From HUMINT to Virtual HUMINT

Security - Being Proactive vs. Reactive

The Challenges of Endpoint Security

The Purpose of Neural Networks in  
Cryptography

What's next for Cybersecurity?

Five Steps to Least Privilege Success

Cybersecurity as a Priority in 2019

Phishing in the Dark: Employee Security  
Gaps Are Growing

*.....and much more!*



**FEBRUARY 2019**

***MORE INSIDE!***

# CONTENTS

Security - Being Proactive vs. Reactive .....	19
Using PAM for Cyber Forensics & Security Breach Remediation—Key to a Safer 2019	22
Cyber Attacks: The Biggest Threat for Future Weapons .....	25
Cybersecurity in New York City, the Financial Capital of the United States .....	30
Best Practices for Balancing BYOD with Mobile Security.....	32
How to Combat a Terrorist Attack Using Modern Communications .....	35
The Challenges of Endpoint Security.....	38
The Purpose of Neural Networks in Cryptography .....	41
Overcoming the Cybersecurity Staffing Drought .....	44
From HUMINT to Virtual HUMINT .....	49
What’s next for Cybersecurity?.....	53
Operational Excellence: The Key to Federal Agencies’ Compliance.....	56
Five Strategies to Optimize Cloud Security in 2019 .....	58
Five Steps to Least Privilege Success.....	62
Top 10 Business Requirements for an Enterprise Cyber Threat Hunting Solution .....	65
Cybersecurity as a Priority in 2019.....	67
10 Considerations When Bringing in IT Outsourcing Contractors versus Working with a Managed Services Provider.....	71

# CONTENTS (cont')

<b>The US Must Catch Up to Other Prominent Powers in Cyberwarfare Defense .....</b>	<b>74</b>
<b>Operation Eligible Receiver 97's Impact on Ransomware .....</b>	<b>77</b>
<b>9 Ways to Safeguard Privileged User Accounts and Protect Your Business.....</b>	<b>87</b>
<b>Open-Source Code .....</b>	<b>91</b>
<b>Overcoming Software Security Issues Caused by the Third-Party Software Procurement Model .....</b>	<b>93</b>
<b>Phishing in the Dark: Employee Security Gaps Are Growing .....</b>	<b>97</b>
<b>Mid-Market Businesses, Don't Think Small about Security .....</b>	<b>100</b>



**@MILIEFSKY**

From the

# Publisher...



**[CyberDefenseTV.com](http://CyberDefenseTV.com) and [CyberDefenseRadio.com](http://CyberDefenseRadio.com) are up. Please check them out!**

Dear Friends,

***It's February already and time is flying by, with RSA Conference 2019 right around the corner March 4-9, 2019 in San Francisco, CA, USA and it will be our 7<sup>th</sup> year in attendance as a Media Partner.***

As promised, by the end of the first quarter of 2019, we 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 7<sup>th</sup> year in 2019 with over 7,000 original pages of searchable InfoSec content.

While there are new 'copycat' brands out there on the market, you'll find they have very little original content and we hope to continue to keep our pace, so you'll independently see the incredible difference, in our value proposition. We also offer our own statistics that you are free to reuse anytime, from this page: <http://www.cyberdefensemagazine.com/quotables/>. We believe in sharing information and helping educate others with as much open source intelligence (OSINT) and unique, daily updated content as possible. One of my new competitors has absolutely inspired me. He and his team are the hare and we are the tortoise, slow and steady we will continue to prove ourselves to be the best source for infosec content and with more exciting platforms coming out this year. 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



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

## From the Editor...

We've been tracking new forms of exploitation – whether it's backdoors in the internet of things and personal computing supply chain, or advanced covert data exfiltration from new Remote Access Trojans (RATs) or points of presence (PoPs) in North America with traffic re-routing to China, it appears that the Chinese government has decided to scale and multiply their exploitation methods to collect all the data they possibly can on the United States and its citizens. We'll continue to watch and report on this trend as it evolves as it appears to be the most dramatic nation state cyber espionage activity for 2019.

Please Enjoy This February Edition of CDM!  
**To our faithful readers,**  
Pierluigi Paganini



**@CYBERDEFENSEMAG**

### CYBER DEFENSE eMAGAZINE

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

#### PRESIDENT & CO-FOUNDER

Stevin Miliefsky  
[stevinv@cyberdefensemagazine.com](mailto:stevinv@cyberdefensemagazine.com)

#### EDITOR-IN-CHIEF & CO-FOUNDER

Pierluigi Paganini, CEH  
[Pierluigi.paganini@cyberdefensemagazine.com](mailto:Pierluigi.paganini@cyberdefensemagazine.com)

#### ADVERTISING

Marketing Team  
[marketing@cyberdefensemagazine.com](mailto: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](http://CYBERDEFENSEMEDIAGROUP.COM)

[MAGAZINE](#)

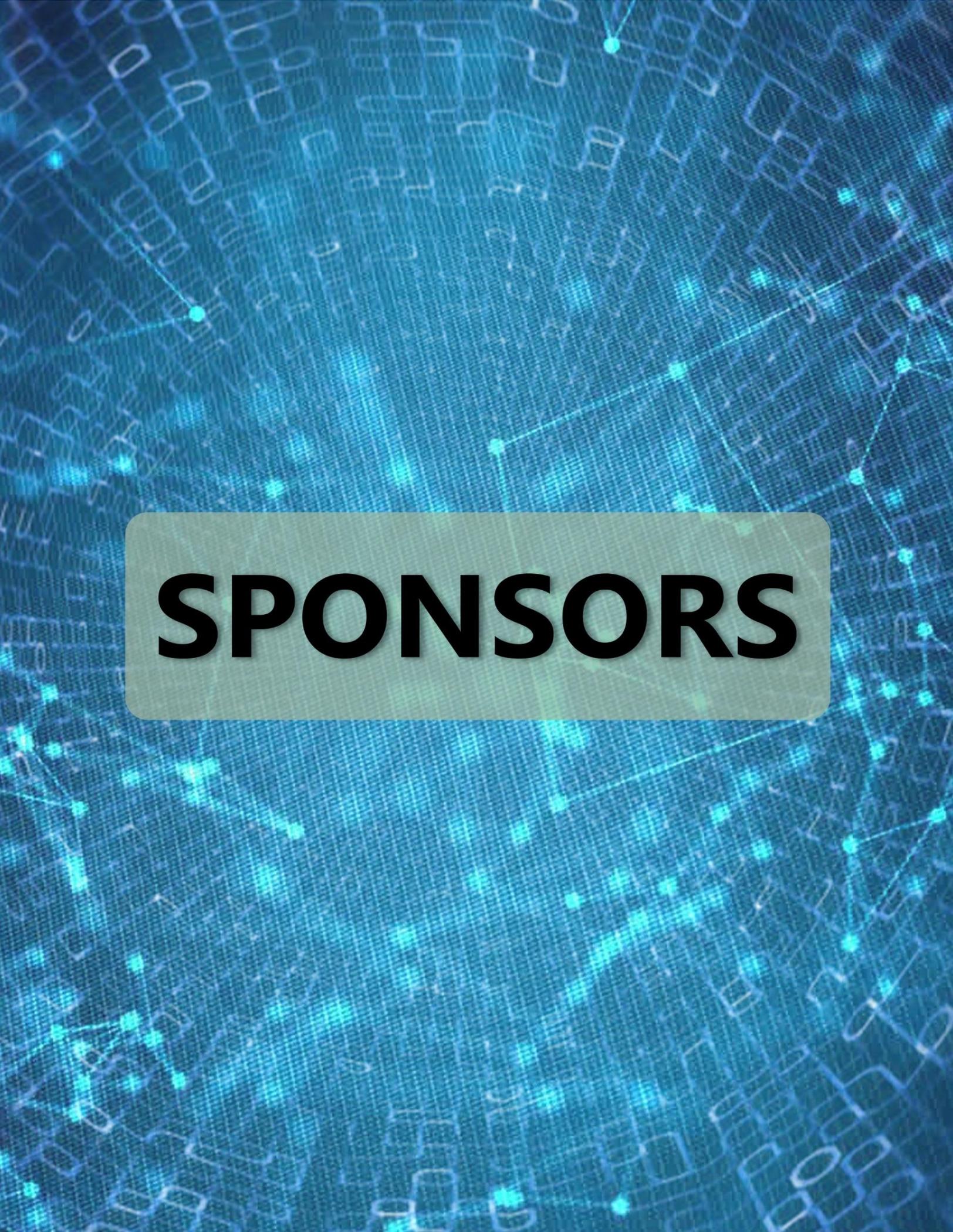
[TV](#)

[AWARDS](#)

SEE US IN MARCH 2019 AT...

RSAConference2019  
Moscone Center | San Francisco  
March 4 - 8, 2019





**SPONSORS**

# InfoSec Knowledge is Power Free Cybersecurity Resources



[www.cyberdefense.tv](http://www.cyberdefense.tv)  
[www.cyberdefensemagazine.com](http://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.**



**Vaporstream**

Visit us at [www.Vaporstream.com/security](http://www.Vaporstream.com/security).

# New Year, New You, New File Transfer Solution

# 2019



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

You might benefit from MFT if:

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

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

Try GoAnywhere today!  
Download a free 30-day trial of our  
award-winning MFT solution at  
[www.goanywhere.com/trial](http://www.goanywhere.com/trial)



**GO ANYWHERE<sup>®</sup>**  
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**<sup>®</sup>  
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:



Simplify Your Processes and More with Secure Cloud Integrations  
Request a Demo: [www.goanywhere.com/demo](http://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**

# Array of tools for Endpoint Security and Systems Management



## One Platform

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

# 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



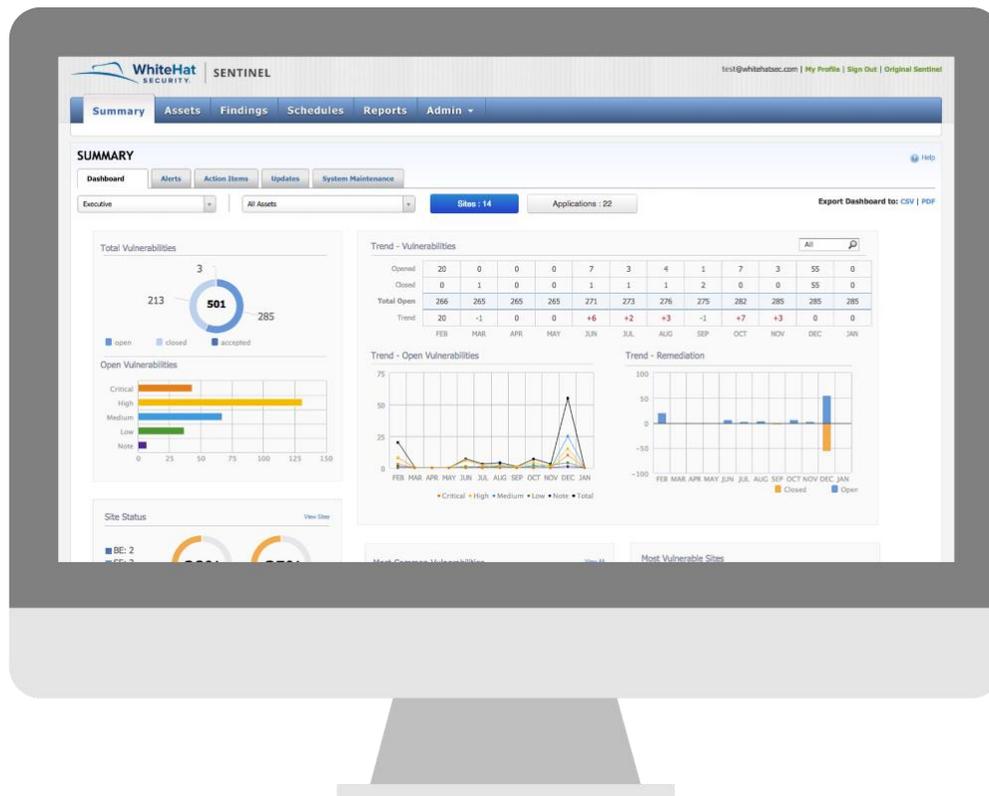
Monitoring of risky &  
unsanctioned activity.

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.



**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](https://www.whitehatsec.com/info/security-check/) to sign up at this URL: <https://www.whitehatsec.com/info/security-check/>

**PLEASE NOTE: Trial participation is subject to qualification.**

# 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.

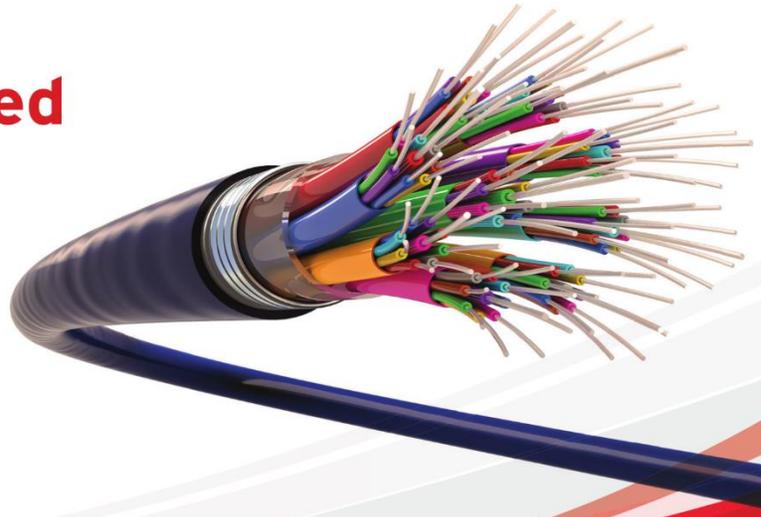
Visit [info.goanywhere.com/use-cases-for-mft](http://info.goanywhere.com/use-cases-for-mft) to get the free guide sent right to your inbox.



**GO ANYWHERE®**  
Managed File Transfer



# 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.



## 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



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

[www.trendmicro.co.uk/xgen-cyber](http://www.trendmicro.co.uk/xgen-cyber)

# Hacking Experts

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

TRAINING

SERVICES

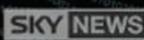


HACKER HOUSE™

AS SEEN IN

Forbes

Bloomberg



## 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



## Security - Being Proactive vs. Reactive

*by Amit Ashbel, Security Evangelist at Cognigo*

In today's IT market, no other sector is currently as large or relevant as cybersecurity. From endpoint security and network protection to anti-fraud and malware, there are many critical issues that organizations need to keep top of mind. And while new vendors are emerging to provide new solutions, the reality is that cyberattacks are growing increasingly more powerful and sophisticated each day.

This quote from Verizon's 2019 Data Breach Investigations report is quite telling: "This year we saw, yet again, that cybercriminals are still finding success with the same tried and tested techniques, and their victims are still making the same mistakes."

It probably makes sense for the industry to think of a new approach instead of falling victim to the same attacks.

And make no mistake -- these attacks will keep occurring as long as cybercriminals are making money. As with most crimes, the end goal of most cybercrime is cash – but in order to get there, hackers first need to get access to personal user data.

## Data is the new currency

According to Verizon's report, there were over 2,200 breaches reported in 2019. That averages out to about six per day, meaning a data breach is taking place approximately once every four hours.

For any company that utilizes personal customer data (i.e. all of them), it is up to management to adequately prepare for a breach, making sure that all steps have been taken to identify their data silos and continuously protect that data.

The report also notes that "the time it takes cybercriminals to compromise a system is often just a matter of minutes – or even seconds. They don't need much time to extract valuable data – they usually have much more than they need as it typically takes organizations weeks or months to discover a breach."

Diving deeper into this point, most businesses have vast amounts of unknown data that they've collected over the years and stored in various isolated silos. This "dark" data can make up as much as 80% of an organization's total database and, according to Forrester, 62% of companies don't even know where it is located.

A few years back, hackers were able to break into Yahoo's database and access hundreds of millions of accounts. The company said that its information was encrypted using the hashing algorithm MD5, which is not a secure form of protection. Even the most basic penetration testing service would identify MD5 as insecure and call for stronger encryption.

Yahoo probably would have been able to better encrypt their data if they'd had full visibility into where it was and how it was being stored.

With new privacy regulations like the General Data Protection Regulation now in effect and California's Consumer Privacy Act soon to be made law, organizations can no longer afford to not know where their data is stored. All personally identifiable information needs to be properly maintained and protected regardless of its usage.

If your company has been breached, your first question shouldn't be "How did this happen?" The more urgent question to answer is "What data was affected?" It's no longer an option to claim you were "unaware."

## What actions must be taken?

Back in 2014-15, CISOs faced similar visibility challenges when it came to their IT infrastructure, including their cloud computing and IoT networks. The cyber industry was quick to act, coming up with a host of new solutions such as endpoint detection and response (EDR) and cloud access security brokers (CASB). These technologies gave security teams the power to be proactive in their risk management strategy.

Unfortunately, it looks like data security is still a few steps behind cybersecurity. It will require a large amount of effort and resources if companies hope to ever catch up.

Only by being proactive will organizations have a chance of defeating the bad guys and protecting their data and their customer data. One promising technology is artificial intelligence (AI), which has proven very effective in automating the process of risk mitigation and ensuring that security teams are not left scrambling when they uncover a data vulnerability.

### About the Author



Amit Ashbel is the Security Evangelist at Cognigo. Amit has been with the security community for two decades and has taken on multiple tasks and responsibilities, including technical positions and senior product lead positions. Amit has experience with a wide range of security solutions, including network, endpoint, fraud detection, and application security. Amit's familiarity with emerging threats, allows him to address multiple aspects of an organization's security portfolio while constantly studying how organizations can adapt to the ever-changing landscape. Amit is a well-known speaker at high-profile conferences such as Black Hat, Defcon, Info Security Europe, IDC, OWASP AppSec, and more. Amit can be reached at [amit@cognigo.com](mailto:amit@cognigo.com). Come see how Cognigo can help you manage your data at [Cognigo.com](http://Cognigo.com)



## Using PAM for Cyber Forensics & Security Breach Remediation—Key to a Safer 2019

*Author: Morey Haber, CTO, BeyondTrust*

No one wants to *respond* to a security incident or a breach, particularly at the start of a new year! Instead the highest priority should be to stop a cyber threat *before* it compromises the organization. But in reality, preventing a cyberattack from landing is not always possible. The steps for incident or breach identification—from threat hunting to searching for explicit Indicators of Compromise (IoC)—are well established. While the processes will vary from organization to organization, malware, compromised accounts, lateral movement, etc. will all need to be addressed as a part of any formal clean-up plan.

If a breach is severe enough (for example, including the compromise of domain controllers), organizations may have no choice other than to reinstall the entire environment from scratch. While that is a worst-case scenario, it does happen. In many cases, businesses may choose to scrub servers as best as possible versus performing a complete reinstall. That is a business decision based on risk, feasibility, and cost. It also represents a no-win scenario if the threat is a persistent presence that uses techniques to evade traditional identification measures. If you think that is far-fetched, just look at the history of threats like rootkits, Spectra, and Meltdown that prove that there is always a way to attack a technology resource.

### Threat actors are after your credentials

Regardless of your remediation strategy, you can be assured that, via some fashion or another, threat actors will have access to your credentials. This implies that any clean-up effort should not reuse any existing passwords or keys. If possible, you should change (rotate) all credentials across every affected or linked resource. This is where Privileged Access Management (PAM) comes into play. The clean-up or redeployment needs to be protected from password reuse or from a threat actor regaining a persistent presence due to poor credential management, as remediation efforts begin.

Password management is a core aspect of PAM, and includes the automatic onboarding, rotation, session management, reporting, and check-in and check-out of passwords from a password safe. While PAM technology is most prominently used for privileged passwords like administrator, root, service accounts, and DevOps secrets, it can also be used as a least privilege solution to remove administrative rights for applications and tasks. This means that end users would no longer have, or need, a secondary administrator account to perform business functions.

### **PAM's role in clean-up after a breach**

With this mind, how does PAM help with security breach clean-up? During a security incident or breach, you first need to investigate and address the following:

- Determine which accounts were compromised and used for access and lateral movement.
- Determine the presence and resources using any linked, compromised accounts. For example, the same account that was compromised on asset X or application Y is also used on assets A, B and C for applications D, E and F so they can all communicate.
- Identify and purge any illicit or rogue accounts created by the threat actor.
- Identify, and remove or segment, any shadow IT, IoT, or other resource that was part of the cyberattack chain, to protect against future threats.
- Analyze the accounts that have been compromised and determine the least amount of privileges needed for them to perform their functions. Most users and system accounts do not require full domain or local administrator or root accounts.
- Analyze how data was used/accessed by the attacker during the breach. Was any IoC data captured during abuse of the privileged account? If data was captured, did it help identify the threat? If data was not captured, determine what needs to change to monitor future misuse of privileged accounts. This includes privileged account usage as well as session monitoring and keystroke logging, where appropriate.

This analysis is not trivial. Tools are needed to discover accounts, identify resources, determine usage patterns, and, most importantly, flag any potential abuse. Even if all the log data is sent to a security information and event management (SIEM), it still requires correlation or user behavior analytics to answer these questions.

