CYBER DEFENSE MAGAZINE

eMAGAZINE

IN THIS EDITION

MAY 2020

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

NEW PLATFORMS: CyberSecurityMagazine.com (SMB/SOHO/B2C) CyberDefenseWebinars.com (B2B)

Dear Friends,

Cyber Defense Magazine has established an important presence in the marketplace of cybersecurity ideas. With 8 years' experience, we are now entering a new phase. For the first time, we are seeing the effects of social distancing and lockdown protocols in the national and international conduct of private and government activities, due to the battle against the spread of the Coronavirus.

In today's world, this shift emphasizes the importance of keeping up to date on the cutting edge of theory and practice of cybersecurity. Cyber Defense Magazine is the go-to resource for cyber security professionals. In many instances, this starts with the CISO, but the spread of Work from Home ("WFH") practice of more and more employees now requires the attention of all those with access to any portion of the organization's electronic information.

CISOs can be most effective in taking the lead by staying tuned in to the thoughts and presentations of their colleagues. In pursuit of the most timely and efficient means of distributing this kind of guidance, Cyber Defense Media Group has launched a series of webinars at www.cyberdefensewebinars.com, bringing a new level of direct communication to the front-line executives and those for whose online activities they are responsible. We've also launched www.cybersecuritymagazine.com to focus on mid market, smb business (mid-to-smaller B2B) and consumer (B2C) cybersecurity news, tips, ideas and products, while our main magazine site www.cyberdefensemagazine.com continues to focus on large to mid enterprise (larger B2B) and government cybersecurity solutions (B2G), as we grow our brands and our platforms.

We'll also be launching an online cybersecurity game show and our traditional annual awards programs, starting in May, 2020. We are pleased to provide this powerful combination of monthly eMagazines, daily updates and features on the Cyber Defense Magazine home page, and webinars featuring national and international experts on topics of immediate interest and rekindling having fun, during these trying times.

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, Publisher

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

From the International Editor-in-Chief…

With growing incredulity, we in the forefront of international cybersecurity developments continue to observe a lack of coordination among government and corporate organizations in this period of turmoil. Professionals might hope for, or even expect, a greater degree of cooperation in confronting the common enemy, COVID-19.

Unfortunately, the fragmentation we observe appears to be based upon the splintering of national and political interests. Looking only at gross reported statistics on confirmed cases and mortality (which vary widely in accuracy and transparency), the divergence in actions and outcomes seems to reflect a lack of common purpose. If indeed one of the hopeful prospects is for the development of "herd immunity," this human herd does not appear to be on track to reach such a desirable conclusion.

Let me take this occasion to renew the call for all of the affected organizations and individuals to take the lead in creating cybersecurity defenses to protect all aspects of IT in our lives, including (but not limited to) medical, financial, social, and government functions.

Once again, may I suggest, that in the days ahead, we agree to put our differences aside in favor of responding to our common enemies: the COVID-19 virus itself and those who would take advantage of this crisis to perpetrate criminal schemes.

To our faithful readers, we thank you,

Pierluigi Paganini

International Editor-in-Chief

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

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

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

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

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

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

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

http://www.cyberdefensemagazine.com

PUBLISHER

Gary S. Miliefsky, CISSP®

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

8 YEARS OF EXCELLENCE!

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

CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE TV RADIO AWARDS

Welcome to CDM's May 2020 Issue

From the U.S. Editor-in-Chief

"New Normal" – It's a phrase we hear and read more and more frequently.

What will life in general, and remote work in particular, be like when the current spread of Coronavirus is finally overcome? What are the likely changes in the world of cybersecurity?

Almost nobody suggests that life will simply return to pre-COVID-19 circumstances. It's more like the old saw about asking 10 experts and getting 15 opinions: there is no clear and convincing picture of the elements of the "New Normal."

Nonetheless, there are certain steps we can all take, in our own capacities, to prepare for these eventualities. First and foremost is to maintain current familiarity with the threats and responses to the most harmful potential results of the shift in the patterns of accessing and protecting sensitive information.

To reach that objective, the May issue of Cyber Defense Magazine features articles drawing a closer focus on some of the challenges and responses to today's (as well as tomorrow's) threats and vulnerabilities.