Once you have made the initial investigation, here are the five ways PAM can help after a breach and should be considered an essential component of your clean-up efforts:

1. After a discovery, automatically onboard your privileged accounts and enforce unique and complex passwords with automatic rotation for each. This will help ensure any persistent presence cannot repeatedly leverage compromised accounts.
2. For any linked accounts, have your PAM solution link and rotate them all together on a periodic schedule; including for service accounts. This will keep the accounts synchronized and potentially isolated from other forms of password reuse.

3. When applicable, remove unnecessary privileged accounts all the way down to the desktop. This includes any secondary administrator accounts associated with an identity. For any application, command, or task that requires administrative rights, consider a least privilege model that elevates the application—not the user—to perform privileged management.
4. Using PAM, look for IoCs that suggest lateral movement, either from commands or rogue user behavior. This is a critical portion of the cyberattack chain where PAM can help identify whether or not any resources have been compromised.
5. Application control is one of the best defenses against malware. This capability includes looking for trusted applications that are vulnerable to threats by leveraging various forms of reputation-based services. PAM can help here too. Decide on an application's runtime based on trust and known risks before it is allowed to interact with the user, data, network, and operating system.

Privileged access management should not only be considered for new projects and legacy systems to stop privileged attack vectors. It should be considered for forensics and remediation control after an incident or breach. PAM will help stop a threat actor from acting on some of the lowest hanging fruit within your organization—poor password and credential management.

As a security best practice, privileged access should always be limited. When a threat actor gains administrator or root credentials, they do have the keys to your kingdom. The goal is stop them from obtaining them and “rekeying” the accounts via passwords on a frequent basis, so even if they steal a password, their usage can be limited and monitored for potential abuse. Therefore, after an incident or breach, this helps ensure that any lingering persistent presence can be mitigated and represents a valuable methodology in the clean-up and sustainment process.

#### About the Author



With more than 20 years of IT industry experience and author of *Privileged Attack Vectors*, Mr. Haber joined Beyond Trust 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.



# Cyber Attacks: The Biggest Threat for Future Weapons

*Are cyber-attacks become more efficient than kinetic ones?*

*by Julien Chesaux, Cyber Security Consultant, Kudelski Security*

## Introduction

Cyber-attacks have become a conventional component of warfare domains, joining the traditional ones (sea, land, air, and space) as NATO announces in July 2016.<sup>1</sup> The complexity of developing armaments and components provides opportunities for hackers who can infiltrate defense contractors during the weapon development process. For the military world, the principal threat comes from other states' cyber operations or patriotic freelance hackers who perform extensive and highly sophisticated intelligence activities.

## The more sophisticated, the more Vulnerable

Weapons are evolving. They are becoming more sophisticated and more lethal. Their development is long, complex, costly, and increasingly integrates electronic and cyber elements. The integration of Artificial Intelligence (AI) elements and lethal semi-autonomous and autonomous decision-making devices increases the cyber vulnerability of these armaments. An opponent, through a cyber-attack, could eliminate the threat of a machine or a weapon (e.g. an aircraft or missile), by turning it off without using any kinetic action or, worse, by taking its control. Similarly, there is a debate about the control of the technology of armaments by a country in the arms industry. Worth noting is that China unveiled a national plan to develop AI and expects to reach the same level as the U.S. by 2020 and to “become the world’s premier artificial intelligence innovation center” by 2030.<sup>2</sup> Russia also wants to play its part of this digital

<sup>1</sup> NORTH ATLANTIC TREATY ORGANIZATION (NATO), “Cyber defence”, *NATO website*, Jul 16, 2019  
[https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm)

<sup>2</sup> MOZUR Paul. “Beijing Wants A.I. to Be Made in China by 2030”, *The New York Times*, Jul 20, 2017

AI chessboard as President Vladimir Putin stated in September 2017 that “whoever becomes the leader in this sphere will become the ruler of the world”.<sup>3</sup>

The last U.S. military aircraft, the Lockheed Martin F-35 Lightning II, the costliest U.S. weapons program (development and production costs estimate around USD 406 billions)<sup>4</sup>, exemplifies these issues and the complexity of the geopolitics of armament. The F-35, which comes in three versions, is a complex plane that integrates a lot of electronic components, enabling it to be both a performance aircraft and a device that gathers and shares plenty of data. For example, the aircraft maintenance system called ALIS (Autonomic Logistics Information System) is centralized in the U.S. for all users of the F-35, American or foreigners. Currently, more than ten countries have bought or will acquire it (the United Kingdom, Italy, Netherlands, Australia, Canada, Denmark, Norway, Turkey, Israel, Japan and South Korea).

This gives hackers the opportunity to perform a man-in-the middle attack that provides access to the management of the aircraft maintenance, the missions system and the cryptographic keys used in every aircraft in service.<sup>5</sup> In addition, the U.S. will be in control of maintenance management of the aircrafts, which means that they can avoid supplying pieces to repair or update them. This risk forced Israel to create a complete maintenance system with firewalls to ensure that no data will be sent to the U.S. This, with a stock of spare parts, will increase the independence in case of a conflict.<sup>6</sup> Some analysts claim that thanks to this share of data between the plane and the U.S. centers, the Department of Defense can switch off the aircraft, even when flying, in case of necessity.

## The Masters of APTs and Reverse Engineering

China and North Korea have been for a long time accused of cyber intrusions to spy and steal data of Western and East Asia states’ aerospace and defense industries. Two major Chinese Advanced Persistent Threat (APT) campaigns dubbed “Titan Rain” and “Byzantine Hades” enabled massive exfiltration of classified information. One of the latest cyber-attack happened in 2017 when North Korea probably stole warship blueprints from South Korean Daewoo.<sup>7</sup>

U.S. military aircraft are a special focus of the Chinese government. In January 2015, Edward Snowden revealed that China stole designs of the F-35.<sup>8</sup> Indeed, in March 2016, Chinese hackers pleaded guilty

---

<https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html>

<sup>3</sup> MEYER David. “Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World”, *Fortune*, Sep 04, 2017

<http://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/>

<sup>4</sup> TURNER Julian. “The \$1 trillion question: is the F-35 project too big to fail”, *Airforce Technology*, Jul 16, 2019

<https://www.airforce-technology.com/features/f-35-project/>

<sup>5</sup> KÜMMERLING Pascal. “Le F-35, une machine à broyer la concurrence européenne”, *24 Heures Blog*, Oct 05, 2017

<http://psk.blog.24heures.ch/tag/f-35>

<sup>6</sup> KÜMMERLING Pascal. “Le F-35, une machine à broyer la concurrence européenne”, *24 Heures Blog*, Oct 05, 2017

<http://psk.blog.24heures.ch/tag/f-35>

<sup>7</sup> CHOI Haejin. “North Korea hacked Daewoo Shipbuilding, took warship blueprints: South Korea lawmaker”, *Reuters*, Oct 31, 2017

<https://www.reuters.com/article/us-northkorea-missiles-cybercrime/north-korea-hacked-daewoo-shipbuilding-took-warship-blueprints-south-korea-lawmaker-idUSKBN1D00EX>

<sup>8</sup> PAGANINI Pierluigi. “Chinese hacker admitted hacking US Defense contractors”, *Security Affairs*, Mar 24, 2016

on charges of hacking U.S. defense contractors, such as Boeing, to steal blueprints and intellectual property for the F-35, the Lockheed Martin F-22 Raptor and the C-17 transport aircraft. One of the hackers was then sentenced to nearly four years in a U.S. prison.<sup>9</sup> During 2017, 30 GB of sensitive data regarding Australia's F-35 and P-8 surveillance aircraft programs was stolen from an Australian government defense subcontractor.<sup>10</sup>

Thanks to reverse engineering, joint projects and technology transfers, China can produce the majority of its military's indigenous armament systems. Therefore, spying and data stealing of blueprints or technical information are part of the Chinese strategy to catch up with the most advanced military technologies. An example of reverse engineering is their second aircraft carrier, based on the first one, which is a refurbished second-hand vessel from the 80's bought from Ukraine in 1998 uncompleted. Based on it, the Chinese Navy is planning to launch in 2020 its first home-built aircraft carrier with top-notch technologies.

Thus, China is stealing confidential files of military aircraft to be able to replicate the design and technologies, such as radar, engines or software. The latest Chinese military aircraft, the Chengdu J-20 integrates elements that were apparently stolen from the U.S. F-22, the first fifth-generation fighter aircraft of the world, and the Russian MiG 1.44, a project that never ended in a produced aircraft. Although physical likenesses can be highlighted, like with the Chinese prototype Shenyang J-31, which closely resembles the F-35, it is hard to evaluate the components and internal elements of these aircraft to establish whether or not they were genuinely reverse engineered.

## Why Military Aircrafts?

Having performance military aircraft is important, as air supremacy is still a vital element on the battlefield as evidenced by, for example, the 1991 the Gulf War aka Operation Desert Storm and the 2003 Iraq War aka Operation Iraqi Freedom. During these wars, the coalitions led by the U.S. had total domination in the sky thanks to their technologically advanced military aircraft. The coalition's network-centric military approach, which used the collection of data and the share of information to achieve a competitive advantage on the battlefield, had the most rapid and appropriate decision-making process of integrated and synchronized teams and services (Army, Air Force, Navy, etc.).

Now, military experts talk about fifth-generation jet fighters encompassing the most advanced features available, such as stealth signature, high maneuverability, advanced avionics (electronic systems), network data fusion (create data through sensors and share it) and multirole capability (able to perform different missions).<sup>11</sup> Therefore, developing advanced aircraft and drones will provide air supremacy for

---

<http://securityaffairs.co/wordpress/45597/intelligence/china-hacked-us-defense-contractors.html>

<sup>9</sup> WORLAND Justin. "Chinese Man Sentenced to Prison for Trying to Hack Boeing", *Time*, Jul 14, 2016

<http://time.com/4405934/chinese-hacking-boeing/>

<sup>10</sup> AFP. "F-35 Stealth Fighter Data Stolen in Australia Defence Hack", *Securityweek*, Oct 12, 2017

<http://www.securityweek.com/f-35-stealth-fighter-data-stolen-australia-defence-hack>

<sup>11</sup> DE BRIGANTI Giovanni. "F-35 Reality Check Ten Years On - Part 1: 'Fifth-Generation' and Other Myths", *Defense-Aerospace*, May 09, 2012

years to come, especially in the next hotspots of the world. All these efforts are supporting elements of power projection in the implementation of an Anti-Access/Area Denial tactic [A2/AD] in the South China Sea (aka the Nine-Dash Line) regarding China and the Yellow and Japan Seas for North Korea. Hence, these armament hacks.

## Dynamic Cyber Defense through Espionage

Combined with traditional electronic warfare, which is the use of electromagnetic systems to disturb and gain an advantage over a foe, hackers can support military operations. There are already questions regarding the possibility of hacking a commercial airplane while flying.<sup>12</sup> Thus, states launch intrusion campaigns to collect information that might be leveraged, sooner or later, to defend themselves. They want to get valuable or “actionable intelligence” by collecting, processing and stocking data. The NSA talks about “foreign intelligence in support of dynamic defense”.<sup>13</sup> Thereby, they can collect operations or armament plans to increase their defense and mitigation in case of an attack while also enabling cyber-attacks options (such as hacking the planes so that they are “switched off” instead of using missiles to shut them down).

One of the issues is that these APTs create a cyber security dilemma in a way that, when discovered, these cyber-attacks increase tensions instead of reducing one’s vulnerabilities. Some academic cyber experts argue that these “defensive-minded network intrusions...are not invasions, but intelligence efforts”.<sup>14</sup> Therefore, intelligence is part of international politics whether through traditional espionage or through hacking. In the end, “all nations spy and all nations know this”.<sup>15</sup> The real question to answer is at what point these efforts pose a vital threat that requires a kinetic response.

## The Future of War Battlefields

Terminator-like machines are not marching across the battlefield yet. But, it is a reality that autonomous weapons that can decide who and when to kill without direct human interaction in the decision-making process hold the potential to dramatically change the way we fight wars. Multiple weapons systems can

---

[http://www.defense-aerospace.com/article-view/feature/135080/f\\_35-reality-check-10-years-on-%28part-1%29.html](http://www.defense-aerospace.com/article-view/feature/135080/f_35-reality-check-10-years-on-%28part-1%29.html)

<sup>12</sup> WOLFF Josephine. “Hacking Airplanes”, *Slate*, May 03, 2016

[http://www.slate.com/articles/technology/future\\_tense/2016/05/the\\_aviation\\_industry\\_is\\_starting\\_to\\_grapple\\_with\\_cybersecurity.html](http://www.slate.com/articles/technology/future_tense/2016/05/the_aviation_industry_is_starting_to_grapple_with_cybersecurity.html)

<sup>13</sup> BUCHANAN Ben. “Prevalence and Dangers of Defensive Hacking”, *Motherboard*, Feb 20, 2017

[https://motherboard.vice.com/en\\_us/article/4xbv7j/the-cybersecurity-dilemma-the-prevalence-and-dangers-of-defensive-hacking](https://motherboard.vice.com/en_us/article/4xbv7j/the-cybersecurity-dilemma-the-prevalence-and-dangers-of-defensive-hacking)

<sup>14</sup> BUCHANAN Ben. “Prevalence and Dangers of Defensive Hacking”, *Motherboard*, Feb 20, 2017

[https://motherboard.vice.com/en\\_us/article/4xbv7j/the-cybersecurity-dilemma-the-prevalence-and-dangers-of-defensive-hacking](https://motherboard.vice.com/en_us/article/4xbv7j/the-cybersecurity-dilemma-the-prevalence-and-dangers-of-defensive-hacking)

<sup>15</sup> BUCHANAN Ben. “Prevalence and Dangers of Defensive Hacking”, *Motherboard*, Feb 20, 2017

[https://motherboard.vice.com/en\\_us/article/4xbv7j/the-cybersecurity-dilemma-the-prevalence-and-dangers-of-defensive-hacking](https://motherboard.vice.com/en_us/article/4xbv7j/the-cybersecurity-dilemma-the-prevalence-and-dangers-of-defensive-hacking)

coordinate with each other through interlinked computer networks much faster than the human brain can.<sup>16</sup> Think about the developing of military swarming drone attacks. The best and easiest solution in the end will be to hack a weapon instead of fighting it directly. Governments need to invest in operation security (OpSec) capacities to identify critical information to avoid its diffusion and reduce exploitation of it.

### About the Author



Julien Chesaux is a Cyber Security Consultant at Kudelski Security, a Swiss and American cyber security company. Julien mainly works on cyber security, information security and geopolitics analysis in order to help clients to find solutions regarding their threats. He is also a mediator and writer for the Swiss Think Tank Foraus and the co-founder of the [www.stralysis.com](http://www.stralysis.com). He has worked in diplomacy and cyber security for seven years in Switzerland, Australia and France. His main research interests are Global Security, Cyber Geopolitics, and International Affairs. LinkedIn profile: [www.linkedin.com/in/julien-chesaux-65279456](https://www.linkedin.com/in/julien-chesaux-65279456) You can reach me at [julien.chesaux@gmail.com](mailto:julien.chesaux@gmail.com)

---

<sup>16</sup> MAXEY Levi. “Can Robots Fight Wars? The Future of Lethal Autonomous Weapons Systems”, *The Cipher Brief*, Nov 20, 2016  
<https://www.thecipherbrief.com/article/tech/can-robots-fight-wars-the-future-of-lethal-autonomous-weapons-systems>

# 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 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.
- **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 Extensive experience in supporting global corporations with the setup and execution of their open innovation programs. Deep visibility and insights into: FinTech, InsurTech, Big Data, IoT, IIoT and Construction Technologies. Uzi has vast experience in building businesses and operations hands on and in supporting early stage companies with their go-to-market strategies and execution. Learn more about him here: <https://www.linkedin.com/in/uzi-scheffer-24302a11/>



# 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 2019 alone, Zimperium discovered two 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 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](http://www.zimperium.com).



# How to Combat a Terrorist Attack Using Modern Communications

By Milica D. Djekic

Combating the terrorist attack is a challenge for security, safety and community. Through the previous period of time we are witnessing the different types of terrorist offenses and those occurrences could teach us to take the active role in fighting against such a security issue. The modern defense doctrine would appoint us to observe the terrorist activities as the incidents happening on the battlefield as well as within some populated areas. The terrorists would target the places with so many people as the impacts of their actions would get so spectacular. They would believe that more people get affected with their operations; the easier they would spread the fear, panic and hesitating within the societies. At this stage, we would notice that the current terrorist incident within the urban areas could get characterized as guerilla attacks usually including the lone wolves operations. Once the terrorist incident happens, it's so important to resolve such a crisis at the crime scene. Sometimes the authorities cannot save the human lives and in those cases – the bad guys are getting the battle. If we talk about the hostage situations, we frequently need a team of the experienced Special Forces persons who are capable to tackle such a scenario and negotiate with the malicious actors. The question here would be if we could prevent the terrorist activities anyhow. The answer to this question is quite clear and it would suggest that there are the methods, techniques and strategies to maintain the risk from terrorism at the quite acceptable level. The near past experiences would indicate to us what the possible targets of the bad guys are and the entire defense and intelligence community would cope with the situation on the terrain from hour to hour. The role of this effort is to provide the better insight how the terrorist plans could get discovered in the practice and how we could potentially prevent any serious losses within our communities.

So, we would suggest that there are the ways to monitor the situation constantly and continuously and probably respond to any terrorist attack attempt. First, we need to realize that the terrorist groups are vitally dependable from the emerging communications technologies and if you want to get some of those actors, you need to cut on their information exchange. So many dedicated individual from a defense sector would work day by day and spend a lot of sleepless nights in order to protect the values of our ongoing civilization. That's not the easy task at all and such a profession seeks a lot of patience and

concentration in order to remain focused on your mission. The fact is defense forces would try to prevent the terrorist attacks putting under a control the entire cyberspace and the rest of the communications channels. Why it matters to do a surveillance of the web, phone lines and so many connected devices? The answer to this concern is quite obvious and it would indicate that those places got so busy and if you put them under the monitoring – you would undoubtedly find something. The experience would suggest that the bad guys would choose to frequent spots to operate and either they do something in the public or from the safe locations using their computers with the internet connectivity – they would get capable to exchange a plenty of information and make some plans on. The role of the defense persons is to discover such a communication and prevent any malicious stuff happens. The point is the good guys would deal with the technology that would provide them a chance to manage the risk at the quite good stage.

The fact is so many terrorist incidents would get discovered before anyone tries to do anything and from time to time the terrorists would succeed in their intent to cause harm to innocent civilians. Unfortunately, the defense community would sometimes fail to protect the people from those malicious operations and the entire societies would get wounded with those occurrences. The systems for the communications surveillance could get manual, semi-manual and fully automatic requiring more or less human engagement. Anyhow, the role of the defense professionals could not get underestimated in any fashion, because they would need to serve those technological advancements. The crucially important thing to such a task is the skill. In other words, if we need anyone preventing us from any crime – it's so significant to understand that such a person should get trained for that job. So many role-based systems would offer us an opportunity to do the administration of the user's accounts and monitoring such a communication – we would be in position to search for the possible malicious activities. The good instance of the role-based system is a Tor and if we want to make a deep dive into the Dark net, we would need to invest a lot of time and effort in order to analyze those communications. Also, if we use the modern technologies to prevent some kind of terrorist incidents, we should get aware of that such an approach could demand from us to search area by area attempting to figure out what is going on in some neighborhood. In addition, it's well-known that the majority of the international phone conversations are monitored and recorded by the authorities, so it's quite obvious that such a methodology could offer us the quite satisfactory results in preventing the both – crime and terrorism.

At this stage of our technological development – we are in position to take the advantage over the new technologies in order to prevent a lot of potentially malicious incidents. Combating the terrorism is the challenge as we have suggested at the beginning and we are quite confident that the coming technological solutions would offer us nearly limitless options to cope with such a concern. In other words, anyone wishing to commit the crime or organize the terrorist attack should think twice for a reason that sooner or later there will be the time to pay the big price on. The terrorism is the challenge and that's the fact, but would it be worth to take a part into such an adventure? We know that the people doing such a criminality would get led by some beliefs and in our opinion, it's so important to educate the human community how to deal with the highest values and standards. It's not that hard as it may appear at the first glance!

## About The Author



[Milica D. Djekic](#) is an Independent Researcher from Subotica, Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the book “The Internet of Things: Concept, Applications and Security” being published in 2017 with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert’s channel and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. She is the member of an ASIS International since 2017 and contributor to the [Australian Cyber Security Magazine](#) since 2019. Her fields of interests are cyber defense, technology and business. Milica is a person with disability.



## The Challenges of Endpoint Security

*By Milica D. Djekic*

The endpoint devices are those gadgets that would be the part of a big computing network dealing with the endpoints as its final destinations. The endpoints computing units could be capable to send and receive the information packets once they are connected to the web. Also, if we talk about the ordinary network traffic – those devices could get able to conduct the similar operations, so far. All data being stored on the endpoint spots should meet the certain security procedures and policies. In so many cases, the endpoint computers would serve to the end users and either they are simply with the internet connectivity or any network connection – they would need some suggestions to get protected from cybercrime and the other hacker's operations. In other words, when we talk about the endpoints – we would mean by that the computers with the web connectivity that would cope with some IP addresses and get some data and applications being the part of their storage. It's quite obvious that anything being exposed to the internet could deal with some kind of cyber breach, so in such a case – we need to do a lot to secure our final destinations from those scenarios. In the practice, so many IT security experts would agree that the cyber breach is something being so inevitable and the best way to cope with such a situation is to apply the tools that would provide you an option to detect the breach. In addition, there are some best practice advices how to secure your data being on the endpoint device. The fact is so many computing networks would use the firewalls and the other protections, so the signal coming to the endpoints could get assumed as quite reliable. On the other hand, the hacker's incidents are not the rare case, so it's quite important to think hard how to tackle that sort of the risk.

The endpoint spots being connected to the internet would deal with their own IP addresses and once the hackers get how to find the certain device – they may try to start exploiting its vulnerabilities. The encryption at the endpoint places is from the vital significance if we want to protect our sensitive information. There are suggestions that the cyber breaches should get accepted as our reality and the huge question here is how we could cope with any data recovery and business continuity strategies. The quite tricky situation is if your endpoint spot got the target of cyber criminals and if you literally got so annoying hacker inside your system. In such a case, it's so important to take into consideration how to deliver the incident response being the key pillar of your cyber defense. In other word, maintaining the risk within your endpoints could get the quite complicated task, so our tip here is that you need so skillful cybersecurity professionals who would get well-trained in order to overcome all those challenges.

Providing the security to the network's end users is the serious business, so we would recommend to anyone being with such a task to think smart in order to protect us from any kind of disadvantages. The endpoint security is not the job for amateurs and it seeks a huge knowledge that could support the IT security practitioner and his team to respond so actively to the wide spectrum of so different situations. The point is that there is no the real prevention in case of endpoint systems and what we can do only is the risk management. The people may believe that the endpoints are less important in the entire security practice, but sometimes they may appear as so strategically important places.

Through this effort, we would indicate it's the challenge protecting the endpoints and the fact is you need to deal with all three aspects of cyber defense being prevention, monitoring and incident response if you want to adequately cope with such a task. In our opinion, investing into IT infrastructure capacities could be the good decision, because your network's asset could provide the quite qualitative and safe web traffic to the end users. Also, there are a plenty of methods to discover someone's device being the part of the global network and then you should attempt to think like a hacker in order to realize what got uncovered within your infrastructure and at the next stage, you should think a bit as a cyber professional who is capable to cover the uncovered pieces of the situation. The reality would suggest that some parts of the cyberspace could get chronically uncovered and you would need to cover them on again and again in order to manage your risk. No problem could get resolved over the night and the purpose of cyber defense staffs is to get on a duty day by day, night by night with the task to tackle any single concern coming on. Even within some business your employees would rely on the endpoint systems and in such a case if their computers collapse – you should need to assure the regular backuping of their data. We would also mention that some of the files being on the endpoint machines should get encrypted in order to provide the lower level of the risk in case someone gets the idea to compromise them. The hackers would so clearly see all these vulnerabilities and they would know how to take advantage over your unprotected details, so if you are chronically the target to the cybercrime operations – you should know that the incident response solutions with the option to terminate someone's connection to your endpoint machine could get the right choice.

Finally, we should see that the endpoint security is so time consuming and it needs a lot of effort to get invested into the entire process of its cyber defense. The main point in this effort is that maybe we could try to apply a bit different point of view in terms of security and begin observing the things from the perspective of something being uncovered or vulnerable and try to figure out how such a weakness could get covered on. Once we cover our weakness – we would get less sensitive to the potential attacks or in other words, more resilient in any manner. In conclusion, cybersecurity as any defense is about the good covering on and if we master that practice, we would get in position to maintain the balance between the forces of offence and defense.

## About The Author



[Milica D. Djekic](#) is an Independent Researcher from Subotica, Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the book “The Internet of Things: Concept, Applications and Security” being published in 2017 with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert’s channel and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. She is the member of an ASIS International since 2017 and contributor to the [Australian Cyber Security Magazine](#) since 2019. Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

# CRYPTO JUNKIES

## The Purpose of Neural Networks in Cryptography

By Milica D. Djekic

Through the entire history of the Human Kind, the nature would keep surprising and surprising us with its wonders. So many beings on our planet got the capacity to learn and absorb the new knowledge and techniques. On the other hand, so many scientists would suggest that the humans got the best possible learning curve amongst all living things. In other words, we would get something the psychologist would call the intelligence. It's our ability to connect the stuffs with each other and do some reasoning about our surrounding. Apparently, the entire scientific community would recognize such a capacity with so many living beings and there would appear the need to mimic the nature in order to produce some technological solutions that would get the characteristics of the intelligent creatures. Here how we come to the term artificial intelligence or AI being the good representation of the natural intelligence. Moreover, it's quite clear that the AI projects would need the teams of the multidisciplinary experts and researchers, so if we want to use some inspiration coming from the natural phenomena – we would need to get familiar with so many fields of science and technology. The greatest challenge to the modern cognitive science is how human nervous system works and there are still a lot of questions in such an area that seek the rational answers and explanations. One of the biggest mysteries in the world is the human brain and many scientists believe that such a mechanism could provide us a deep understanding of the entire nature. At this stage of our development, we would know something about how the neurons function and as time goes on our perspectives will change and we would get some kind of the better situational awareness. So, the basic building block of our brains is the neuron and in case of the AI – the researchers would attempt to mimic how it works.

The fact is the human nervous system would use the electricity to transmit the signals through the human body. All the information from the body's peripherals would go to the brain and that organ would process any of those electrical signals. Every neuron would simply deal with its activation potential being the electrical impulse that would trigger the entire process of thinking, feeling and judging. The quite complicated, right? Practically, the human organism would transfer the time changing electrical impulses through itself and such electricity would cause the existence of the magnetic field making the huge electromagnetic field around our bodies. The majority of biological systems would cope with that sort of

bio-electromagnetic field and there are a lot of branches of science and technologies that would suggest to us we do not completely understand the life's processes within our environment. As we have indicated – the emerging technologies would try to cope with the biological systems intending to create something being capable to mimic the life. The human intelligence is quite complex to get simulated and the experience would suggest that there are still a lot of things that need to get resolved. At this stage, we would notice some progress in such a research and we would be at the beginning of the new exciting epoch in science and technology being recognized as the AI. The AI would rely on the findings coming from neural science and it would try to deal with the well-known theories of the human mind. In such a case, we would talk about the most famous AI tool being the neural networks. That sort of advancements would show some capacities to get used for machine learning, pattern recognition and control engineering as well as some cybersecurity purposes. The quite powerful weapon, you would agree with us?

From one perspective, the neural networks would so smartly mimic the human brain transferring the electrical signals through connections and using the activation functions in order to produce the activation potential. The majority of these instances would get tackled using the computing systems and those projects would increasingly need the skillful developers who would create the useful software solutions. The activation function would normally be some mathematical rule that would give us a chance to produce some signal. In other words, the neural networks' design and programming is definitely the job for mathematicians and you need to be seriously creative in order to make your own neural network. As we said – the neural networks got ability to learn and such an advantage could get applied in so many areas of the interest. For instance, if we talk about the cyber defense – we would notice that our neural network AI solutions could help us better understand the cyberspace and everything happening there. In addition, if we try to apply the neural network in cryptography, we could get the quite dynamic encryption that could offer us key, strong or even perfect ciphering. The opportunities coming with the neural networks and the entire AI wave are nearly limitless and if we attempt to correlate those areas with the quantum computing we could get so close to discover some secrets of the nature. As we know, the defense is about covering the uncovered details and if we try to apply something that fast learning as AI is – we could figure out what the weaknesses in our cyberspace are and how they could get repaired. The point is that the application of neural networks in cryptography could open us the doors to some new dimensions of science, technology and security at the same glance.

The future may seem so promising and hoping and if we take into account all the products of our technological revolutions – we would notice that the coming times could offer us so exciting landscapes. As we got so talented mathematic scientists to design the new and new generations of neural networks, we believe that the similar effort could get used in making the cryptographic systems being based on the AI. Such a sort of discovery could find the strong applications in a constantly changing environment as the web is. The human intelligence would describe the ability to cope with the unknown surrounding and if we try to observe the AI from such a perspective – we would realize why it's so important to get capable to handle any technological environment including the good defense solutions.

## 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 2019. Her fields of interests are cyber defense, technology and business. Milica is a person with disability.



## Overcoming the Cybersecurity Staffing Drought

*COMPANIES WON'T EVER BE ABLE TO HIRE ENOUGH QUALIFIED PROS. PARTNERING WITH FULL-SERVICE CYBERSECURITY PROVIDERS IS NOW A VIABLE ALTERNATIVE.*

*By Gary Fish, Founder and CEO, Fishtech Group*

### Introduction

Whether you're responsible for managing IT security at a large multinational corporation with facilities spread across the globe or at a startup in Boulder or Beaufort, chances are your cyber defenses don't measure up to the high standards you set when you took the job.

I would also bet that the biggest single reason is an inability to hire enough personnel with the skills and experience necessary to mitigate your worst cyber threats. And even if you have beat the odds and assembled your cyber dream team, try retaining them when another company comes along tomorrow promising larger paychecks or more authority.

### The Resources Gap is worse than You Think

There's no question that the skillsets of today's top cyber-defense personnel are far superior to their predecessors. The problem is that there simply aren't enough of them to go around. Even individuals with base-level qualifications are getting harder to find, and more expensive to hire.

Worse yet, the gap is getting wider, not narrower. In a well-known 2017 study, Cybersecurity Ventures predicted there will be 3.5 million open cybersecurity positions worldwide by 2021, with at least 500,000 of those unfilled jobs in the U.S. alone. That's more than triple the shortfall that existed just two years ago.

With cyber-attacks expected to cost global enterprises some \$6 trillion annually by 2021, according to Cybersecurity Ventures, companies are under intense pressure to demonstrate they have the security in place to protect against the diverse types of technological and behavioral threats they face.

Many are counting on colleges and universities to start churning out large pools of qualified recruits. But while computer science departments everywhere are making great strides in expanding their undergraduate and masters programs, most are still years away from producing sufficient numbers of graduates with the qualifications that are most relevant to today's cybersecurity challenges — let alone tomorrow's. We're going to need several *dozen* Carnegie-Mellons, not just one.

Other promising avenues exist. Women, currently only about 15% of the cybersecurity workforce, are being more diligently recruited than ever before, as are military veterans. Promoting, training and certifying tech-minded staff from within is becoming more common, too. The more daring companies are even hiring kids with cutting-edge IT skills straight out of high school. Geek Squads and Genius Bars also make very good farm teams.

As commendable as these initiatives are, however, they could take up to a decade to have a meaningful impact. In the near to medium-term, meanwhile, demand for cybersecurity jobs in both the private and public sectors will continue to far outstrip the available supply of people, a shortage that is exposing organizations to ever-greater levels of risk.

## Cyber-Partnerships to the Rescue

If organizations won't be hiring or training their way to full strength any time soon, then what's the solution?

In my ongoing discussions with CIOs and CISOs, I'm seeing a much greater willingness to forge close partnerships with specialty companies that can meet some or even all of their cybersecurity mission requirements.

Behind this long-overdue shift in thinking is an acknowledgement among corporate leadership that: 1) cybersecurity has become too specialized, technologically complex and labor intensive to manage only in-house; and 2) digital transformation — in particular the adoption of cloud-based platforms, artificial intelligence-based analytics and open-source software — is making these partnerships a viable option even for something as consequential as their company's own security.

This new breed of partner is neither a conventional outsourcing firm nor a pure consultancy. Instead, it is deeply embedded with the client and offers hybrid cloud-based and on-premises solutions — plus services like managed detection and response — using data-driven analytics, a high degree of automation and some staffing support. At the top end it can include subscription-based 'security as a service' offerings, plus strategic staffing and advisory services.

## Enterprise-Level Security for Everyone

A well designed cybersecurity partner program offers several distinct advantages over a purely in-house operation. These include:

*Adaptability.* The cyber-threat landscape is evolving at warp speed, as are the technological countermeasures. Meanwhile, organizational security priorities are shifting in fundamental ways, for example from protection and prevention to detection and response (an overdue acknowledgement that not all cyber threats will be stopped by perimeter defenses). The expectation of rapid adaptability is not something that should be imposed on already overtaxed security organizations.

*Scalability.* As threats grow in scope and complexity, companies will fall further behind, putting their systems, facilities, finances and people at risk. Detecting the most advanced persistent threats also will require *more* data sources, not less. This is a significant problem when so many security analysts are already experiencing alert fatigue just from monitoring network data. Partners with strong data science teams can help, for instance by applying machine learning and other artificial intelligence techniques to reduce the noise and highlight the biggest threat signals. Likewise, leveraging the operational efficiencies, rapid elasticity and on-demand resourcing of the cloud is critical in managing analytics at the volume, velocity and variety of today's threat data. This integration of AI, open-source software and the cloud produces solutions that alleviate a major work burden from the client's security team.

*Automation.* A third way to address the staffing shortfall is orchestration and automation, which offers a 'force multiplier' for overworked analyst teams. The best outside providers can tailor such a system to take account of an organization's existing policies and procedures, for faster and more automated incident responses.

Finally, from a top- and bottom-line perspective, the biggest advantage of cyber-partnerships is cost-effectiveness. Small and medium-sized business are looking at bare-minimum outlays of \$1-2 million apiece to stand up a security operations center (SOC) with three shifts of three analysts each, plus backups. Organizations with more than 5,000 employees require even more expansive (and expensive) cybersecurity operations, while multinationals will need a SOC not just in the U.S. but most likely in Europe and Asia as well.

A partner with virtual SOC capabilities, by contrast, can offer superior 24/7 security for a fraction of the total cost of ownership — due to economies of scale, reliance on cloud infrastructure and deployment of AI techniques to handle the heavy analytical lifting, while limiting human involvement only to the most critical cybersecurity management functions. For smaller companies in particular, partnering with an outside provider is probably the only way to obtain enterprise-level security without breaking the bank.

In order to get more comfortable with cyber-partnerships, IT security leaders are developing their own set of selection criteria. Some of the most critical differentiators they look for are:

*Full-Spectrum Expertise.* We're no longer in an era when one IT security expert can understand an organization's entire risk profile and manage its mitigation efforts. The threats have become too multifaceted and the solutions too specialized. In addition to the right technologies, a partner needs a deep bench of human expertise to keep up with and help explain the complexities of the cybersecurity landscape, freeing the client to focus its internal resources on what *it* does best.

*'Hybrid Cloud' Experience.* Cloud-only cybersecurity solutions offer superior capabilities to on-premises hardware and software. But while many users assume that cloud adoption means life will be easier, in reality it often means the opposite. The primary challenge is that many companies have invested heavily in on-prem solutions, but these can't realistically be transitioned to the cloud. As a consequence, a partner's ability to design and manage hybrid cloud/on-prem architectures will be critical for the foreseeable future.

*Vendor Agnosticism.* Many companies have discovered that they are 'locked in' to particular point solutions. This is dangerous in an industry that: 1) has fragmented into a bewildering assortment of sub-disciplines; and 2) is simultaneously undergoing a wave of consolidation that will result in a number of vendors going out of business or being absorbed into larger entities. The best cybersecurity partners will be independent of, but deeply familiar with, *all* the players. They thus can recommend the best integrated solution based on the user organization's size, geographic scope, threat priorities, legacy systems and future needs — without favoring one vendor over another.

*Consulting Culture.* Companies need help fleshing out their cybersecurity programs, filling in capability gaps, transitioning to the cloud, understanding new threats and much more. The ideal partner spends a lot of time fully understanding the strategic priorities and operational protocols of a company's security team in order to craft right solution the first time.

## Conclusion

Not too many years ago, it was unthinkable to organizations that they would permit their operations and sensitive intellectual property to be placed in the cloud. Yet that's exactly what happened. I would argue we are well past that inflection point when it comes to staffing cybersecurity operations. With plenty of evidence in hand about the growing cyber personnel shortage, alternatives should have already been put in place.

Fortunately, many organizations are now seeing that the best way to alleviate their current long-term staffing drought is to find a trusted partner that excels at leveraging cloud, AI and open-source technologies into integrated solutions that are optimized to mitigate the cybersecurity risks of today *and* tomorrow.

## About the Author



Gary Fish is Founder and Chief Executive Officer of Kansas City-based Fishtech Group. Gary's focus is to set strategy, assemble top talent, point the team in the right direction and let them do what they do best. Gary has over two decades of experience as an entrepreneur, technologist and CEO in the cybersecurity space. In his career he has bought and sold over a dozen companies and established himself as a thought leader in his space. Gary founded and built FishNet Security, the largest cybersecurity integrator in the world, and he also founded FireMon, the first software company focused on firewall policy orchestration. Gary graduated from DeVry University and was a proud member of the US Army National Guard. Gary can be reached online at <https://www.linkedin.com/in/garyfish/> and at the Fishtech Group website <https://fishtech.group/>.

password

## From HUMINT to Virtual HUMINT

*The new frontier of Intelligence*

*By Antonio Teti*

*Professor of IT Governance and Big Data, University "G. D'Annunzio" di Chieti-Pescara*

### From Humint to Virtual Humint

Virtual intelligence, or virtual humint, as in the case of human intelligence (HUMINT), focuses its attention on the identification, recruitment and management of human sources, but through techniques and methodologies that can be used in the virtual world. HUMINT, understood in its traditional form, can never be completely replaced by online digital technologies, as the need to have human sources able to access direct information is the best way for intelligence activities. Human Intelligence, however, presents some critical issues due to the research / presence of human sources in particular geographical contexts and high risk, an aspect that has always had high levels of danger. Another aspect, certainly not irrelevant, is the growing difficulty of being able to dispose of sources, equipped with a specific background and experience, in the areas and in socio-cultural contexts in which the necessary requirements related to intelligence activities are manifested<sup>17</sup>.

A significant contribution to reduce these complexities that affect the collection of information can be represented by the use of virtual instruments usable in Cyberspace, a digital ecosystem able to ingest, without limits of any kind, information of any kind. However, considering that the collection of information within the network could be the key to the elimination of human intelligence, would be a very serious mistake. The proof of this lies in the activities of cyber espionage conducted, for example, against ISIS, which did not produce the astonishing results on the hopes of many intelligence agencies.

Historically, the development of VIRTUAL HUMINT (VHUMINT or CYBERNETIC HUMINT, as it is often defined in intelligence circles) began around the middle of the last decade, initially through the analysis of online forums, through the use of proper names or pseudonyms. Subsequently we proceeded to create false identities (fake identities) in an attempt to disguise the real authors of the activities of

---

<sup>17</sup> Russell D Howard, *"Intelligence in Denied Areas: New Concepts for a Changing Security Environment"* (Joint Special Operations University, 2007), <http://www.dtic.mil/dtic/tr/fulltext/u2/a495385.pdf>

intelligence, and consequently to the creation of groups dedicated to the study and analysis of the profiles to verify their veracity. Although these techniques are projected towards the assimilation of information within the network, they have not produced particularly striking results, also in consideration of the vastness of the instruments available in the virtual world and according to the different psychological approaches that push the individual to the use of the web and social media. The substantial difference between the traditional and the digitally conducted HUMINT resides, as it is easy to perceive, in the activities of the operative agents.

HUMINT is mainly made of direct contacts, aimed at creating a climate of trust, interactions with people who belong to circuits of interest, meetings to develop personal affinities, long-term relationships, tracking, surveillance, direct control of environments, etc. All this allows to develop what in the intelligence environments is defined as "handling from a long-term perspective", namely the development of a movement of the relationship on a long-term perspective, constantly monitoring the reliability of the relationship and the growth of the level of confidentiality. VHUMINT is based on relationships that are not necessarily permanent, that have a lower degree of commitment and loyalty, which do not allow levels of depth in the management of relationships because they are not based on a direct human bond. Furthermore, they are significantly affected by the many anomalies attributable to the peculiarity of anonymity on the network. HUMINT involves people within a physical contact, intimate and direct, with an emotional language that fosters connection and closeness, beyond the shared interests. The physical contact, eating and drinking together, sharing emotions and situations, are exercises that allow you to create a special connection, which contributes to the increase in motivation in the development of the relationship. In cybernetic VHUMINT sharing is based, on the contrary, on a strong convergence of interests.

If the level of commitment in HUMINT is higher, since the direct relationship imposes immediate responses and actions that can also seriously endanger the management of the relationship, in VHUMINT the level of danger is greatly reduced due to the absence of time barriers and geographical. The digital world makes it possible to conduct a virtual contact that has only a few minimal similarities with a physical relationship. The advantage of a virtual relationship lies in the structuring of an interaction that involves minimal risks, thanks to the confidentiality and anonymity guaranteed by the Internet network. In the world of VHUMINT it is possible to recruit new agents and sources in different ways, and the choice is practically unlimited. Intelligence agencies can quickly locate them, based on techniques that can be applied to an endless pool of users. It is also possible to conduct a "step-by-step" recruitment and management activity (based on a series of particular steps), with relatively low risks and almost zero costs. Links with individuals and groups can be activated easily and without the dangers of physical contact. But the most innovative aspect of VHUMINT lies in the possibility to reach, without limits of space and time, a target audiences difficult to approach in any other way.