We trust this information will continue to provide much-needed support to our over 5 million individual readers, as CDM maintains its position as the leading publication for cybersecurity professionals.

Wishing you all success in your cyber security endeavors,

Yan Ross

US Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & US Editor-in-Chief for Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him via his e-mail address at:

yan.ross@cyberdefensemediagroup.com


SPONSORS

cythereal

Predictive Cyber Defense

Lucio Frega, Threat Researcher
Deutsche Telekom - Cyber Threat Intelligence

MALWARE

YARA

HUNT

PREDICT

cythereal.com

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

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

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

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

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

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

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

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

About the Author/Disclosure

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

RSAConference | Where the world talks security

Ensuring the security of your organization is always challenging, even in the best of times.

We created an **online resource center** to help you find the answers you may be looking for. It includes relevant content such as interviews with CISOs dealing with today's realities, preventing ransomware attacks, tips on how to improve your virtual presenting skills, and much, much more.

Browse our specially curated resources today, and keep checking back as new information is added regularly.

rsaconference.com/cyberdefense-2020

Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

Founder & Managing Partner

SEAN DRAKE

U.S.ARMY

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

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

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

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

DECEPTION-BASED THREAT DETECTION

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

Attivo NETWORKS®

Deceive. Detect. Defend.

Learn more at attivonetworks.com/ebook

Setting the Standard

in Cyber Defense Training & Education

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

CORPORATE | GOVERNMENT | MILITARY | EDUCATION

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

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

Learn More

regent.edu/cyber | 757.352.4590

REGENT UNIVERSITY | Institute for Cybersecurity

OneTrust

Privacy Management Software

World's #1 Most Widely Used Privacy Management Software

For Privacy, Security & Third-Party Compliance

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

Privacy Program Management:

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

Marketing & Privacy UX

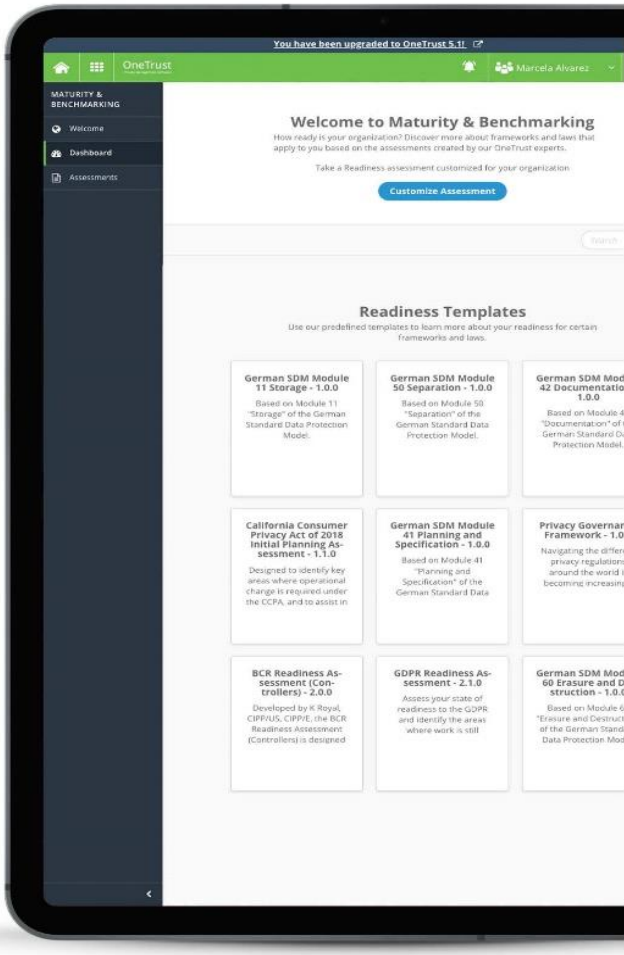
- **Cookie Compliance:** Website Scanning & Consent
- **Mobile App Compliance:** App Scanning & Consent
- **Universal Consent:** Consent Receipts & Analytics
- **Preference Management:** End User Preference Center
- **Consumer & Subject Requests:** Intake to Fulfillment
- **Policy & Notice:** Centrally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

Third-Party Risk Management

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

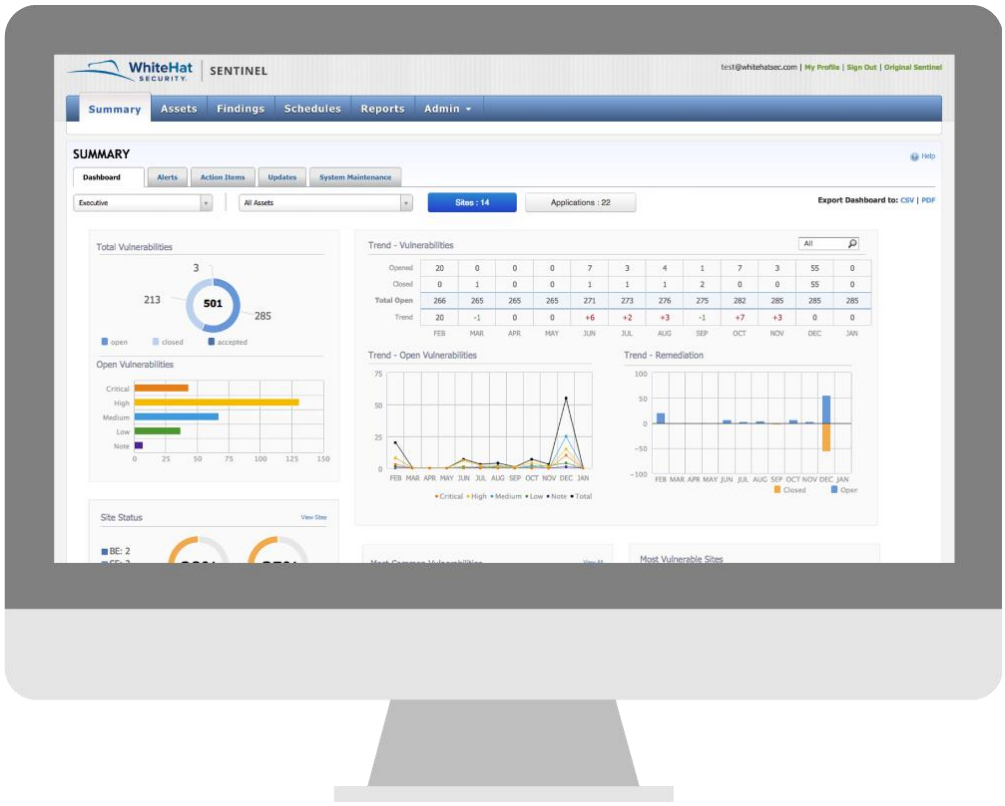
Incident & Breach Response

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



GET STARTED TODAY | ONETRUST.COM/FREE-EDITION

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



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

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

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

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

A customized review and complimentary final executive and technical report

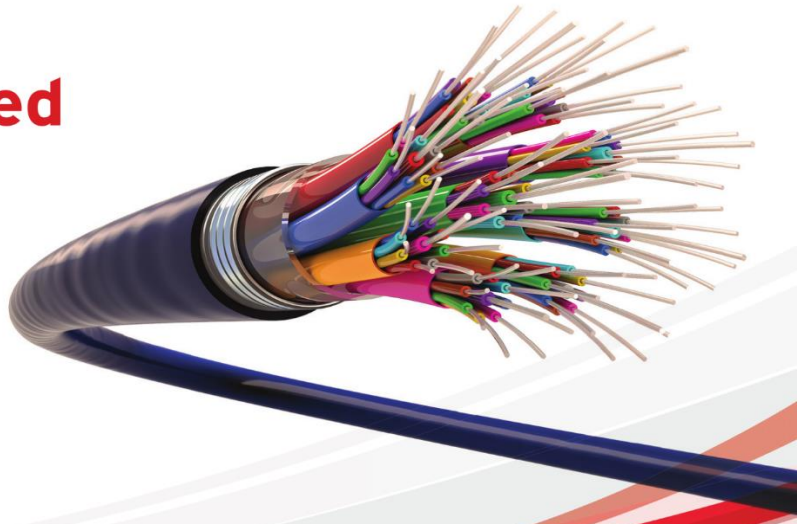
Click here to sign up at this URL: https://www.whitehatsec.com/info/security-check/

PLEASE NOTE: Trial participation is subject to qualification.