The virtual world offers useful tools, for example, for the conduct of investigative activities aimed at verifying the reliability of the agents to be recruited, in addition to the production of checklist questions for the conduct of interrogations. A hypothesis is the verification of the reliability of an individual who is subjected to an interrogation, which can be enriched with the analysis of the information he shared on the social media used (Facebook, Twitter and Instagram), or other news that can be downloaded from the web. The problem of anonymous sources, therefore unknown, seems to become insignificant when information is destined to research and to the understanding of a phenomenon. On the other hand, it is undeniable that information, of any nature or provenance, is fundamental for the fight against a threat. Nevertheless, Cyberspace allows to hide, if not to vanish, in the sea magnum of information, disguising

its identity through a myriad of nicknames, false profiles or severe entities, guaranteeing, in a determined manner, the communications and identities of the agents.

At one time they were entrusted with the task of managing paper messages, baggage, radio material and codes to share with the sources, aspects that exposed them to incalculable risks and difficult to manage. Today it is enough to share a USB stick, some electronic mail account or profile on a social network to transmit large amounts of multimedia information protected by encryption algorithms that make the content inaccessible. But if the virtual world has reduced the "face-to-face" relationship, substantially reducing the risks deriving from direct contact, at the same time it has stimulated in a colossal way that part of active intelligence that can be transformed, however, into a short or long-term danger. The uncontrollable increase in false identities, rampant disinformation, the indiscriminate monitoring of network traffic, the unstoppable spread of malware, the continuous violation of user privacy, the development of network connection technologies better known as the Internet of Things (Internet of things), are just some of the pitfalls generated by the human mind for the achievement of purposes of various kinds. With VHUMINT it is possible to penetrate Cyberspace in search of information on people, situations, geographic and political contexts, inserting itself into forums, chats, e-mails, social networks and the web.

Cybernetic agents can profitably conduct a wide range of online activities, for example, to recruit new agents or informants, to disseminate information aimed at conditioning public opinion, to create false rumors about a person to discredit / publicly accredit it (cybernetic shaming). By virtue of the peculiarities typical of the virtual world, the presence of cybernetic double agents, i.e. cybernetic agents that make double the game, is constantly increasing. In the Internet, the avatar image is very widespread because it can allow you to have an unlimited number of identities that can be spent in different environments and for other purposes. Over the past decade US intelligence agencies have warned users about using avatars to conduct terrorist attacks (as in the case of Osama Bin Laden's avatar), and for the recruitment of terrorists<sup>18</sup>.

It is known the infiltration activity of the American and British intelligence in Second Life and Warcraft to verify the presence of terrorists who used the virtual environments mentioned to recruit new sympathizers to Jihad. Indicative is the study of 2008<sup>19</sup> (3D Cyberspace Spillover: Where Virtual Worlds Get Real), commissioned by the Director of the Office of the Director of National Intelligence (ODNI), which provides unique indications on the use of intelligence activities in games online. It should be noted that the disclosure of the classified study, which took place in 2014 at the request of the Federation of American Scientist under the Freedom of Information Act, takes place about a month after the disclosure of confidential documents conducted by the former employee of the National Security Agency (NSA) Edward Snowden, who claimed that US and British spies suspected that many online games were being used as "... a goal-rich communication network" that could provide terrorists with "... an easy way to hide" and to plan attacks<sup>20</sup>, although in the final part the study confirmed that "... there is little evidence that Islamic militant groups and jihadists have begun to exploit extensively the opportunities offered by virtual

---

<sup>18</sup> Sara Malm, *A Threat for the Digital Age – An Avatar Osama Bin Laden: U.S. Intelligence Warned Terrorists Could Create Virtual Jihadist To Preach and Issue Fatwas for Hundreds of Years*, MailOnline, January 9, 2014, <http://www.dailymail.co.uk/news/article-2536440/A-threat-digital-ageavatar-Osama-bin-Laden-U-S-intelligence-warned-terrorists-create-virtualjihadist-preach-issue-fatwas-hundreds-years.html>; David Kravets, *US Intel: Bin Laden Avatar Could Recruit Terrorists for Hundreds of Years*, Wired, January 9, 2014, <http://www.wired.co.uk/news/archive/2014-01/09/osamabin-laden-avatar>

<sup>19</sup><https://fas.org/irp/eprint/virtual.pdf>

<sup>20</sup> <https://www.wired.com/2014/01/osama-bin-laden-avatar/&prev=search>

*worlds*". Contrary to the final consideration of ODNI, especially the Israelis, they have invested heavily in the development of avatars, also using them in the Deep Web, as witnessed by one of the spearheads of Israeli computer security: SenseCy<sup>21</sup>, a leading company in the field of cyber security modal level that bases the information research activities through the massive use of avatars on the web, on social networks, and in forums. Through the use of false users, Netanya company analysts can extract an impressive amount of information on the planning of hacker attacks and proselytism for terrorist purposes. In addition to SenseCy, some US companies, such as Crowd Strike and iSight Partners, which collaborate on a regular basis with the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA), rely on the use of spy tactics based on avatars to conduct proactive activities aimed at countering cyber-attacks. In December 2013<sup>22</sup>, SenseCy analysts, through the use of virtual humint techniques, have intercepted the first cyber-attacks in code #OplIsrael, planned by AnonGhost, a group of Tunisian hackers. In closed forums, AnonGhost has provided its supporters with a list of targets and tools to conduct attacks, including a self-developed malware called AnonGhost DdoSer. The technicians of the Israeli company, thanks to the previously used cyber intelligence activities, were able to collect and analyze the data relating to the malware before its release, thus activating the cyber defense measures aimed at rejecting the malware. What is shared by companies that use virtual humint techniques lies in the growing awareness that the capabilities of firewalls and systems protection software are less and less resolute. On the contrary, as analysts admit, through the use of social media intelligence and web intelligence activities, it is possible to design very effective preventive actions to counter cyberattacks.

### About the Author



Antonio Teti is Head of the Information Systems and Technological Innovation Department of the "G. D'Annunzio" of Chieti-Pescara and professor of IT Governance, Cyber Intelligence and Big Data at the Master's Degree in Economics and Management of the Department of Business Economics. Expert in Cyber Intelligence, ICT Management and ICT Security, he has accumulated thirty years of experience in studies, research and consulting in public, private and government institutions. He has been a professor of Computer Science, Cyber Security and Cyber Intelligence at several Italian universities including La Sapienza University, the Catholica University of the Sacro Cuore in Rome, the University of Teramo, the

University of Foggia, The Link University, the LUISS University and the University of Calabria. He is a lecturer in Cyber Security and Cyber Intelligence at the School of Specialization for the Police Forces of Rome. He is a Technical Consultant in the IT sector of various Italian prosecutors. Author of numerous scientific publications he collaborates with several newspapers, magazines and periodicals of the sector, and participates in national and international conferences and radio and television programs on national broadcasters as opinion leaders. Awarded several prizes and honors in science and institutions, he is the author of numerous computer books adopted by Italian and foreign universities and over 180 publications.

<sup>21</sup> <https://www.sensecy.com/>

<sup>22</sup> <https://www.ft.com/content/7f4e5d56-df64-11e3-a4cf-00144feabdc0>

# Cybersecurity

## What's next for Cybersecurity?

By Min Pyo Hong, CEO and Founder, [SEWORKS](#)

What just happened? Unfortunately, many organizations may find themselves asking that question as they review their network security after suffering a breach.

There's no question that serious cybersecurity attacks are occurring more frequently, across sectors. Adding to an extensive list of hacking attacks that took place during 2019, the United States National Aeronautics and Space Administration (NASA) [confirmed in a memo](#), first published by Spaceref.com, that the personal information of some of its current and former employees may have been compromised after at least one of the agency's servers was hacked.

And while bad actors have uncovered vulnerabilities using tactics such as spray-and-pray and distributed denial of service (DDoS) attacks that flood a targeted system, these tactics won't go away. In the coming year, expect to see new threat approaches using artificial intelligence. For example, the spray-and-pray approach is commonly employed in AI hacking.

What will be different? Automated smart attacks

Significant advancements are happening in the field of artificial intelligence, whether it's to identify cancer in tissue slides, play Go better than humans, or create a portrait that recently sold for more than \$400,000 at Christie's. What's the next thing that AI can do better than humans?

AI's capabilities, along with the associated rich data, will shift AI products and services into the spotlight of cyber criminals – whether it's to access the data or manipulate the AI system itself.

We believe the new trends in hacking will deploy methods that will be almost 99% automated, detailed and will target both known and unknown security vulnerabilities. Most likely we'll see one-day or zero-

day vulnerabilities that can be used to compromise a system's authority by attacking different networks. The consequences could range from hijacking confidential information, bypassing existing security measures and taking control of the system to much more. What differs from traditional hacking is that AI hacking is more efficient in terms of time and resources.

Unfortunately, artificial intelligence is teaching bots to be more human-like and it's becoming more difficult to distinguish between real human users and sophisticated systems powered by AI. We're also becoming comfortable with the concept of AI in our everyday lives. After all, many of us think nothing of starting the day by asking our omniscient digital friend (who lives with us), "Alexa, what's new?"

The advent of automated hacking carried out by artificial intelligence means the volume of attacks that can be conducted is much bigger than attacks carried out by humans.

The internet of things and a growing ecosystem of always-connected devices -- that may or may not be secure and may or may not control critical infrastructure -- also presents more hacking opportunities.

Cyberattacks using machine learning continuously and simultaneously probe wider areas for weaknesses, and insert malware almost instantaneously. The ability to quickly scale these attacks poses yet another threat.

### **The showdown: AI hacking vs. AI penetration testing**

Security experts strongly recommend ongoing cybersecurity vigilance, such as regular penetration testing, to ward off these upcoming smart attacks. After all, AI cyberattacks and penetration testing using artificial intelligence are fundamentally similar. The main difference is the intention.

When attackers utilize AI-powered attack tools more and more, it will be difficult to take appropriate action in terms of time and resources when employing first generation security practices because AI tools can execute a larger scale of attacks, faster than human attackers. The consequence? Insufficient time and resources to respond to attacks when they happen.

The bottom line is that enterprises and InfoSec professionals must prepare for advanced and automated cyber-attack programs. We highly recommended conducting security tests on a regular basis to discover security vulnerabilities before AI tools compromise them.

## About the Author



Min Pyo Hong, CEO and founder of SEWORKS, advises corporations, NGOs, and governments on digital and cyber security issues. Min led a team of five-time finalists at the annual DEF CON conference in Las Vegas, and is a PhD candidate at Korea University in SANE-LAB Information Security. A serial entrepreneur, his previous company, SHIFWORKS, was sold to InfraWare. Min also founded the WOWHACKER Collective, a non-profit security research group in Korea.

# Operational Excellence: The Key to Federal Agencies' Compliance

By Stan Lowe, Global Chief Information Security Officer, Zscaler

In many realms of life, there's a difference between compliance and excellence. For instance, you could build a house that complies with all local zoning and coding regulations, but that wouldn't necessarily make it a place anyone would want to live. And we've all known the "A" students who study hard and memorize lots of details so they can get a high grade on a test, but don't actually understand or appreciate what they've learned when it comes time to write an essay about it.

In terms of cybersecurity, the difference between compliance and operational excellence is especially pronounced for federal agencies. Traditionally, cybersecurity in the federal government is a compliance-driven activity, due to the huge amount and multiple layers of oversight that federal agencies receive from Congress, the General Accounting Office (GAO), and Inspectors General (IGs). All of these entities require checklist-based evidence showing that agencies have followed all the certification and accreditation rules when granting their Authority to Operate (ATO). Some agencies have hundreds of systems for processing these rules and have large organizations staffed with compliance experts specifically to produce, track, and curate the required documentation.

The considerable oversight and requirements lead to a situation in which agencies are more worried about complying with regulations, and showing they've done so, than about actually securing themselves or the government from operational threats. Agencies end up focusing on questions like "Are we compliant or not?" and "Do we have documentation that proves we are compliant?" when they should be concentrating on the much more significant question about whether they are creating a world-class operationally focused security program that ensures the security of the enterprise and its mission. An emphasis on compliance activities can inadvertently cause agencies to deemphasize other important aspects of their operations, such as understanding their complex environment and its activity, as well as what "excellence" really looks like for their agencies.

This isn't the fault of the agencies themselves, but rather the way cybersecurity is approached in the federal space, where agencies are constantly required to prove that they are doing what they say they're

doing through elaborate documentation—and they're rewarded for doing so. Security shouldn't be measured by how well an agency does paperwork; that's akin to driving your car using the rear-view mirror. It should be measured by how well an agency performs actual **cyber operations**. If federal agencies concentrate on operational excellence, the compliance aspect of cyber happens organically as a result of that effort.

## An operational imperative

Federal agencies are moving to cloud-based applications and operations. Sometimes the move is supported by agencies' security organizations and sometimes not, but it is happening, nevertheless. The use of cloud services makes compliance even more onerous and confusing, and agencies are left to make individual decisions based on their understanding of compliance as it relates to the cloud. For the mission areas, compliance is often viewed as an obstacle to go around, over, or underneath.

Fed RAMP was designed to help agencies securely use the cloud and save the government a tremendous amount of money in the process. By using a cloud security platform that has Fed RAMP approval, agencies can offload much of their compliance burden. While it's not a panacea—and a Fed RAMP approved platform like Zscaler can't eliminate all compliance issues—it can enable agencies to turn their focus to securing the mission and to operational excellence.

### About the Author



Stan Lowe, a cybersecurity and technology executive, has successfully led transformational change in large, complex environments, as well as small and mid-size cybersecurity and IT organizations. As Zscaler Global Chief Information Security Officer, Stan oversees the security of the Zscaler enterprise and works with the product and operations groups to ensure that Zscaler products and services are secure. Part of his focus is to work with customers to help them fully utilize Zscaler services and realize the maximum return on their investment. Prior to joining Zscaler, Stan served as the VP & Global Chief Information Security Officer for PerkinElmer, where he was responsible for global enterprise security and privacy. He has also been a Cyber Security Principal at Booz Allen Hamilton. Stan has extensive federal experience, serving as the U.S. Department of Veterans Affairs (VA) Deputy Assistant Secretary for Information Security, Chief Information Security Officer, and Deputy Chief Privacy Officer, as well as Deputy Director of the Department of Defense/VA Interagency Program Office. Before joining the VA, Stan served as Chief Information Officer of the Federal Trade Commission. Stan's public service record extends to the U.S. Department of Interior in the Bureau, the U.S. Postal Service Inspector General, and the U.S. Navy. Stan has also served as an executive in several technology startups, and currently serves on several boards advising on cybersecurity. He is a frequent speaker and writer on security topics.



# Five Strategies to Optimize Cloud Security in 2019

By Dannie Combs, CISO at DFIN

As more companies move data to the cloud, cybersecurity becomes a growing concern. Keeping ahead of evolving threats takes vigilance and a solid architecture. Here are five strategies every IT team should consider to improve its company's cloud security processes in 2019:

## 1 - Address Limited Visibility

With the rapid rise of cloud technology and DevOps practices, some security teams attempt to minimize risk by limiting the speed of change. Though minimizing risk is a valid goal, this method fails to address extremely fast-moving, technology-dependent business requirements and, as a result, in-cloud Shadow IT often emerges.

Cybersecurity teams must be able to answer three fundamental questions in order to successfully ensure visibility across their cloud footprints:

What applications are running in their cloud?

What data is being stored and/or processed within each cloud application?

Who has access to the data and applications?

In 2019, teams should resolve to incorporate technology solutions, such as Cloud Access Security Broker (CASB), in combination with native cloud provider accounting and audit tools to address visibility gaps.

## 2 - Establish Formalized Cloud Governance

For many organizations, business processes, policies and standards have not been developed to support the rapidly growing cloud landscape. Evolving data privacy and other regulatory obligations such as the European Union's General Data Protection Regulation (GDPR) add further complications for IT professionals. The implementation of a strategic, enterprise-wide approach to overseeing, managing and securing vital data in a multi-cloud environment must be a top priority.

Consider adopting these basic Cloud Governance principles in 2019:

Identity and Access Management with well-defined Role-based Access Controls (RBAC). Define roles clearly and control access based on business needs and data ownership. This approach will significantly minimize the exposure if user credentials are compromised as RBAC ensures user access is limited to a need-to-know basis.

Track and manage your cloud resources by using tags. Department, customer, data classification and environment tags are good examples. Security incident response is much easier when you can locate the owner quickly.

Use native cloud cryptographic key and secrets management capabilities. Managed Hardware Security Module (HSM) services are offered by the majority of cloud providers and easy to adopt and use.

## 3 - Make security and privacy the cornerstones of the cloud architecture

Most companies are still in the process of developing policies and standards for designing and configuring cloud infrastructure. Oftentimes, cloud architecture is the result of ad-hoc efforts driven by developers using cloud as a rapid prototyping environment, and poorly designed or misconfigured systems can be exploited quickly.

In 2019, IT executives should design comprehensive security architecture that includes a complete security stack consisting of:

Identity and access management and governance

Data protection and encryption

Data loss prevention

Data classification tagging

Security monitoring and operations.

Cloud technologies continue to innovate and evolve quickly. Everyday major cloud providers announce new features and capabilities, and businesses are eager to use them to differentiate from competitors. Tracking industry-leading best practices and the latest cloud security trends is a must. Cloud security blueprints must be constantly updated to ensure relevance to today's current threat landscape.

#### 4 - Extend your on premise security operations into the cloud

Many cloud providers and security solutions vendors are still catching up with cloud security capabilities as compared to traditional on premise solutions. Tracking data flow between on premise systems and the cloud, and providing consistent protection throughout the data flow is critical. Companies should also correlate their on premise and cloud incidents to ensure they have a complete picture of their systems.

Resolve to make identity and access management policies consistent across multiple cloud and on premise footprints in 2019, while also reviewing incident response procedures to reflect any changes to the cloud environment.

#### 5 - Automate security tasks

Given the speed and elasticity of cloud operations, it is next to impossible to secure the cloud using manual procedures.

In 2019, companies should automate the deployment and operations aspects of the cloud security by automating core security tasks, including:

- Secure orchestration and provisioning

- Vulnerability threat management

- Vulnerability patch management

- Continuous integration and deployment

- Security operations and incident response

- Security metrics generation and reporting

The cloud is here to stay and companies must have a cloud architecture that is designed with security and privacy in mind. Safeguarding cloud-based data from attacks requires not only strong security capabilities but also routine monitoring and updating throughout the year. As a new year begins, resolve to remain vigilant in securing your cybersecurity programs and protocols to mitigate risk of security breaches and to optimize your cloud services.

## About the Author



[Dannie Combs](#) is Chief Information Security Officer at DFIN ([Donnelley Financial Solutions](#) NYSE:DFIN), a global leader in risk and compliance solutions. As the CISO for a company with more than 3,000 employees across 17 countries, Dannie is responsible for all aspects of corporate cybersecurity not only for internal data, but ensuring clients' information is highly secure as well. He was formerly Director of National Network security for U.S. Cellular, and IT Compliance manager for Redbox. Earlier in his career, he was with the US Air Force and managed information security for NORAD and various Intelligence agencies. Dannie can be reached online at

[Dannie.Combs@DFINSolutions.com](mailto:Dannie.Combs@DFINSolutions.com)

[www.dfinsolutions.com](http://www.dfinsolutions.com)



# 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.

## 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.

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.

Let your least privilege cybersecurity journey begin!

### 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 blockchain, endpoint security, application security & virtualization and privileged access management. Prior to joining Thycotic Joseph worked on innovative blockchain 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. Joseph can be reached online at [https://twitter.com/joe\\_carson](https://twitter.com/joe_carson) and at our company website <http://www.thycotic.com/>.

# Top 10 Business Requirements for an Enterprise Cyber Threat Hunting Solution

*A cyber threat hunting solution should not simply be another layer of real-time detection. There are significant differences in the goals of a real-time detection tool (like antivirus) and a pure threat hunting solution. This article explores the top ten business requirements for selecting an enterprise cyber threat hunting solution.*

*By Chris Gerritz, Co-founder and Chief Product Officer at Infocyte*

Threat hunting—traditionally a highly specialized skillset—is now entering conversations about enterprise endpoint security. Within the realm of endpoint security, Threat Hunting Platforms complement your existing cybersecurity defenses (like EDR, EPP, AV, and UEBA) by approaching endpoint security from a different angle...

The practice of threat hunting is a proactive approach to cybersecurity, whereby a hunter forensically inspects the endpoints on your network for indications of compromise, threats (malware, ransomware, breaches, etc.) and vulnerabilities. Traditionally, it's a very time-consuming process; however, threat hunting platforms like Infocyte HUNT have automated and simplified the process of threat hunting, enabling enterprise security teams to hunt an entire network in as little as a day.

Threat hunting solutions produce, sort, and score “leads” (threats) into suspicious activity and adversary presence. A threat hunting solution should not simply be another layer of real-time detection. There are significant differences in the goals of a real-time detection tool (like antivirus) and a pure threat hunting solution.

For example, enterprise antivirus and real-time intrusion detection solutions focus on actionable alerting of attacks in progress while minimizing false positives. Threat hunting solutions, on the other hand, focus on two things:

- Post-compromise behavior and indicators of compromise (i.e. as described by MITRE ATT&CK).

- Enable proactive and effective investigation into anomalies, outliers, and other suspicious activity which may have not produced an actionable, high confidence alert.

The following goals are examples tailored for a typical enterprise which has to balance budgets, time, manpower, and skills.