TREND MICRO™

POWERED BY XGen™ SECURITY

Detect and prevent breaches at wire speed



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

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

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

NSS LABS RECOMMENDED

Proven capability

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

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

Industry leading threat intelligence

TREND MICRO SMART Protection Network™

TELUS®

Web App Digital Vaccine BY TippingPoint

ZERO DAY INITIATIVE

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

www.trendmicro.co.uk/xgen-cyber

Database Cyber Security Guard

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

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

Product Features

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

Get a FREE COPY now.

www.DontBeBreached.com/Free

NIGHTDRAGON

***"NightDragon** Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"*

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com

Two Years Later

NotPetya's Game-Changing Lessons for Cybersecurity and Collective Defense

In early Summer 2017, the highly destructive NotPetya malware appeared and spread with devastating efficiency across data systems and architectures worldwide. The attack not only shattered records for speed and destruction, but also served as a wake up call for security professionals to up their game on cyberdefense. Here are key lessons learned from NotPetya, and how those lessons continue to shape today's leading practices in cybersecurity.

LESSON 1

Malware is increasingly designed to disrupt business operations in the physical world.

NOTPETYA CREATED AN UNPRECEDENTED

$10 billion

IN DAMAGE WORLDWIDE[1]

How NotPetya changed the game — Unlike ransomware and other profit-driven attacks, NotPetya was built simply to destroy.

How the cybersecurity industry is adapting — NotPetya has taught today's security teams to assume destruction is a potential goal, appreciate the elevated risk and then act accordingly.

LESSON 2

NotPetya raised the speed limit for modern cyber attacks.

NOTPETYA SPREAD TO MORE THAN

64 countries

IN JUST THE FIRST

24 hours[2]

How NotPetya changed the game — NotPetya was built for speed, with code designed to proliferate automatically, rapidly and indiscriminately.

How the cybersecurity industry is adapting — Cyberdefenses today should ideally use near-real time network traffic analysis and behavioral analytics to rapidly catch new forms of attacks that perpetually outdated signature-based systems would miss.

LESSON 3

The worst attacks take lateral movement to the extreme — across all organizational and industry barriers.

THE FAR-FLUNG INDUSTRIES AFFECTED BY NOTPETYA INCLUDE

shipping, pharmaceuticals, banking, advertising, energy

AND OTHER MAJOR SECTORS [3]

How NotPetya changed the game — NotPetya's spread was not only fast, but also far and wide — with cross-sector damage at major organizations like Maersk, FedEx and others. NotPetya was also patch-resistant, vacuuming up credentials on infected targets for use later as workarounds on protected servers.

How the cybersecurity industry is adapting — Companies must assume the when, not if, mindset to penetration and lateral movement, and embrace collective defense and threat information sharing — across entire industries and even between many different sectors.

LESSON 4

NotPetya shows the limits of attribution.