## An ideal enterprise threat hunting solution:

Should produce, sort, and score leads into suspicious post-compromise activity or indicators.

Should enable a quick path to verify and investigate those leads to a conclusion.

Must provide answers to questions that were previously unanswerable.

Must not cause outages on the way to those answers [low business impact]

Must not take a team of engineers to support.

Must be accessible and approachable to a wide level of skill and experience.

Must be cost effective; must not take excessive resources to deploy, staff, and fund.

Must find things related to a real adversary you are likely to find in your environment.

Should provide data and conclusions useful for responding or mitigating a discovered compromise.

Should scale to the maturity of the organization.

To learn more about cyber threat hunting and request live demonstration of Infocyte's Threat Hunting and Incident Response Platform, Infocyte HUNT, please visit [infocyte.com](http://infocyte.com).

### About the Author



Chris Gerritz, a retired Air Force officer and service-disabled veteran, is a pioneer in proactive cybersecurity operations, having stood up the U.S. Air Force's first interactive Defensive Counter Cyberspace (DCC) practice. After medically retiring from the Air Force, Chris helped co-found Infocyte and develop the leading independent Threat Hunting & Incident Response platform, Infocyte HUNT.



## Cybersecurity as a Priority in 2019

*Cybersecurity has an increasing impact on the business and future of organizations.*

*By Pedro Tavares, Founder of CSIRT.UBI & Cyber Security Blog [seguranca-informatica.pt](http://seguranca-informatica.pt)*

Cybersecurity is a crucial element these days and it has an increasing impact on the business and future of the organizations. Tools that keep organizations safe against new emerging threats are today indispensable to follow a health doctrine focused in keeping away any cyber-problem. Those tools include Security Information and Event Management (SIEM), Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), Threat Hunting Frameworks, Anti-Malware Services and several solutions based on Intelligence Systems. A new and modern culture is growing and we are now walking on a novel and important pathway.

Words like cybersecurity, cyberterrorism, cyberwar, data breaches, phishing or “fake news” are already part of our everyday life. The weight the Internet has on society is such that it can be used to change democracies. With this, new malicious activities are expected from cybercriminals in 2019.

### Cybersecurity and the business impact

The last few years were heavily attacked as a result of the emergence of new types of threats with a higher degree of complexity and difficult to annihilate. A great number of threats like WannaCry, Bad Rabbit, and Presidential Elections in France, USA and Brazil, Equifax and British Airways data breaches, Mage cart APT, and many bad news and cases left the world on alert along 2019. How about 2019 — how will it be?

There is no doubt. The damage caused by these type of attacks on organizations and even on the future of the nations is clearly notorious.

According to Europol, ransomware, carding and skimming and also crypto jacking represent some threats that will continue to give IT professional’s nightmares over the next few years. Ransomware was a kind of attack involving around \$11.5 billion — data collected by Checkpoint. Carding and skimming attacks

are used to collect card data for later use and manipulation of personal data. The latter threat is related to crypto coins where the bandwidth and processing power of victims is used to mine cryptocurrency without user consent.

From the business point-of-view, the loss of information obtained by crooks represents the most costly component for all companies, whose average is 130 security breaches per year and this number tends to increase in the coming years due to fast grown and sophisticated methods that criminals are using.

Malware and web-based attacks are the kind of attacks that most hurt businesses, both with global losses of over two billion dollars. Web-based attacks typically include phishing attacks that still are a critical problem; business email compromise (BEC) attacks, where a large number of companies are targeted and with great losses recorded; and all what can be executed with malicious intent via an internet connection.

No surprise, PDFs are the most commonly attack vector used to widespread malware. Most malware domains, about 60 percent, have been associated with spam campaigns as the email continues to be the preferred channel to reach the victim easily.

Physical security is a topic of interest as well. The impact of cyber security on physical security is, in fact, a security top trend. About 30% of industry leaders consider this to be the most striking trend that companies expect to meet in 2019.

In contrast, ransomware will continue to be increasingly sophisticated, using live encryption and packing techniques in an attempt to hide itself in the operating system process tree. However, a portion of them will be replaced by the miners of crypto coins.

I want to highlight another critical subject: botnets. Massive targeted attacks that will produce bigger and smarter IoT botnets capable to “stop” the critical operations of great companies, including bank, governmental and military platforms, are expected. In recent years the number of devices connected to the internet has grown. These botnets are therefore getting bigger and smarter and operating with strong components based on artificial intelligence. We need to be prepared.

## What can we do to be safe in 2019?

There is a set of practices that can be described and that compose the current cybersecurity trends in organizations.

A resilient security perimeter should be built in order to enforce the organization's defenses (e.g., demilitarized zones - DMZs, firewalls, etc.). Well-segmented networks also need be one of the first preoccupations to maintain the infrastructure away from cyber threats, and Identity and Access Management (IAM) or user rights assigned according to the actual need of the organization's structure must be managed in a right way.

The implementation of data and device backups is the last resort when data loss happens. It should be supported in a policy with definition of target files, periodicity and retention, and with validation procedures and also recovery tests.

Have a strong password policy shared with all employees is extremely important. Long and complex passwords are the best way to protect accounts and the valuable information available behind the door. The use of other factors of authentication such as, Multi-factor Authentication (MFA) or Two-factor Authentication (2FA) is an additional step that need to be used.

The principle of the least privilege — employees should only have the information and resources necessary for their daily work, avoiding being used as a guiding wire for access to confidential data and documents of the organization.

Keeping security solutions up-to-date with regularly updating antivirus programs and signatures-based protections, and using protection solutions based on knowledge and behavior is another indispensable measure.

Ensure that all the information is sent in an encrypted channel, for instance, your emails. This can reducing that it can be obtained in a man-in-the-middle (MITM) attack.

The rule of thumb: all the activity and security events need be analysed. For example by using a SOC services or tools for this purpose.

And finally, employee's training still the best way to educate all the organization. Knowledge of safety principles should be passed on to ALL employees, a key step in cases such as phishing.

## Final Thought

The number of security threats is increasing and due to that investment in this field is needed, as well as a different mindset and new strategies that can influence and motivate people to fight in this battle.

As a final topic, I would like to say the following: — “Invest and go ahead, be an influencer, and cultivate and educate the people. This is the recipe and the success choice for a stronger and resilient future”.

At the end of the day, the goals are so simple: safety and security.

## 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](http://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 pretesting (Kali Linux), malware, hacking, cybersecurity, IoT and security in computer networks. He is also a Freelance Writer. Segurança Informática Blog: [www.seguranca-informatica.pt](http://www.seguranca-informatica.pt)  
LinkedIn: <https://www.linkedin.com/in/sirpedrotavares>  
Contact me: [ptavares@seguranca-informatica.pt](mailto:ptavares@seguranca-informatica.pt)

# 10 Considerations When Bringing in IT Outsourcing Contractors versus Working with a Managed Services Provider

By Mitesh Patel, Managing Director, Fifosys

## Do you really need them or can the internal teams deliver the work?

From either outsourcing elements of the support function to a managed IT services provider or potentially employing an in-house IT Director (at great expense!). In order to get the right service, it is essential for organizations to delve deeper into their core processes and begin to understand what is being delivered. Begin with a solutions assessment. Consider the current state of your IT systems. Identify areas for redevelopment then do a service assessment to ascertain what levels of service are required.

## What skill level are you buying in?

In any organization fewer than 250 employees - it is hard to justify employing a full-time experienced IT Director with skills to manage procurement, assess technology innovation and drive forward IT strategy in line with business needs. SME's need to work closely with individuals of expertise to inform technology direction based on clear business objectives. IT strategy should be a core component of corporate strategy – not a last-minute consideration. It should be based upon clear business targets and assessed upon clear performance measurement and reporting.

## How long is the contract?

Having a figure and duration of time in mind prior to any agreement will allow you to budget accordingly. Bear in mind the contractor will have their own expectations.

## Is the contractor working independently or as part of the team?

This will depend on the environment with which the contractor is arriving to. Are they coming in to fill in a position vacated by previous personnel or is this a new role? Is there an existing toolset waiting for them or will they be expected to develop a system with processes from scratch?

### What tools will the contractor need to deliver the job?

In addition to the level of standard you expect of the contractor, the contractor may have a clear idea of the toolset they will require to meet demands expected of them. The clearer the contractors' understanding is of work previously done within your existing setup as well as your expectations, the better the recommendations they can put forward prior to any work being undertaken.

### Is the contractor required to fit in to an existing structured team?

Unless the contractor possesses undoubted exemplary skills - it can be a tall order to bring in someone new to an existing management team when they neither know (a) how the business works, (b) nor the teams within the business whom they are expected to manage. In addition, the people within those teams will be familiar and accustomed to the company, therefore, may be better suited to making critical judgement calls. Depending on the agreed duration of the contract, have you factored in the initial outlay for the 'bedding-in' period when the contractor familiarizes themselves with your organization's infrastructure?

### What knowledge will the contractor take away once the project is complete?

In relation to accountability, the [managed service provider](#) will likely have a higher degree of responsibility to ensure that the knowledge is retained and documented within its standard business processes. With regards to the contractor, you will be reliant on enforcing this responsibility.

### What documentation is required during, and post project?

To ensure the work done can be picked up by somebody else and supported in an ongoing manner, documentation needs to be a key consideration such as project plans, configuration information, run books, normal documentation projects like RAID logs, lessons learned, outstanding issues etc.

### What happens if the contractor leaves midway through the project?

There is no guarantee at the end of the contract period that all the objectives will be met, or the contractor will not leave midway through the project. There is often very little in the way of loyalty to contracting, so it is essential to reduce the risk you are exposed to. A key consideration here is ensuring all the work is documented as point 8 above so that if the worst happens, all the knowledge doesn't leave with the contractor. Also, the resource needs to be correctly managed throughout the lifecycle to ensure there are no surprises and you can plan accordingly.

There is a limited risk with a managed service provider as they will have a wider pool of resource who can be brought in with very limited notice and impact on cost.

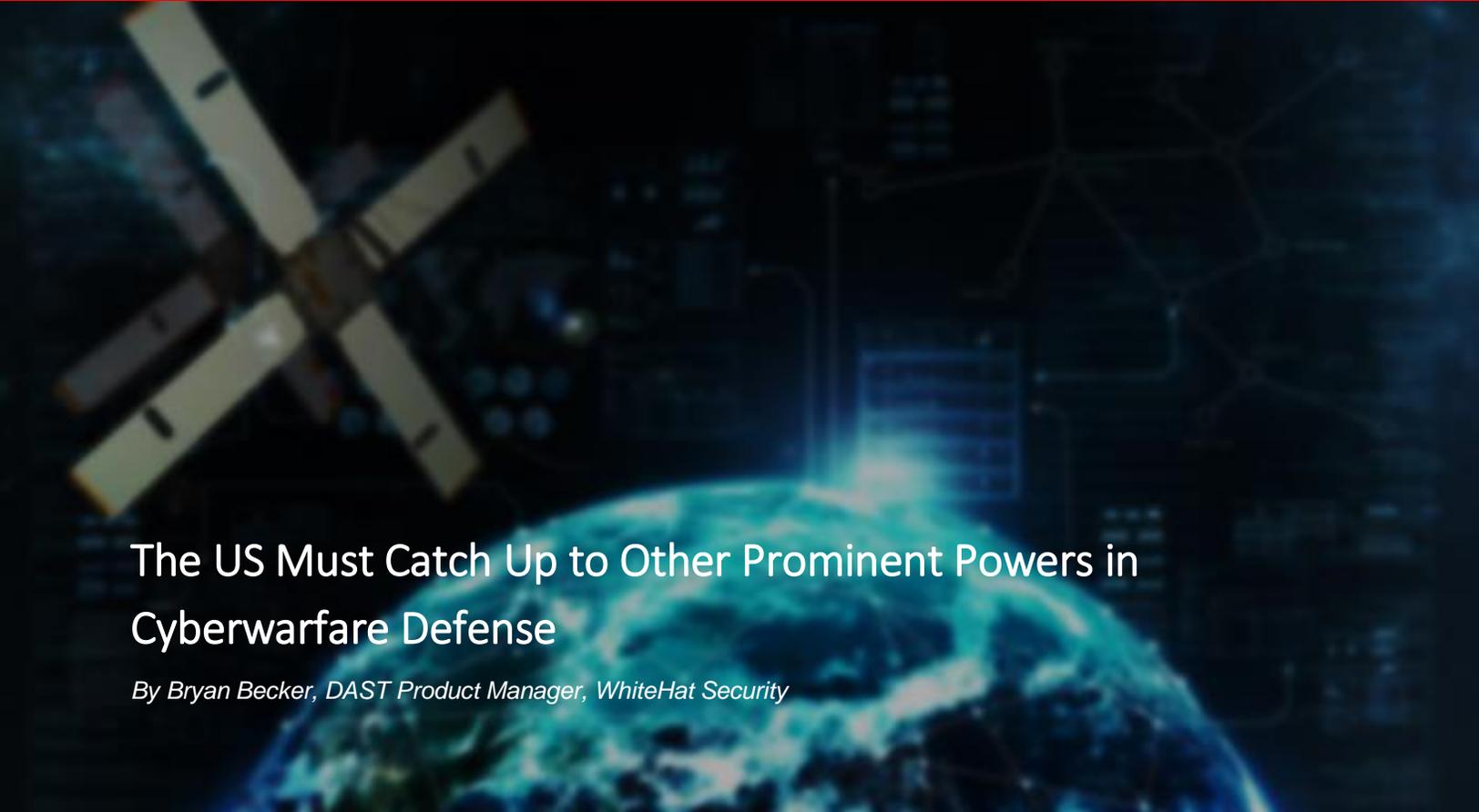
### How to build a strong working relationship with the contractor?

There is no substitute for time, and one great indicator to a strong relationship than consistency over time. Consistency in open communication, consistency in understanding of expectations from both sides and accountability in the delivery of all expectations. Human error is a growing but preventable issue with all the automation possibilities nowadays. Therefore, all manner of mistakes or misunderstandings can be forgiven so long as one has courage to admit their own and take ownership of them.

#### About the Author



Mitesh founded Fifosys, an [IT Support Company in London](https://www.fifosys.com/), in 2001 following completion of a master's in computer science. He has a reputation for straight talking, delivering focused and effective directives to his clients. Mitesh has an in-depth understanding of both operational and transformational IT projects and leads the business strategy at Fifosys. He also acts as a mentor, guiding junior aspirants commencing their business career. Mitesh can be reached online at <https://www.linkedin.com/in/miteshrpatel/> and at our company website <https://www.fifosys.com/>



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

By Bryan Becker, DAST Product Manager, WhiteHat 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 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.

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 WhiteHat Security. Bryan has been working in application development and security since the startup scene in 2003. Before working at WhiteHat 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.

# RANSOMWARE



## Operation Eligible Receiver 97's Impact on Ransomware

In 1997, the NSA conducted an organized attack on the Department of Defense's critical information systems, an exercise named Operation Eligible Receiver 97 (ER 97). Throughout the exercise, the NSA gained super user access to high-priority devices and compromised almost all of their primary targets.

During the exercise, one of the only recorded instances of breach prevention occurred when an anonymous marine noticed suspicious activity on the network and immediately made configuration changes to only allow essential connections. This visibility into anomalous activity, partnered with proper configuration management, proved to be essential and was ultimately implemented into today's security frameworks.

Operation Eligible Receiver 97 provided the blueprint for a strong cybersecurity posture and preventing breaches; however, many organizations still struggle to comply with these frameworks today, which ultimately leads to Ransomware attacks. Although there are countless unique instances of Ransomware, the attack vectors used today remain the same as those used in ER 97 by the NSA.

### Attack Vectors

Ransomware will commonly use emails, downloads, compromised software, or malicious websites in an attempt to gain access to administrative rights. This is done by exploiting misconfigurations, vulnerabilities, or socially engineering users with elevated rights assignments.

The ability to debug programs, seen as "SE\_DEBUG", is one of the rights assignments that Ransomware programs use to hash the Security Account Manager database and capture login credentials. Typically,

SE\_DEBUG is set either by mistake or as a result of a vendor with broken services on install. This setting requires continuous monitoring, as it often changes unintentionally.

Similarly, Local Admin privileges also change unintentionally. These privileges are designed to only be distributed to users in accordance with organizational missions and business functions. NIST 800-53 defines this principle as “least privilege” seen in control AC-6; however, misconfigurations and configuration drift will cause Local Admin privileges to be granted unnecessarily. These unnecessary Local Admin privileges increase the likelihood of Ransomware entering via social engineering.

Social engineering occurs when individuals hoping to introduce Ransomware into organizations attempt to manipulate a large group of users into revealing confidential information. Though a large body of users is targeted, it only takes one user with unnecessarily elevated privileges and the belief of “why would anyone attack me” to click on a malicious link and introduce a Ransomware attack.<sup>23</sup>

## Frameworks as a Guideline

Numerous security frameworks have outlined specific controls to guard against these attack vectors:

### NIST800-53

AT-2 (Awareness Training) - Practical exercise may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks or malicious web links.

AT-3 (Role-Based Training) - A well-trained workforce provides another organizational safeguard that can be employed as part of a defense-in-depth strategy, in which organizations would be protected against incoming malicious code via email or web applications.

IR-6 (Incident Reporting) - Incident reporting addresses both specific incident reporting requirements for an organization and within the organization itself. For instance, suspected security incidents may include the receipt of suspicious email communications that can potentially contain malicious code.

CM-1 (Configuration Management Policy and Procedures) - An additional method of guarding against attack vectors is establishing and distributing a configuration management policy in order to address purpose, scope, roles, responsibility, and coordination among organizational entities and compliance.

---

<sup>23</sup> <https://www.sans.org/reading-room/whitepapers/riskmanagement/securing-common-vectors-cyber-attacks-37995>

CM-3 (Configuration Change Control) - Configuration Change Control determines which types of changes to the system that are configuration-controlled and reviews these proposed system changes. In turn, the proposed changes are approved or disapproved with explicit consideration for security impact analysis.

CM-7 (Least Functionality) - The Least Functionality Control configures the system to provide only essential capabilities and to prohibit or restrict the use of the following functions: ports, protocols, and/or services.<sup>24</sup>

### CISControls™

(4) Controlled Use of Administrative Privileges - Users with administrative account access are required to use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities. Systems must be configured to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

(5) Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers - All authorized systems and software have documented, standard security configuration standards. Additionally, a Security Content Automation Protocol (SCAP) compliant configuration monitoring system is utilized to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

(7) Email and Web Browser Protections - Protections that ensure that only fully supported web browsers and email clients are allowed to execute in the organizations, ideally only using the latest version of the browsers and email clients provided by the vendor. In order to reduce the likelihood of spoofed or modified emails from valid domains, implement Domain-based Message Authentication and Reporting and Conformance (DMARC) policy and verification, beginning with the Sender Policy Framework (SPF) and the Domain Keys Identified Mail (DKIM) standards.

(9) Boundary Defense - Boundary defenses deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries. These defenses also deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.

---

<sup>24</sup> <https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf>

(17) Implement a Security Awareness and Training Program - A Security Awareness and Training Program first begins with a skills gap analysis to understand the skill and behaviors workforce members are not adhering to. Then, using this information, the program builds a baseline education roadmap and trains the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.

(19) Incident Response and Management - Written incident response plans define roles of personnel and phases of incident handling/management, as well as detail information on third-party contact information. These third-parties include Law Enforcement, relevant government departments, vendors, and ISAC partners.<sup>25</sup>

Ransomware exploiting misconfigurations in order to target user accounts with elevated privileges represents a huge potential risk for organizations and security teams. User privileges are essential for organizations to manage, but when done manually, they are nearly impossible to manage efficiently.

## Overcoming Obstacles

The current practices for managing account privileges are extremely time-consuming and lack the details that a next-generation security solution can offer.

One current method for privileged account management is to use group policy to examine user rights. This requires security teams to spend countless hours individually examining rights assigned to each user on each machine. On top of not being time-effective, using group policy will not show the history of changes made or validate if planned changes were applied properly.

Using a SIEM to analyze logs creates similar problems. For example, the task of finding users with Debug Privileges would require a security team to first write a PowerShell script and then convert the results into a text file. This process shows results for only a static point in time and will not be able to show any changes unless the script is run regularly and the results are compared each time. Tools like SIEMs have great uses for IT, but when repurposed for security, these become overly time-consuming and fail to achieve the same results as a next-generation security solution.

---

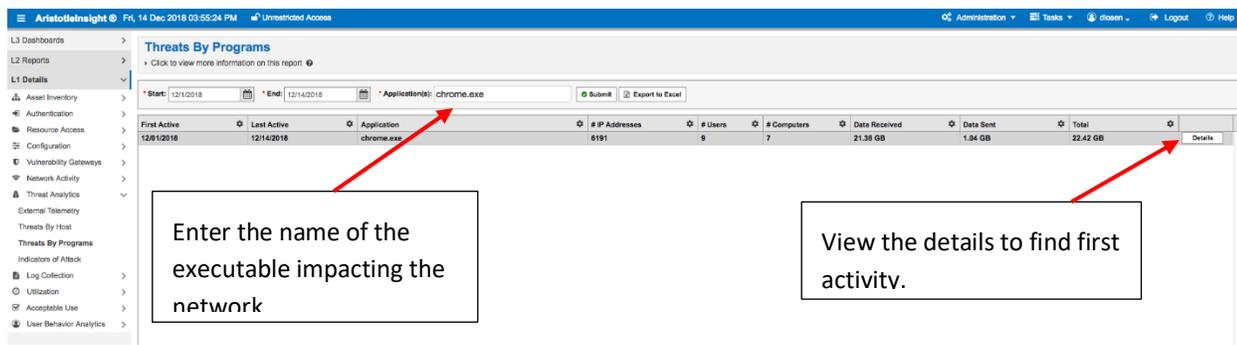
<sup>25</sup> <https://www.cisecurity.org/controls/>



The User Privileges Report in AristotleInsight lists all user privileges across all domains or only specified domains. The report may be filtered by a specific user and/or computer.