CYBERATTACK ATTRIBUTION IS GETTING MORE COMPLEX, WITH AT LEAST

10 variations

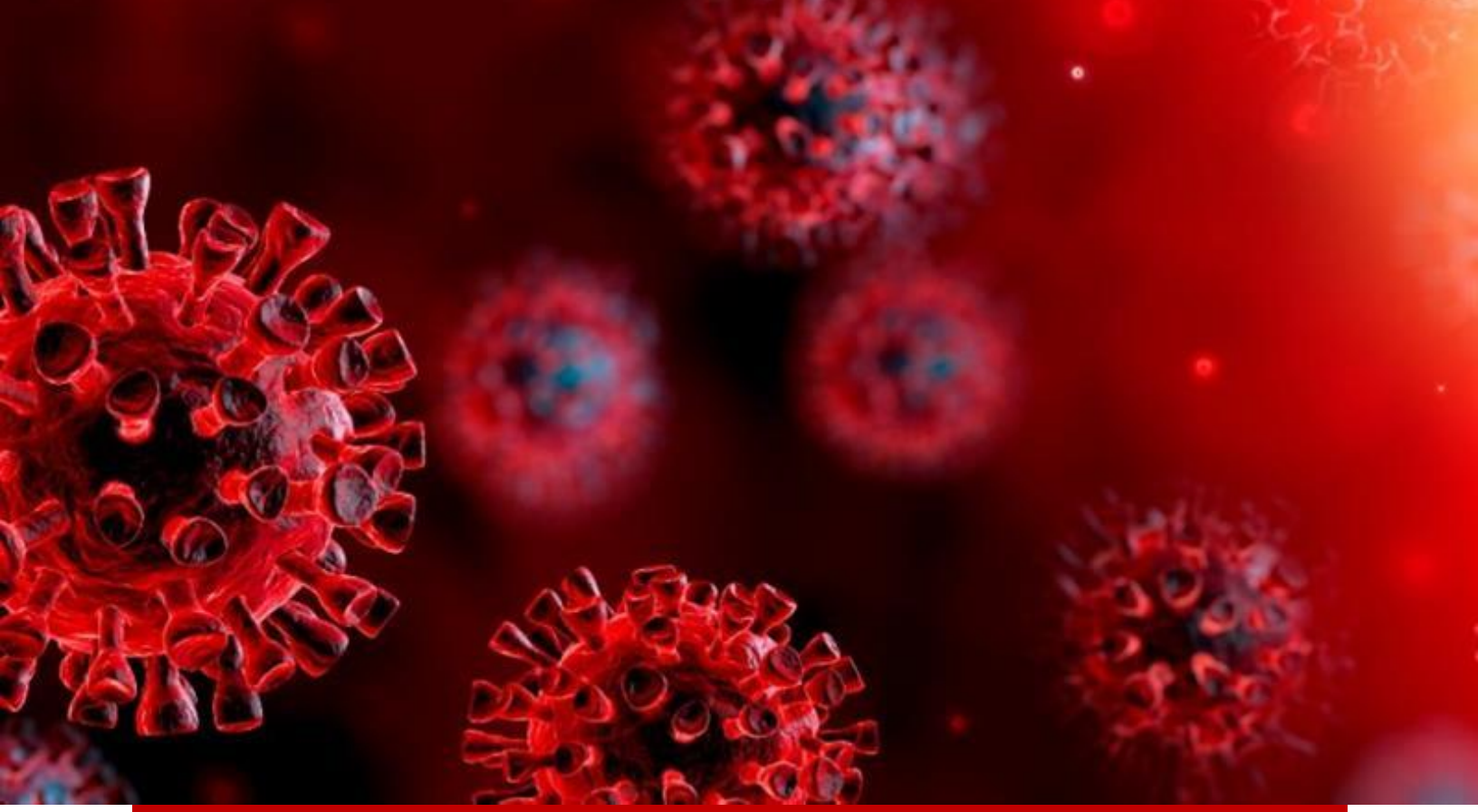
OF NATION-STATE RESPONSIBILITY [6]

How NotPetya changed the game — While Russia is generally blamed for NotPetya,[4] the attribution is less critical, given the indiscriminate nature of the attack and increased "collective offense" between criminal groups and nation-states sharing tactics and targets.[5]

How the cybersecurity industry is adapting — Security teams must meet threat actor's collective offense approach with collective defense — working with peers to share threat information and identified attack techniques.

1 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
2 https://www.securityweek.com/petyanotpetya-what-we-know-first-24-hours
3 https://www.securityweek.com/notpetya-attack-costs-big-companies-millions
4 https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/
5 https://ironnet.com/white-paper-survey-download/
6 https://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF


ARTICLES



A Cyber Approach to Coronavirus Containment

By Zohar Rozenberg

What lessons can be learned from reviewing how we manage cybersecurity and applying it to an anti-Coronavirus campaign?

In recent years, some in the cyber world recognize that there is a lot to learn from the biological world when protecting systems against viruses. Now, the Corona epidemic presents an opportunity for the medical world to learn something from the cyber world. To analyze the strategies selected by various countries, let's review it through the lens of cyber strategies.

Let's begin by recognizing that cybersecurity is built in layers. There is no one magic solution or layer which will prevent all the possible attacks. Furthermore, in the cyber world, it has been realized for some time that it is impossible to protect everything for all eternity. There will be victims. Computers will be attacked, information will be stolen, and activity will be interrupted, etc. It has already been accepted in the business world that it is not possible to maintain an extremely high level of protection, while at the same time enabling a business to run at its required pace.

A compromise must always be found, and risks managed. Extremely high levels of security are possible, but this will give rise to a situation where work may grind to a halt. Businesses accept that by running freely, they expose themselves to various levels of cyber threats.

The challenge, which has become the main responsibility of information security managers, along with their organizations, is to learn how to live with this day-to-day compromises. To understand the risks they take, determine what level of risk they can accept, and what level of risk is too great.

Just as businesses weigh various protection approaches, we can see several strategies for protection against Coronavirus being implemented by various countries. In Asia, South Korea, and Taiwan, a relatively advanced approach have been adopted of detecting the threat, finding where it is harbored, and dealing with it surgically wherever identified. All this is in conjunction with a basic layer of disinfecting large areas.

As in the cyber world, this can be seen in the use of advanced concepts of threat hunting and extensive investment in detection and incident responses. All this is above and beyond the basic layer of a standard firewall and endpoint protection in order to provide some basic level of protection throughout the whole organization. This approach is a reflection of an understanding that the "point of contact" to the world will be breached, or in the professional slang, "the perimeter is dead". It is not possible to achieve full protection and keep the threat outside the perimeter forever. The threat must be sought out on a targeted basis and dealt with wherever identified without giving up on a basic layer of protection, which will succeed anyway in preventing the simpler threats from penetrating.

Aside from these countries, most countries in the world, including Israel, Italy, and The USA have adopted approaches that are considered traditional and older, according to the cyber world. Israel began with an approach that derives from the belief that there is indeed a "perimeter" and that the threat can be blocked externally and prevented from getting inside. As mentioned, in the cyber world, this approach is now widely thought to be inherently irrelevant. Subsequently, Israel, like Italy and the USA, transitioned to taking the approach of a callous and aggressive policy. In the cyber world, such an approach equates to a policy of a strong lock-down of the network, preventing the transmission of information between points in the network. This makes any approach to the resources of the network difficult and, in general, terms attempt to reduce traffic on the network. Such an approach can indeed succeed in producing achievements in terms of preventing breaches of the network and the endpoints, but it also has the effect of preventing most of the activity on the network and, consequently, having an adverse effect on the organization's business activity. Such an approach to protection was previously beneficial at sensitive locations such as Defense Establishment Institutions, but over the years, they have also understood that it is impossible to operate over time with such difficulties piling up over the activity of the organization.

In the IDF, it was realized several years ago that in order to achieve the aims of the organization, it must allow more access to the network, to facilitate more connections and transmission of information between endpoints. In order to reduce potential risk, the organization has sought more advanced protection approaches.

Throughout the industry, it is now difficult to find organizations that still stick with the approach of a robust and aggressive cyber policy. In the last decade, we have witnessed a shift towards more sensible and considered risk management, which attempts to strike a balance between the need to facilitate activity and the desire for protection.

Britain has attempted to adopt its own unique approach, which, by contrast, the cyber world finds slightly illogical. In fact, Britain has attempted to rely upon the immunity of all its citizens, and in cyber terms, it is as if they are content with the installation of anti-virus software at all the endpoints. This protection approach has not been relevant in the cyber world for approximately 20 years, and there are currently no organizations in existence that use it as their approach for protection, with the possible exception of very small businesses.

It is possible to analyze the operational approaches of the countries from another angle in the cyber world, and that is "threat intelligence". On one side of the spectrum is the USA, which appears to have approached this situation with a profound lack of information, to the point of ignorance in the face of the threat. On the other hand, Israel has learned as much as it could about the threat and has attempted to prepare for it ahead of time.