AristotleInsight includes the unique and revolutionary ability to track ransomware back to ground zero. The system provides advanced cybersecurity professionals with the metrics to determine exactly when Ransomware first entered the network and what threat vector it entered through.

### 1.) Tracking the Executable



Visiting the L1 Threats by Program page will allow security teams to search for the exact executable used by whatever ransomware is impacting the environment.

## 2.) Finding the Source

Sort activity by First Active to see when an executable first ran.

Use More Info to view the specific user and device impacted.

First Active	Last Active	IP Address	Hostname	Received	Sent	Total	# Users	# Computers	Application	More Info
12/01/2018 12:06	12/14/2018 01:56...	172.217.8.174	N/A	9.27 MB	8.87 MB	18.14 MB	8	7	chrome.exe	More Info
12/01/2018 12:06	12/14/2018 03:23...	172.217.8.170	N/A	9.88 MB	10.79 MB	20.67 MB	7	7	chrome.exe	More Info
12/01/2018 12:05	12/14/2018 03:52...	172.217.8.99	N/A	5.07 MB	2.08 MB	7.15 MB	8	7	chrome.exe	More Info
12/01/2018 12:04	12/14/2018 10:17...	172.217.8.106	N/A	2.38 MB	717.17 KB	3.09 MB	8	7	chrome.exe	More Info
12/01/2018 12:05	12/14/2018 03:11...	173.194.74.188	N/A	1.3 MB	269.52 KB	1.57 MB	5	5	chrome.exe	More Info
12/01/2018 12:09	12/14/2018 02:52...	172.217.8.170	N/A	2.02 MB	797.56 KB	2.79 MB	8	7	chrome.exe	More Info
12/01/2018 12:09	12/14/2018 03:54...	8.39.55.162	N/A	5.70 MB	5.4 MB	11.19 MB	4	4	chrome.exe	More Info
				762.75 KB	150.89 KB					More Info
				1.1 MB	226.52 KB					More Info
				2.85 MB	544.28 KB					More Info
				3.19 MB	1.36 MB					More Info
				3.19 MB	646.15 KB					More Info
				1.21 MB	252.65 KB					More Info
				3.1 MB	617.28 KB					More Info
				1.31 MB	201.38 KB					More Info
				1.69 MB	216.95 KB					More Info
				524.22 KB	180.91 KB					More Info
				655.82 KB	130.85 KB	786.67 KB	5	5	chrome.exe	More Info
12/01/2018 01:27	12/14/2018 01:00...	64.233.181.188	N/A	1.42 MB	275.5 KB	1.69 MB	5	5	chrome.exe	More Info
12/01/2018 01:31	12/14/2018 03:04...	173.194.192.188	N/A	1.41 MB	275.08 KB	1.68 MB	5	5	chrome.exe	More Info
12/01/2018 01:43	12/14/2018 12:06...	209.85.147.188	N/A	1.29 MB	256.27 KB	1.54 MB	5	5	chrome.exe	More Info
12/01/2018 02:17	12/14/2018 01:43...	74.125.70.188	N/A	990.62 KB	190.7 KB	1.19 MB	5	5	chrome.exe	More Info
12/01/2018 02:35	12/14/2018 10:53...	173.194.197.188	N/A	1.33 MB	209.19 KB	1.59 MB	5	5	chrome.exe	More Info
12/01/2018 02:36	12/14/2018 09:41...	74.125.201.188	N/A	108.01 KB	59.22 KB	167.23 KB	3	3	chrome.exe	More Info
12/01/2018 02:50	12/13/2018 07:43...	172.217.8.107	N/A	858.36 KB	165.52 KB	1023.87 KB	5	5	chrome.exe	More Info
12/01/2018 03:15	12/14/2018 03:17...	108.177.120.188	N/A	426.11 KB	186.39 KB	612.49 KB	4	4	chrome.exe	More Info
12/01/2018 05:20	12/10/2018 02:10...	74.125.89.189	N/A	985.94 KB	198.59 KB	1.16 MB	5	5	chrome.exe	More Info
12/01/2018 05:30	12/14/2018 01:12...	173.194.198.188	N/A	3.44 KB	1.75 KB	5.2 KB	1	1	chrome.exe	More Info
12/01/2018 05:42	12/01/2018 05:46...	74.125.89.95	N/A	24.41 KB	14.02 KB	38.43 KB	3	3	chrome.exe	More Info
12/01/2018 05:50	12/10/2018 11:05...	172.217.8.171	N/A	48.19 MB	5.24 MB	54.43 MB	7	7	chrome.exe	More Info
12/01/2018 06:11	12/14/2018 02:56...	172.217.8.110	N/A	1.23 MB	671.53 KB	1.79 MB	4	4	chrome.exe	More Info
12/01/2018 06:20	12/14/2018 03:54...	74.125.124.189	N/A	746.5 KB	143.05 KB	889.55 KB	5	5	chrome.exe	More Info
12/01/2018 06:20	12/14/2018 03:46...	74.125.129.188	N/A	7.41 KB	1.51 KB	8.92 KB	1	1	chrome.exe	More Info
12/01/2018 06:43	12/01/2018 06:46...	173.194.198.94	N/A							More Info

Sorting the details by First Active will show the first instance of activity from whatever executable is being used by the Ransomware. Clicking the 'More Info' button will show the username and device the executable impacted.

### 3.) Finding the Cause

The screenshot shows the 'Drilldown Report' interface in Aristotlenight. The table below represents the data shown in the report:

Start	Stop	Computer	User	Application	Title	URL	Total Time
12/03/2018 07:40:10	12/03/2018 07:40:15	sgtisuport-win7	herman	Windows Explorer		N/A	00:00:05
12/03/2018 07:40:16	12/03/2018 07:40:21	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:05
12/03/2018 07:40:21	12/03/2018 07:40:26	sgtisuport-win7	herman	Zoho Support Base3	sergeant laboratories - google chrome	https://support.zoho.com/support/gfaba/ShowHom...	00:00:05
12/03/2018 07:40:27	12/03/2018 07:40:32	sgtisuport-win7	herman	Update Server 113	sergeant laboratories - update server - google chrome	https://192.168.168.113/Admin/Information/	00:00:05
12/03/2018 07:40:33	12/03/2018 07:40:38	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:05
12/03/2018 07:41:20	12/03/2018 07:41:25	sgtisuport-win7	herman	Update Server 113	new tab - google chrome	https://192.168.168.113	00:00:05
12/03/2018 07:41:26	12/03/2018 07:41:32	sgtisuport-win7	herman	Update Server 113	aristotlenight™ login - google chrome	https://192.168.168.113	00:00:10
12/03/2018 07:41:36	12/03/2018 07:41:43	sgtisuport-win7	herman	Google Chrome	new tab - google chrome	N/A	00:00:05
12/03/2018 07:41:44	12/03/2018 07:41:49	sgtisuport-win7	herman	Zoho Support Base5	sergeant laboratories - google chrome	https://support.zoho.com/support/gfaba/ShowHom...	00:00:05
12/03/2018 07:41:50	12/03/2018 07:41:56	sgtisuport-win7	herman	Google Chrome	new tab - google chrome	N/A	00:00:05
12/03/2018 07:41:56	12/03/2018 07:42:24	sgtisuport-win7	herman	Google Calendar	google calendar - week of december 3, 2018 - google chrome	https://calendar.google.com/calendar/	00:00:30
12/03/2018 07:42:30	12/03/2018 07:42:35	sgtisuport-win7	herman	Google Chrome	new tab - google chrome	N/A	00:00:05
12/03/2018 07:42:36	12/03/2018 07:43:37	sgtisuport-win7	herman	Dropbox	files - dropbox - google chrome	https://www.dropbox.com/home	00:00:10
12/03/2018 07:45:49	12/03/2018 07:45:54	sgtisuport-win7	herman	Windows Explorer		N/A	00:00:05
12/03/2018 07:45:55	12/03/2018 07:46:28	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:30
12/03/2018 07:46:34	12/03/2018 07:46:39	sgtisuport-win7	herman	Microsoft Outlook	[a] os remote login - message (html)	N/A	00:00:05
12/03/2018 07:46:39	12/03/2018 07:46:44	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:05
12/03/2018 07:46:44	12/03/2018 07:46:49	sgtisuport-win7	herman	Microsoft Outlook	ms weekly support numbers & demos - 11/26-11/30 - message (html)	N/A	00:00:05
12/03/2018 07:46:49	12/03/2018 07:46:54	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:05
12/03/2018 07:46:54	12/03/2018 07:46:59	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:05
12/03/2018 07:46:59	12/03/2018 07:47:04	sgtisuport-win7	herman	Microsoft Outlook	[a] os remote login - message (html)	N/A	00:00:05
12/03/2018 07:47:04	12/03/2018 07:47:09	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:05
12/03/2018 07:47:09	12/03/2018 07:47:14	sgtisuport-win7	herman	Microsoft Outlook	deleted items - personal folders - outlook	N/A	00:00:05
12/03/2018 07:47:14	12/03/2018 07:47:19	sgtisuport-win7	herman	Microsoft Outlook	deleted items - personal folders - outlook	N/A	00:00:05
12/03/2018 07:47:19	12/03/2018 07:47:24	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:05
12/03/2018 07:47:24	12/03/2018 07:47:29	sgtisuport-win7	herman	Microsoft Outlook	[a] os admin report - message (html)	N/A	00:00:15
12/03/2018 07:47:29	12/03/2018 07:47:34	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:10
12/03/2018 07:47:34	12/03/2018 07:47:39	sgtisuport-win7	herman	Microsoft Outlook	[a] admin report 16 - message (html)	N/A	00:00:05
12/03/2018 07:47:39	12/03/2018 07:47:44	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:10
12/03/2018 07:53:02	12/03/2018 07:53:07	sgtisuport-win7	herman	Microsoft Outlook	[a] os remote login - message (html)	N/A	00:00:05
12/03/2018 07:53:07	12/03/2018 07:53:12	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:20
12/03/2018 07:53:29	12/03/2018 07:53:34	sgtisuport-win7	herman	Microsoft Outlook	[a] os remote login - message (html)	N/A	00:00:05
12/03/2018 07:53:35	12/03/2018 07:54:08	sgtisuport-win7	herman	Microsoft Outlook	inbox - personal folders - outlook	N/A	00:00:35
12/03/2018 07:54:14	12/03/2018 07:54:25	sgtisuport-win7	herman	Microsoft Outlook	rescheduled: aristotlenight - deep dive with ledan masseus on december 3, 2018 - message (html)	N/A	00:00:15
12/03/2018 07:54:30	12/03/2018 07:54:35	sgtisuport-win7	herman	Dropbox	files - dropbox - google chrome	https://www.dropbox.com/home	00:00:05
12/03/2018 07:54:37	12/03/2018 07:54:42	sgtisuport-win7	herman	Google Chrome	new tab - google chrome	https://www.maspethfederal.com/about/locations/	00:00:05
12/03/2018 07:54:42	12/03/2018 07:55:22	sgtisuport-win7	herman	Search Engine	maspeth federal savings and loan association - google search - google chrome	https://www.google.com/search?q=maspeth+federal...	00:00:05
12/03/2018 07:54:48	12/03/2018 07:55:22	sgtisuport-win7	herman	Google Chrome	about us   maspeth federal savings bank - google chrome	https://www.maspethfederal.com/about/	00:00:30
12/03/2018 07:55:27	12/03/2018 07:59:39	sgtisuport-win7	herman	Google Chrome	hours & locations   maspeth federal savings bank - google chrome	https://www.maspethfederal.com/about/locations/	00:00:15
12/03/2018 07:55:44	12/03/2018 07:55:50	sgtisuport-win7	herman	Microsoft Outlook	rescheduled: aristotlenight - deep dive with ledan masseus on december 3, 2018 - message (html)	N/A	00:00:10
12/03/2018 07:55:55	12/03/2018 07:56:00	sgtisuport-win7	herman	Windows Explorer		N/A	00:00:05
12/03/2018 07:56:01	12/03/2018 07:56:06	sgtisuport-win7	herman	Google Calendar	google calendar - week of december 3, 2018 - google chrome	https://calendar.google.com/calendar/	00:00:30
12/03/2018 07:56:25	12/03/2018 07:56:30	sgtisuport-win7	herman	Microsoft Outlook	[a] os apt alert - message (html)	N/A	00:00:15

The L1 Drilldown Report will show timestamped activity that can be matched to the initial executable activity seen in the Threats by Program Report. Finally, the Daily Bandwidth Report (shown below) is used to validate what connections were made as a result of the activity.

**AristotleInsight** | Fri, 14 Dec 2018 04:39:01 PM | Unrestricted Access | Administration | Tasks | Logout | Help

**Daily Bandwidth Report**

Start: 12/1/2018 | End: 12/3/2018 | Type: Computer | sgtsupport-win7 | Submit | Export to Excel

Timestamp	Username	Computer	Application	IP Address	Hostname	Received	Sent	Total
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	74.125.69.188	sg-in-F188.1e100.net	97 KB	19.83 KB	116.83 KB
12/01/2018	NETWORK	sgtsupport-win7	c:\windows\system32\svchost.exe	192.168.188.23	N/A	962.15 KB	260 B	962.42 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	172.217.6.110	ord37603-in-f14.1e100.net	311.47 KB	387.07 KB	698.54 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	192.168.188.10	N/A	787.49 KB	815.53 KB	1.55 MB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	108.177.112.189	N/A	148.56 KB	83.5 KB	233.06 KB
12/01/2018	LOCAL_SYSTEM	sgtsupport-win7	system	192.168.188.23	N/A	62.65 KB	150.83 KB	213.48 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Microsoft Office\...	52.114.132.23	N/A	333.85 KB	156.57 KB	490.22 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	162.125.18.133	N/A	622.17 KB	784.15 KB	1.37 MB
12/01/2018	LOCAL_SYSTEM	sgtsupport-win7	system	192.168.255.255	N/A	53.89 KB	53.89 KB	107.77 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	192.29.293.126	N/A	43.93 KB	49.15 KB	92.88 KB
12/01/2018	LOCAL_SYSTEM	sgtsupport-win7	c:\windows\system32\svchost.exe	52.173.24.17	N/A	15.54 KB	9.6 KB	25.14 KB
12/01/2018	NETWORK	sgtsupport-win7	c:\windows\system32\svchost.exe	71.10.216.1	ma01.charter.com	5.1 KB	0 B	5.1 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Sergeant Laborator...	192.168.188.10	N/A	51.43 KB	731.29 KB	782.72 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Users\herman\AppData\Local...	34.195.198.96	ec2-34-195-198-96.compute-1.amazonaws.com	410.92 KB	173.15 KB	584.07 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	172.217.174.174	ord37608-in-f14.1e100.net	286.79 KB	371.69 KB	658.44 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	192.168.200.188	ju-in-F188.1e100.net	96.92 KB	19.83 KB	116.74 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	172.217.111.188	N/A	178.04 KB	36.35 KB	214.4 KB
12/01/2018	LOCAL_SYSTEM	sgtsupport-win7	system	192.168.188.10	N/A	187.82 KB	117.54 KB	305.36 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	192.168.188.10	N/A	915.1 KB	96.51 KB	1011.61 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	172.217.174.174	ord37608-in-f14.1e100.net	173.97 KB	162.51 KB	336.49 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	192.168.188.10	N/A	412.61 KB	1.08 MB	1.48 MB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	192.168.188.10	N/A	32.17 KB	91.38 KB	123.55 KB
12/01/2018	NETWORK	sgtsupport-win7	c:\windows\system32\svchost.exe	192.168.188.10	N/A	323.12 KB	607.52 KB	930.64 KB
12/01/2018	NETWORK_SERVICE	sgtsupport-win7	c:\windows\system32\svchost.exe	192.168.188.10	N/A	195.23 KB	238.13 KB	433.36 KB
12/01/2018	LOCAL_SYSTEM	sgtsupport-win7	c:\program files\sergeant laboratories\...	8.29.29.188	ju-in-F188.1e100.net	84.29 KB	3.69 MB	3.78 MB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	52.173.24.17	N/A	7.2 MB	1.69 MB	9.09 MB
12/01/2018	LOCAL_SYSTEM	sgtsupport-win7	c:\windows\system32\svchost.exe	192.168.188.10	N/A	1.37 MB	136.56 KB	1.51 MB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	192.168.188.10	N/A	48.43 KB	9.95 KB	58.38 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Microsoft Office\...	172.217.174.174	ord37608-in-f14.1e100.net	1.06 MB	110.77 KB	1.17 MB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Sergeant Laborator...	192.168.188.172	AristotleN7	31.71 KB	253.45 KB	285.16 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Microsoft Office\...	192.201.158.97	pl0rmap08-w01.prd.pho.secureserver.net	547.97 KB	97.88 KB	645.85 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	172.217.6.106	ord37603-in-f10.1e100.net	44.68 KB	17.57 KB	62.23 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	172.217.6.99	ord37603-in-f3.1e100.net	17.24 KB	12.37 KB	29.62 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	8.29.29.188	N/A	185.13 KB	170.91 KB	356.04 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	13.107.3.138	N/A	179.88 KB	28.55 KB	208.43 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	c:\program files\windowsapps\microsoft.windows.photos_2...	64.4.54.253	N/A	28.37 KB	6.25 KB	34.62 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Google\Chrome...	209.85.234.188	ju-in-F188.1e100.net	32.29 KB	6.61 KB	38.9 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Windows\System32\background...	204.79.197.200	a-0001.a-msedge.net	30.16 KB	9.69 KB	39.86 KB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	Device\HarddiskVolume1\Program Files\Microsoft Office\...	173.201.192.158	ip-173-201-192-158.ip.secureserver.net	1.28 MB	130.36 KB	1.4 MB
12/01/2018	sgtsupport-win7herman	sgtsupport-win7	c:\program files\windowsapps\microsoft.windows.photos_2...	13.107.5.89	N/A	543.18 KB	114.84 KB	658 KB
12/01/2018	LOCAL_SYSTEM	sgtsupport-win7	c:\windows\system32\svchost.exe	97.74.135.10	ip-97-74-135-10.ip.secureserver.net	4.66 MB	133.45 KB	4.79 MB
12/01/2018	LOCAL_SYSTEM	sgtsupport-win7	c:\windows\system32\svchost.exe	67.114.130.31	N/A	11.41 KB	7.44 KB	18.85 KB

What connections were made as a result of the activity.

Page 1 of 6 | Loading Complete | 1 - 100 of 561 items

Throughout the duration of Operation Eligible Receiver 97, the ability to spot anomalous activity proved to be one of the only successful defense measures against breaches. Today, based on the results of this exercise, Aristotle Insight brings anomalous activity detection to a new level and gives organizations the ability to immediately identify threats and respond accordingly.

## 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.

## 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



# 9 Ways to Safeguard Privileged User Accounts and Protect Your Business

By Anusha K. Muralidharan, Product Consultant, ManageEngine

At Gartner's Security and Risk Management Summit in June 2019, the top 10 security projects that chief information security officers (CISOs) should concentrate on were laid out. Once again, privileged access management (PAM) was identified as the most significant.

Despite these steady reminders, many privileged accounts still remain poorly protected, ignored or mismanaged — making them easy targets. With that in mind, here's a list of essentials policies that every IT manager or security administrator should implement to protect privileged accounts:

## 1. Track and consolidate each privileged account with an automated discovery mechanism.

The first step to secure and manage your organization's privileged accounts is to discover all critical assets on your corporate network as well as the associated accounts and credentials. As your organization grows and expands its infrastructure, you should ensure that your IT team is equipped with a strong discovery mechanism to tackle the proliferation of privileged accounts and keep track of them. Running a fully automated program that regularly scans your network, detects new accounts, and adds them to a central database is the best way to build a strong foundation for your PAM strategy.

## 2. Store privileged accounts in a secure, centralized vault.

Do away with localized, soloed databases that are often maintained by various teams. More importantly, make sure employees stop writing down passwords on sticky notes or storing passwords in plain text files. These practices are dangerous and lead to increased instances of outdated passwords and coordination issues, resulting in operational inefficiency. Instead, privileged accounts and credentials belonging to all departments should be cataloged into one centralized repository. Further, protect your

stored privileged accounts with well-known encryption algorithms, such as AES-256, to protect against unwanted access.

### **3. Establish clearer roles with limited access privileges.**

Once your organization's privileged accounts are securely locked in a vault, it's time to decide who should have the keys. As the Advanced Cyber Security Center (ACSC) states, "restrict administrative privileges to operating systems and applications based on user duties." You can do this by charting clear roles for the members of your IT team and making sure that privileged accounts are not used for routine tasks such as reading email or web browsing — and that each member's role gives them only the minimum required access privileges.