Today in the cyber world, there is a growing acknowledgment of how difficult it is to build a layer of protection against cyber threats without engaging in the acquisition of advanced information related to threats and their nature. Currently, the leading organizations worldwide, with their own ability to protect themselves, are widely reliant upon information when addressing cyber threats.

Another analogy to the cyber world can be analyzed from the public reactions in various countries. Apparently, in Singapore, Taiwan, South Korea, and perhaps other places, the public has strictly complied with governmental directives, understanding the risk and responding well to the threat. On the other end of the spectrum is Italy, which reacted complacently, did not heed governmental instructions, and didn't understand the size of the threat. Thus, in cyber, the sphere of awareness and training which has been gathering momentum in recent years tries to get the personnel of the organization to appreciate the threat and educate them on proper procedures in the presence of a threat. This is regarded as maintaining "cyber hygiene," which reminds employees not to open suspicious emails, how to report something suspicious to the organization, etc.

Organizations that have invested in educating people regarding awareness and correct actions have reported an improvement in the immunity of the organization to cyber threats. In organizations that have not invested in this at all, most people find themselves falling prey to cyber-attacks such as email impersonations.

It appears that in the cyber world, more advanced organizations are adopting more innovative approaches, and the use of advanced tools such as threat hunting, detection, incident response, as well as employee awareness have produced better results in coping with cyber threats. Thus, in the physical world, countries that have adopted similar approaches appear to have succeeded, at least for now, in containing the virus's threat in terms of a dramatic reduction in the number of cases of infection and are on the point of at least a partial return to routine. Countries viewed as maintaining more traditional approaches and that are attempting to sanctify the perimeter or apply tough, aggressive policies as their major effort, are finding it very difficult to contain the threat. These countries are still seeing a rise in cases, coupled with a widespread paralysis of economic activity, and the economy as a whole.

If countries wish to learn lessons from the world of cyber protection in order to deal with the Coronavirus

threat, then they must bear in mind that building defenses must consist of several layers. No one method can avoid the threat.

Investment efforts must be put toward prevention. It is essential to create a basic level of control and monitoring of entrances, but the action is also necessary on the level of detection and treatment. This can only be done properly by adequately gathering and analyzing the latest data. It is to be hoped that more and more countries will consider adopting more advanced protection approaches, finding ways of applying them in the physical world in order to accelerate the end of the threat and bring about a return to a normal routine.

About the Author

Zohar Rozenberg serves as VP of Cyber Investments for Elron, investing in early-stage cybersecurity and Enterprise software startups. Zohar also serves on the board of directors for C

In his previous role as an IDF 8200-unit Colonel (retired), Zohar assisted in the founding of Israel's National Cyber Bureau, formalizing the country's national cyber strategy. His final role with the IDF was as the head of its cyber department.

He is always looking for bold and innovative entrepreneurs which their ideas promise to shape our tomorrow.

Top 5 Coronavirus Scams

By Zack Schuler, founder and CEO of NINJIO

One of the reasons NINJIO content is so successful at capturing and holding employees' attention is its relevance – we release new episodes every month that keep users updated on the latest cyberthreats that could harm them, their companies, and their families. As part of our ongoing effort to keep our partners and customers on the cutting edge of cybersecurity awareness, we wanted to inform you about an alarming new development: how hackers are exploiting the Coronavirus pandemic to send their own destructive viruses out into the world.

As millions of people self-quarantine and get accustomed to working from home (often for the first time), they're especially susceptible to cyberattacks. There are many reasons why this is the case, from the use of personal devices that haven't been updated with the latest security software to an explosion of seemingly lucrative offers of remote work that are actually scams. As is so often the case with cybersecurity, the majority of these attacks can be thwarted by educated people using good judgment and knowing what to look for.

That's why we created this report to expose the **top five Coronavirus scams and cyberthreats**. At a time when you've already taken drastic measures to protect your loved ones and fight back against this pandemic, the last thing you need is to be hacked. Read on to learn how you can prevent that from happening.

#1: Coronavirus malware map

One of the go-to resources for anyone who has been tracking the Coronavirus outbreak is an interactive map managed by Johns Hopkins University that provides real-time updates on the spread of the disease. But cybercriminals are now using a fake map to manipulate victims into downloading malware capable of stealing their passwords.