### **4. Implement multifactor authentication for employees and third parties.**

According to Symantec's 2016 Internet Security Threat Report, 80 percent of breaches can be prevented by using multifactor authentication. Implementing two-factor or multifactor authentication for both PAM administrators and end users will guarantee that only the right people have access to sensitive resources.

### **5. Stop sharing privileged account credentials in plain text.**

Beyond eliminating security vulnerabilities related to loose role division, it's also important to implement secure sharing practices. For ultimate protection, your organization's PAM administrator should be able to provide employees or contractors access to IT assets without disclosing the credentials in plain text. Users should instead be allowed to launch one-click connections to target devices from the PAM tool's interface, without viewing or manually entering the credentials.

### **6. Enforce strict policies for automatic password resets.**

Convenient as it may be for IT teams to use the same password for every privileged account on the network, this is an unhealthy practice that ultimately fosters a fundamentally insecure environment. Secure management of privileged accounts requires the use of strong, unique passwords that are periodically reset. You should make automatic password resets an integral part of your PAM strategy to eliminate unchanged passwords and protect sensitive resources from unauthorized access.

## 7. Add release controls for password retrieval.

Establish a policy that forces users to send a request to your organization's PAM administrator whenever they require specific account credentials to access a remote asset. To further reinforce control, provision users only with temporary, time-based access to these credentials, with built-in options to revoke access and forcefully check in passwords when the stipulated time expires. For further security, you can also automatically reset passwords once users check them in.

## 8. Stop embedding credentials within script files.

Many applications require frequent access to databases and other applications to query business-related information. Organizations often automate this communication process by embedding the application credentials in clear text within configuration files and scripts, but it's hard for administrators to identify, change and manage these embedded passwords. As a result, the credentials are simply left unchanged to not hinder business productivity. Hard-coding credentials may make technicians' jobs easier, but they're also an easy launch point for hackers looking to make their way into an organization's network. Alternatively, your IT team can use secure APIs to allow applications to query your PAM tool directly when they need to retrieve privileged accounts for another application or a remote asset.

## 9. Audit everything.

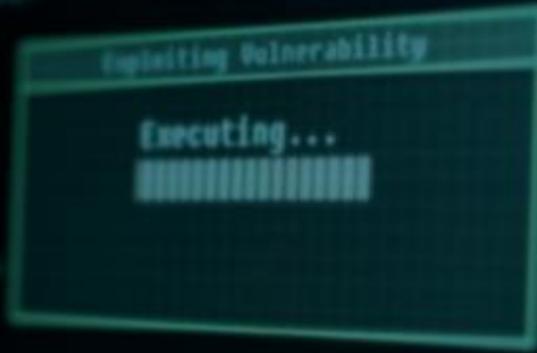
When it comes down to it, comprehensive audit records, real-time alerts, and notifications are really what make life easier. Capture every single user operation, and establish accountability and transparency for all PAM-related actions. An integration with an in-house event logging tool can also help by consolidating PAM activities with other events from the rest of your organization and providing intelligent tips about unusual activities. This proves extremely useful in acquiring a comprehensive overview of security events and detecting breaches or insider exploits.

Executing these nine policies isn't going to be an end-all solution to security — there's always more to be done. According to Verizon's 2019 Data Breach Investigation Report, of the 2,216 confirmed data breaches in 2017, 201 were due to privilege abuse. A statistic like that should highlight the importance of not only protecting privileged accounts but also recording and monitoring privileged sessions to stay vigilant and detect unusual access. Your privileged account management strategy should support your strategy to control privileged access to your critical assets, which should support your identity and access management plan, and so on. That's the best way to protect an organization; keep widening your boundaries and securing those boundaries, because the war against cybercriminals is unending.

## About the Author



Anusha Muralidharan is a product consultant at [ManageEngine](#), a division of [Zoho Corp.](#) For more information on ManageEngine, the real-time IT management company, please visit [www.manageengine.com](http://www.manageengine.com); follow the company blog at <http://blogs.manageengine.com>, and on LinkedIn at [www.linkedin.com/company/manageengine](http://www.linkedin.com/company/manageengine), Facebook at [www.facebook.com/ManageEngine](http://www.facebook.com/ManageEngine) and Twitter [@ManageEngine](#).



## Open-Source Code

*Quick Review of the “Flat map-stream” attack*

### THE SOCIAL ENGINEERING ATTACK

Recently, a malicious attacker socially engineered a developer and had acquired legitimate access to a popular JavaScript library and has inserted malware code that procures digital currency stowed away in certain particular digital wallets. The “ownership” of the package was mutually transferred to an unknown developer called “right9ctrl.” An npm package that has been downloaded 2 million times and is implemented by small start-ups and even Fortune 500 companies.

This attack started out as a social engineering attack. The attacker, posing as a maintainer, took over to maintain the event-stream module. This developer, “Right9ctrl” was able to develop the trust to gain access and ultimately acquire ownership by providing several contributions to the overall package. After eventually gaining full access to the source code he began his malicious intent.

### THE CODE ATTACK

The attacker began his malware journey in a two-step process in modifying event-stream. First, the version released for public consumption in September had been updated with a futile module known as “flat map-stream.” The malicious developer curated “event-stream” to hinge on the malicious code, “flat map-stream.” This section was precisely fashioned for the purposes of this attack. That bundle comprises a fairly meek index.js file, with the inclusion of a minified index.min.js file. The compound files on GitHub seem blameless enough. In the Second step, the user implemented an update in “flat map-stream” to include the payload that attempted to rob cryptocurrency wallets and send the balances to a server in Malaysia.

It zeroed in on a specific wallet to affect, Co-pay. This is a secure bitcoin wallet app for desktop and mobile apparatuses. This is known since the malevolent suite explicitly targets that application because the obscured code reads the “description” field from a project’s “package. Son file,” then implements that description to decrypt an **AES256** encrypted payload. At the onset of the code, the strings become decrypted implementing data from the consuming package. If it hits a dud, it would error out, but the mistake would be situated and disregarded.

## MITIGATION/PREVENTION MEASURES

It may well be enticing to bank on tools which scan npm packages by means of static analysis. This specific attack encrypts the malicious source code to avoid detection. To protect against such an attack a different approach or approaches must be implemented.

First, the developers in open source market must be aware of who they are handing over duties too. It is common practice to hand over source code as that is the nature of the code culture. However, this needs to be addressed to provide some form of a secure measure to make sure this social engineering attack is mitigated.

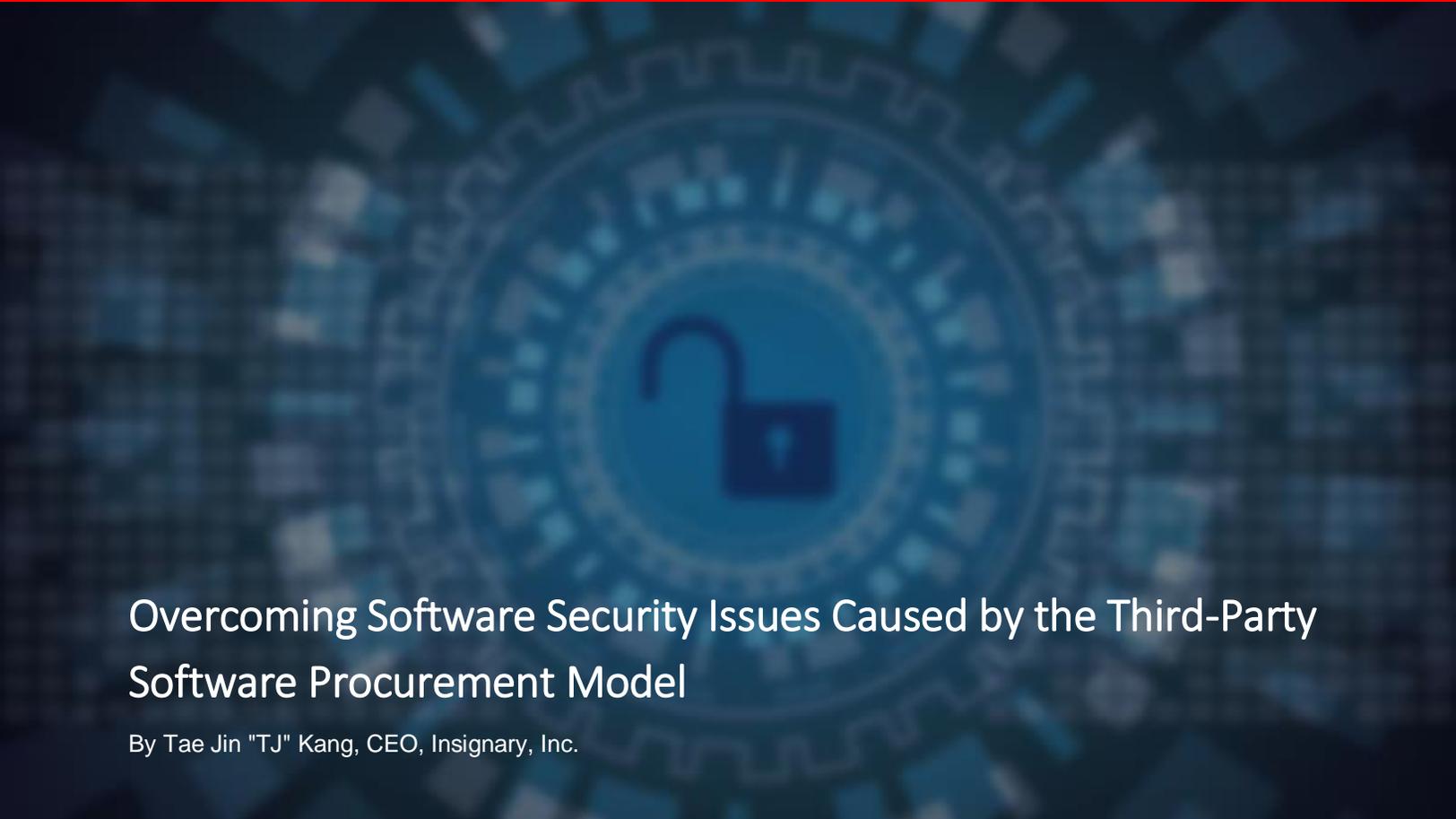
Second, JavaScript is prone to this kind of attack. One approach you may do to help defend it from routinely attacking you is implement a “lock file” so you’re not robotically installing the latest updates without even noticing it. Unfortunately, this also means you might not be up to date with the latest remedies for security vulnerabilities, so you will eventually have to do some risk assessment on your part.

Of course, this was eventually a foreseen security flaw. The “event-stream” attack won’t be the last, and it’s likely right now there are other bits of malicious code in wide use in existing npm packages/open-source code that have not been detected.

### About the Author



Joe Guerra, M.Ed, CySA+,C|EH, Cybersecurity Instructor, Hallmark University .Joe Guerra is a cybersecurity/computer programming instructor at Hallmark University. He has 12 years of teaching/training experience in software and information technology development. Joe has been involved in teaching information systems security and secure software development towards industry certifications. Initially, Joe was a software developer working in Java, PHP, and Python projects. He is constantly researching attack techniques, forensic investigations and malware analysis. He is focused on training the new generation of cyber first responders at Hallmark University.



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

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

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.

### 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.

## 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.

### About the Author



Tae Jin "TJ" Kang is a technology industry executive and entrepreneur. He is the president and CEO of Indignity. 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.

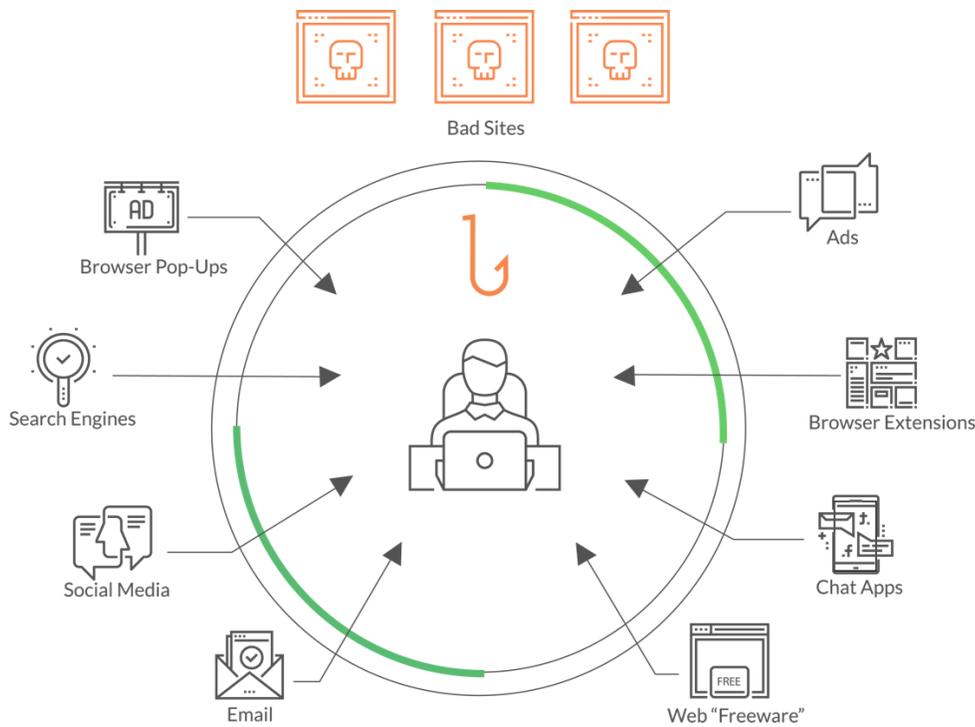


## Phishing in the Dark: Employee Security Gaps Are Growing

*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.



**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 [2019 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 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.



## Mid-Market Businesses, Don't Think Small about Security

By Jake Kiser, CEO, StrongKey

Whether in business or cybersecurity, it doesn't help small businesses to play small. When it comes to cybercrime, hackers don't discriminate - they see small businesses as easier targets, and rich sources of data ripe for the plucking. A report from Cisco found that 53 percent of mid-market businesses have experienced a breach, but you don't have to be part of that unlucky half.

Because mid-size companies are experiencing hacks just as often as large enterprises, they need a comparable level of security. While this has not always been financially feasible, the market is shifting, and the same tools available to the big fish can be easily implemented in smaller environments.

### Three Mid-Market Security Hurdles

Before considering your options, it's important to do your homework and consider the hurdles you most need to overcome.

The first one is the myth that your company is too small to be of interest to cybercriminals. While this contains an element of humility that you may want to project, it's a dangerous mindset—hackers know that mid-market companies often don't have the same financial and personnel resources for security that enterprises do, which makes an unprepared company a sitting duck.

The element of human error is another hurdle. Sure, it's good to train your employees on security best practices, but it's even better to put a security system in place so that when an employee eventually slips up, your data is still going to be protected. An employee slip-up is a matter of when, not if, and you want your data to remain protected.

Finally, in mid-sized organizations, resources are often thin and employees wear many hats. People often have to be both the CISO, responsible for mission-critical data security, and the IT Operations lead, responsible for almost anything IT under the sun. Cybersecurity often gets presented in confusing or convoluted ways that are meant for larger organizations, which means legitimately useful products and services do not always get adopted, and cybersecurity falls short. Sometimes, simpler is better.

## Four Security Recommendations

With these hurdles in mind, the recommendations below will improve cybersecurity and help decision-makers focus on solutions that provide the strongest protection.

### 1. Implement encryption.

Encryption scrambles data to make it unusable to hackers. It protects like no other security solution can, because even if intruders make it past your firewall, they will find only jumbled nonsense.

Encrypting critical data at the source is the strongest way to protect it. The source is the application that brings data in for the first time. Encrypt data here and ensure that only authorized applications may decrypt such data, using FIDO-based strong authentication.

Mid-market companies have traditionally not been able to afford encryption technology, but the market now offers affordable solutions that make enterprise-level encryption available to smaller organizations.

### 2. Get rid of passwords

Intended as a security measure, the age of passwords is ending. They are not only annoying to use, remember and change, but they are also not secure. In 2017, weak or re-used passwords were responsible for more than 80 percent of breaches. They are no longer safe and, in fact, have become the weakest link in data protection.

### 3. Lose the passwords, empower employees.

Easy, anywhere, 24-hour online access is now an expectation. Workers need solutions that enable them to do their jobs securely without constant frustration. There are frequent complaints of having to rely on one-time PINS sent over text, carrying an authentication device dedicated to just one service, or needing to use a personal cell phone.

However, convenience must be balanced with security. The FIDO Alliance and FIDO protocols are changing the nature of authentication by using standards to replace passwords. Replacing passwords means more security, and using standards means that the same protocol can be used across many websites and applications. FIDO can be implemented in ways that make sense to a business – physical USB authenticators, Bluetooth, NFC and more.

### 4. Find a security advisor.

IT security teams in mid-sized organizations should take advantage of the expertise of a trusted advisor or partner who knows the security space deeply. The market is full of conflicting information, and the security landscape shifts quickly. New vulnerabilities and new threats emerge all the time. Wading through this morass alone, in addition to all your other daily job duties, can prove difficult to impossible.

Look for a security advisor with a mindset focused on partnership, and walking through issues alongside their clients.

## Think Big

Malicious actors are in search of easy wins wherever they may be, and they know mid-sized companies are often rich targets. That's why these organizations are getting hit as often as large companies, and why they need the same level of protection. Keep these security hurdles in mind and use the recommendations above to access the tools and expertise you need to discourage attackers and keep data secure.

### About the Author



Jake Kiser is CEO of [StrongKey](#). He is responsible for the company's business strategy, overseeing the company's growth of its open-source cybersecurity solutions and a new product line which brings unprecedented security to small and medium enterprises. He has a diverse wealth of experience in building and executing growth strategies in both the corporate and non-profit world, including multinational clients across the United States and sub-Saharan Africa. He received his master's degree in business administration from Duke University and a bachelor's degree from the University of Maryland.



# 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



[www.connectidexpo.com](http://www.connectidexpo.com)



# 12TH OPERATIONAL ENERGY SUMMIT

January 28-30, 2019 | WASHINGTON D.C.

## WHY YOU CAN'T MISS OUT ON OPERATIONAL ENERGY SUMMIT 2019!

- Discover the military's operational energy priorities and its implications on the industry.
- Learn about the military's interest in intelligent grids to better inform your strategies
- Discuss DoD's initiatives for cutting operational energy waste and pitch solutions
- Build relationships with military and industry thought leaders to give your company an edge

## Executing Future Operational Energy Strategies

No Cost Passes Available  
For Active U.S. Military  
And Federal Government  
Employees





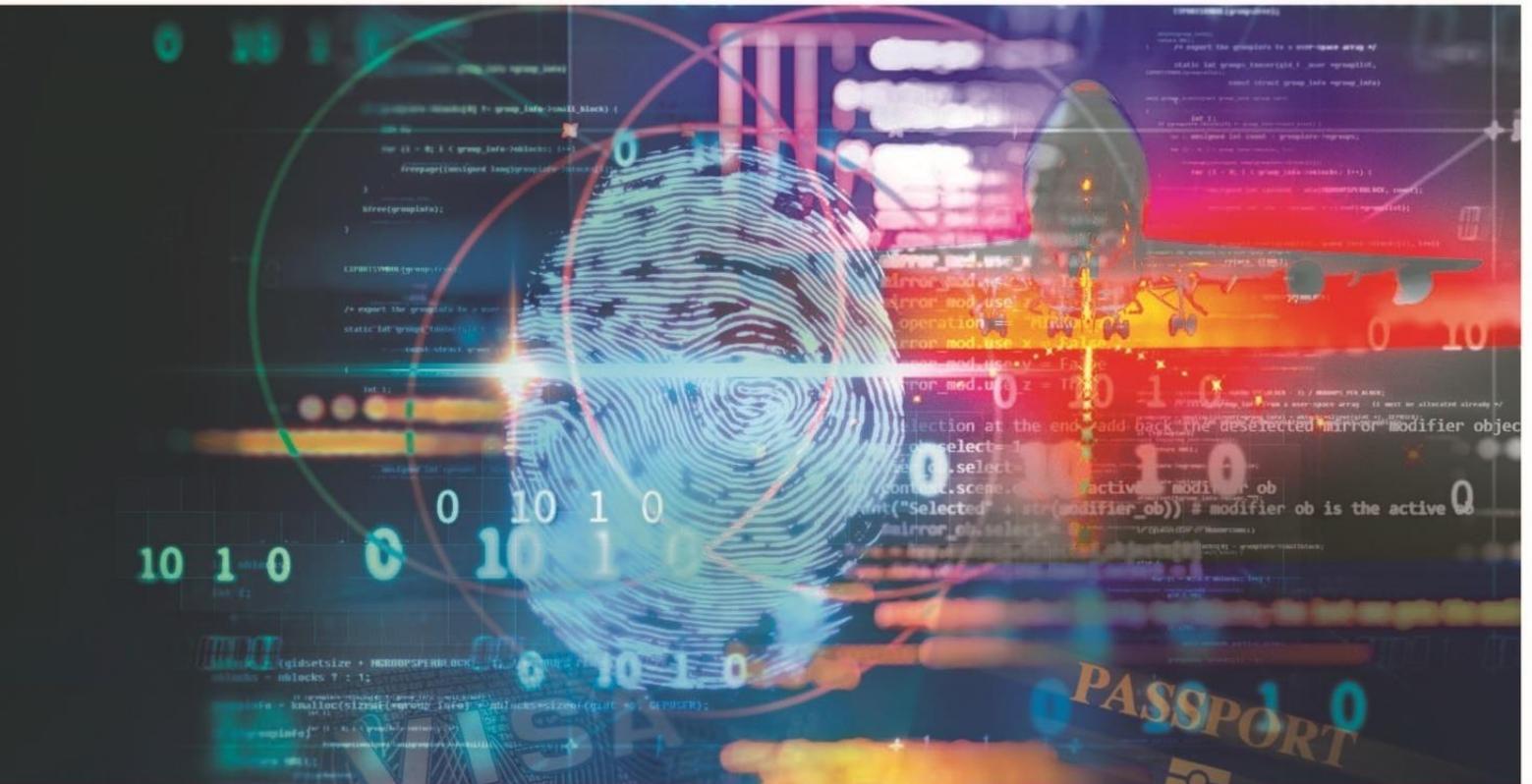
# IDENTITY WEEK

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



[www.terrappinn.com/identityweek](http://www.terrappinn.com/identityweek)



# IT SECURITY

8<sup>TH</sup> INTERNATIONAL INFORMATION  
& NETWORK SECURITY EXHIBITION



**OCTOBER 17<sup>TH</sup>-20<sup>TH</sup>, 2019**

Istanbul Expo Center (İFM) - Yesilkoy / Istanbul

[www.isaffuari.com](http://www.isaffuari.com)



[www.marmarafuar.com.tr](http://www.marmarafuar.com.tr) | Tel: +90 212 503 32 32 | [marmara@marmarafuar.com.tr](mailto:marmara@marmarafuar.com.tr)



BU FUAR 5174 SAYILI KANUN GEREĞİNCE TOBB (TÜRKİYE ODALAR VE BORSALAR BİRLİĞİ) DENETİMİNDE DÜZENLENMEKTEDİR.

# PUBLIC SAFETY INDONESIA

27 February - 1 March 2019

Jakarta Convention Center, Jakarta - Indonesia

Co-located with:

  
**Police Leadership**  
FORUM & CONGRESS 2019

Hosted by:



GET YOUR FREE  
PASS NOW!



## 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](http://publicsafetyindonesia.com)

Title Sponsor:



Platinum Sponsor:

**SAMSUNG**

Silver Sponsor:

**HIKVISION**

Supported By:



Media Partners:



Organised By:





# 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](http://CyberSummitUSA.com) »

**6 CPE CREDITS**

Full day attendance earns 6 credits following the Summit

### 2019 CYBER SECURITY SUMMITS

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

### 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 Or-  
ganizations 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:  
[BBrand@CyberSummitUSA.com](mailto:BBrand@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](http://www.futurecitiesshow.com)

# RSA<sup>®</sup>Conference2019

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 BAE Systems, Rapid7, Tripwire, 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 **Sylvia Acevedo**, Chief Executive Officer, Girl Scouts of the USA, **Megan Smith**, Chief Executive Officer, shift7, Third Chief Technology Officer of the United States (2014-2017); 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](http://www.rsaconference.com/cyberdefense-us19)

Follow us: #RSAC

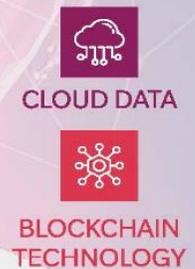




# DIGITALISING THE FUTURE

COMEX BUSINESS

## TRENDING FEATURES



## KEY INDUSTRIES

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



Supporter



Official Artificial Intelligence Sponsor



Lead Sponsor



Platinum Sponsor



Association Partners

**ASSUN MOTOR**



Representing the ecosystem of Internet - Bharat Model

Digital Media Partner



Media Partners

# Noord InfoSec Dialogue UK

26th & 27th February, 2019

The Bull, Gerrards Cross

**"The Noord Infosec Dialogue is very informative. It's useful to understand what others are experiencing in other industries and helps to validate our own efforts and challenges"**

IT Security,  
Virgin Atlantic Airways  
(Delegate)

**Register Your  
Place Now**



# **13<sup>th</sup> ITS EUROPEAN CONGRESS**

## **FULFILLING ITS PROMISES**

Brainport Eindhoven, the Netherlands | 3-6 June 2019



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

**IFSEC**  
INTERNATIONAL 18-20 JUNE 2019  
EXCEL LONDON UK

"40% MORE LEADS THIS YEAR  
THAN LAST. THE MEETINGS  
WITH VIPS HAVE BEEN SO  
BENEFICIAL, WITH QUALITY  
NAMES WHO ARE READY TO  
BUY, NOT JUST SPECULATE."

Managing Director, ZKTeco

SECURITY IS

# CRITICAL

**IFSEC IS ESSENTIAL**

**Position your brand at the centre of the critical security conversation. Be part of IFSEC 2019.**

Unique in attracting the entire security buying chain, IFSEC 2019 is your world-class, integrated security summit. Influence the innovation dialogue with over 27,000 global security integrators, installers, distributors, consultants and end users from over 117 countries – all under one roof.

- ▶ 43,461 Leads were generated onsite at IFSEC in 2018 – an average of 123 per exhibitor
- ▶ 34% of visitors had an annual purchasing budget of over £1,000,000
- ▶ Generate global business with quality buyers – Expand your business into high-growth markets around the world

Find out more at: [www.ifsec.events/international/exhibit](http://www.ifsec.events/international/exhibit)



**BOSCH**

Invented for life

Bosch and Genetec.  
End-to-end security,  
day after day

Find out more at [boschsecurity.com](https://www.boschsecurity.com)

# The 3<sup>rd</sup> 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](mailto: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](mailto:kvari@acieu.net)

# BAPCO

The Annual Event **2019**



12 - 13 MARCH 2019  
RICOH ARENA, COVENTRY

## TWO EVENTS ONE LOCATION

**REGISTER  
NOW**

[WWW.BAPCO-SHOW.CO.UK/REGISTER](http://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



**FREQUENTIS**

SILVER SPONSORS



@BAPCOEVENT  
@CRITCOMMSERIES



BAPCO ANNUAL CONFERENCE AND EXHIBITION  
TCCA CRITICAL COMMUNICATIONS SERIES



[WWW.BAPCO-SHOW.CO.UK](http://WWW.BAPCO-SHOW.CO.UK)  
[WWW.CRITICAL-COMMUNICATIONS-WORLD.COM](http://WWW.CRITICAL-COMMUNICATIONS-WORLD.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**



**nexteer**  
AUTOMOTIVE



• **A P T I V** •

**DELPHI**



**veoneer**

To learn more, contact [Nuria.Frances@iqpc.com](mailto: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**

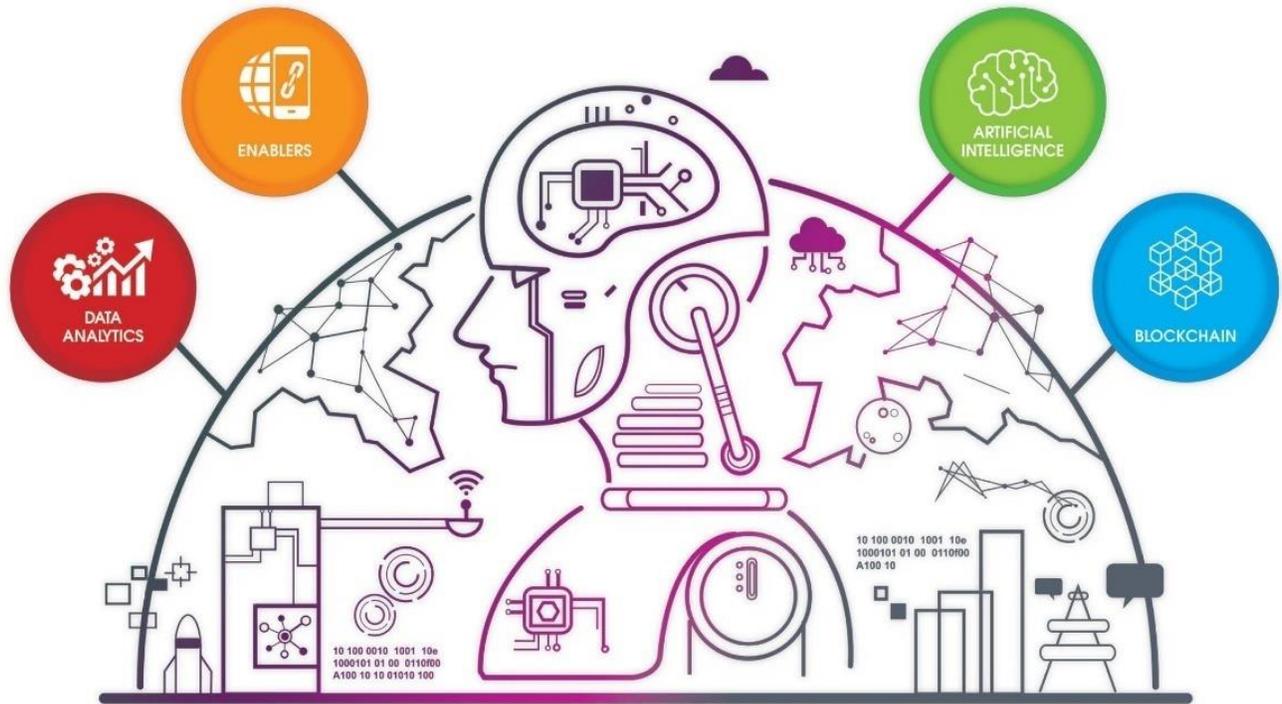
**10% OFF ADMISSION CODE CDMCYVEST19**

**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



Artificial Intelligence  
Blockchain  
Data Analytics  
Enablers  
Data Analytics  
Blockchain

## BUILDING VALUE CHAINS

Enablers  
Artificial Intelligence  
Data Analytics  
Blockchain  
Artificial Intelligence  
Data Analytics

SMART CITIES

INDUSTRIAL IoT

**ENABLERS**

Artificial Intelligence Data Analytics Blockchain Data Analytics  
Blockchain Artificial Intelligence Data Analytics Blockchain

**ARTIFICIAL INTELLIGENCE**

Artificial Intelligence Data Analytics Enablers Blockchain Data Analytics Artificial Intelligence Data Analytics Enablers

**DATA ANALYTICS**

Data Analytics Blockchain Artificial Intelligence  
Blockchain Artificial Intelligence Data Analytics Enablers

**BLOCKCHAIN**

Artificial Intelligence Data Analytics Blockchain Data Analytics Artificial Intelligence  
Blockchain Artificial Intelligence Data Analytics Enablers Data Analytics

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



REGISTER NOW!

[www.internetofthingsasia.com](http://www.internetofthingsasia.com) • #iotasia

Organised by



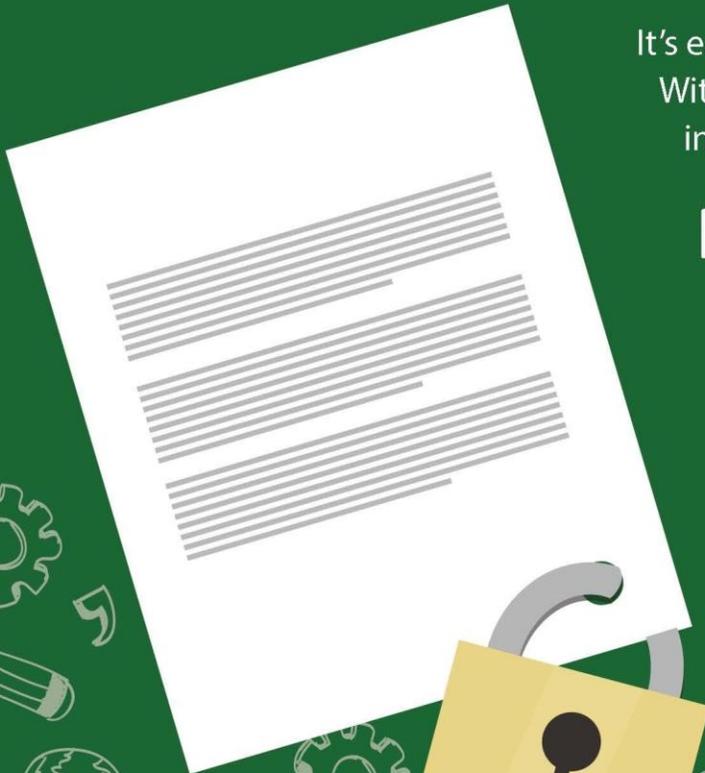
Industry Accolades



# Simplify and Secure Your File Transfers

It's easy to protect and audit your file transfers. With GoAnywhere Managed File Transfer in your toolbox, you can...

- Comply with industry security standards like PCI DSS
- Streamline manual processes
- Encrypt file transfers with modern technologies
- Move data safely between on-premises and the cloud



See what GoAnywhere MFT can do  
in your organization.

[www.goanywhere.com/managed-file-transfer](http://www.goanywhere.com/managed-file-transfer)



**GO ANYWHERE**<sup>®</sup>  
Managed File Transfer

**RSA**®Conference2019

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](http://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](mailto:events@intelligence-sec.com) or  
+44 (0)1582 346 706

Sponsors & Exhibitors



**Resecurity**<sup>®</sup>

For more information visit – [www.intelligence-sec.com](http://www.intelligence-sec.com)

Book your place by:

w: [www.intelligence-sec.com](http://www.intelligence-sec.com) | e: [events@intelligence-sec.com](mailto:events@intelligence-sec.com) | t: +44(0)1582 346706

**INTELLIGENCE-SEC**

The logo features the word "COMEX" in a bold, sans-serif font. The "CO" is red, "MY" is purple, and "EX" is blue. Each letter has a diagonal line through it. Below "COMEX" are the words "TECHNOLOGY" and "SHOW 2019" in a smaller, black, sans-serif font.

**COMEX**  
TECHNOLOGY  
SHOW 2019

The logo is identical to the one above but is set against a solid black rectangular background. The word "COMEX" is white, and the text "TECHNOLOGY" and "SHOW 2019" is also white.

**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](mailto: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](http://cyber.forum.yale.edu) EMAIL [cyber.forum@yale.edu](mailto:cyber.forum@yale.edu)

# 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.

Visit [info.goanywhere.com/use-cases-for-mft](http://info.goanywhere.com/use-cases-for-mft) to get the free guide sent right to your inbox.





**DATA PROTECTION WORLD FORUM**

PRIVACY | TRUST | RISK | SECURITY

**CDM**

**CYBER DEFENSE MAGAZINE**

THE #1 SOURCE FOR IT SECURITY INFORMATION

**Rowena Fell**

Global and EMEA 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'*

**#CYBERBYTE**  
**@ROSSOWESQ**



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

**“Amazing Keynote”**

**“Best Speaker on the Hacking Stage”**

**“Most Entertaining and Engaging”**



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

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



# CYBER DEFENSE TV

## INFOSEC KNOWLEDGE IS POWER

You asked, and it's finally here...we've launched [CyberDefense.TV](http://CyberDefense.TV)

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

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

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

### The Interviews

These anticipated "CEO Hotseat" Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by **Gary Millefsky**. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. [www.cyberdefense.tv](http://www.cyberdefense.tv)

## 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.](#)

**CDM**  
CYBER DEFENSE MAGAZINE  
eMAGAZINE

IN THIS EDITION:

**NEVER STOPS GIVING**

InfoSec Thoughts for 2018  
Network Traffic Insecurities  
Endpoint Security Best Practices  
Vulnerability Equities Process

5 YEARS  
OF PUBLICATION

**IT'S FREE**

DECEMBER 2017 MORE INSIDE!

SUBSCRIBE TODAY! NO STRINGS...

## 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](mailto: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](mailto:marketing@cyberdefensemagazine.com)

### Cyber Defense Magazine

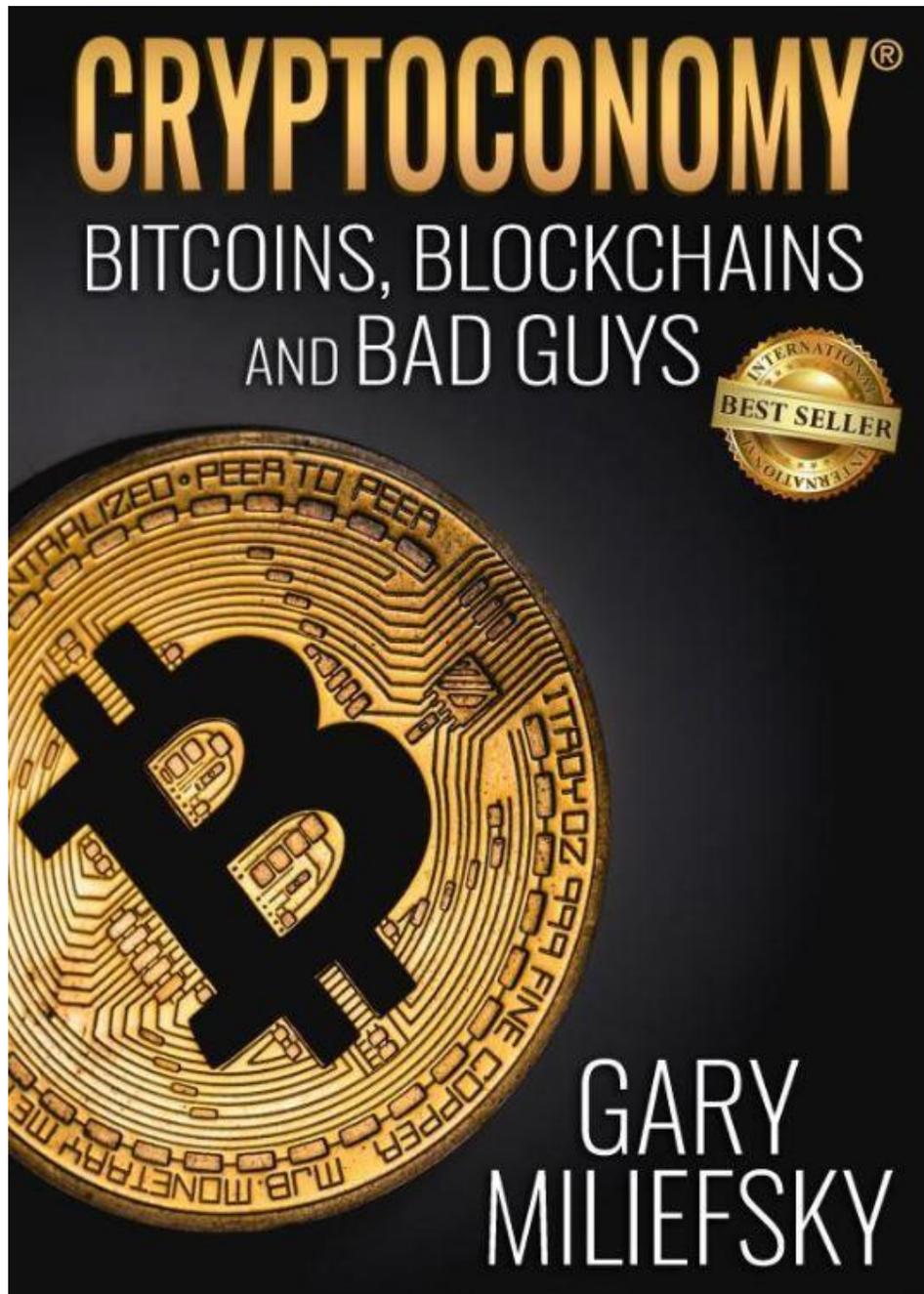
PO Box 8224, Nashua, NH 03060-8224.  
EIN: 454-18-8465, DUNS# 078358935.  
All rights reserved worldwide.  
[marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)  
[www.cyberdefensemagazine.com](http://www.cyberdefensemagazine.com)

### **NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)**

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 02/01/2019

# TRILLIONS ARE AT STAKE

No 1 INTERNATIONAL BESTSELLER IN FOUR CATEGORIES



THE REGENT UNIVERSITY INSTITUTE FOR CYBERSECURITY

# Setting the Standard in Cyber Defense Training & Education



**LEARN MORE >**

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](https://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>

## Setting the Standard

in Cyber Defense  
Training &  
Education



**LEARN MORE >**

# CDM

**CYBER DEFENSE MAGAZINE**

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

# eMAGAZINE

[www.cyberdefenseemagazine.com](http://www.cyberdefenseemagazine.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?**

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.



**GO ANYWHERE<sup>®</sup>**  
Managed File Transfer

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](http://www.goanywhere.com/trial)

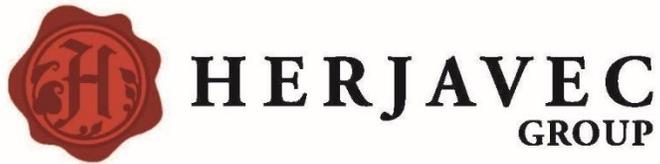


**BOSCH**

Invented for life

Bosch and Genetec.  
End-to-end security,  
day after day

Learn more



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



- ▶ Security Company of the Year
- ▶ Identity and MSSP Leader