The malware is embedded in a file that has to be downloaded before it can infect the victim's computer. And while the victim has to have Java installed for the infiltration to work, cybersecurity analyst Brian Krebs reports that the seller (who was advertising the malware on a Russian hacker forum) claims it will even work on updated versions of the software. This is a reminder that clever social engineering can help hackers get around digital protections.

Users can avoid falling victim to this cyberattack by refusing to click on suspicious links or attachments – particularly if they're offering access to data or information that doesn't require any special download to access. There are countless resources for anyone who's interested in staying up to date on Coronavirus, such as the real map on the Johns Hopkins website, The New York Times' daily tracker, and information provided by the Centers for Disease Control and Prevention (CDC). All of these resources are readily accessible online, so there's no reason to risk downloading a map or anything else.

#2: Fraudulent offers of remote work

While many companies have instructed their employees to work from home until further notice, there are also thousands of workers who are out of work altogether. This means they're on the hunt for new jobs, and given the vast shutdowns and layoffs that are taking place outside their front doors, they're turning to the Internet. While remote work can offer many people a lifeline during this period of isolation and economic contraction, cybercriminals are taking advantage of a desperate situation to manipulate and defraud people.

For example, a group of hackers launched a fake nonprofit called the Vasty Health Care Foundation, which tricks job seekers into thinking they've been hired by a nonprofit that's working to help people affected by Coronavirus. In reality, these victims are being used as "money mules" – unwitting intermediaries who help cybercriminals launder stolen money. The hackers will tell victims that a "donation" needs to be processed, so they'll transfer money and ask that it be converted into Bitcoin.

Of course, not all fraudulent work offers are money mule schemes – many are just a way to gain access to sensitive information such as Social Security numbers. These are all reasons why job seekers should work with established companies whenever possible and do their homework on any potential employer – are there reviews on sites like Glassdoor? Is there media coverage you can reference? Have you spoken to anyone at the company over the phone? Did the interview process seem rushed? Do the terms sound too good to be true?

If you're in search of remote work (especially for the first time), these are all questions you should be asking. You should be even more wary if you're asked to move money around (particularly when

cryptocurrency transfers are involved) or if you're asked for sensitive personal information like your SSN and bank account number.

#3: Fear phishing (fake government alerts)

Cybercriminals have always preyed on the fear of their victims – they use threats and frightening language to coerce people into doing what they say. This is why one of the fastest-growing scams is a fake phone call from the Social Security Administration that convinces victims their SSNs have been compromised or used in criminal activity. Hackers then demand money or "verification" of the SSN, which allows them to steal both. In 2018 alone, 35,000 people were hit with this scam and they lost $10 million.

It's no surprise that cybercriminals are taking full advantage of the fear surrounding Coronavirus. Fake emails from the CDC, the WHO, and other major federal and international agencies are circulating with subject headings like "COVID-19 – Now Airborne, Increased Community Transmission" and offering downloadable information on "little measures that can save you." There are also emails that target people who are more conspiratorial, which claim Coronavirus is a "weapon" designed to "control the citizens of the world." These hackers offer access to information about a fake secret vaccine.

The cybercriminals who create schemes like these use a wide range of hacking tools like keyloggers that can steal credentials and sensitive personal information. Proofpoint researchers report that they've seen "fake Office 365, Adobe, and DocuSign sites" that convince people they're working with legitimate documents. And as with many of the Social Security scams (in which the Social Security Administration's real number appears on caller ID), these hackers are able to imitate legitimate email addresses from organizations like the CDC.

This is why you should always check the email headers, hover your cursor over links to see where they actually lead, and be extremely suspicious of alarmist messages coming from government agencies that are asking you to do something immediately. Instead, check the alerts on real websites and call the agencies if you have any questions.

#4: How hackers exploit our desire to help (fake Coronavirus charities)

Just as cybercriminals know how to manipulate their victims on the basis of fear, they also know how to take advantage of generosity. The aforementioned Vasty Health Care Foundation scheme told job seekers that the sham organization helps "hospitals from underdeveloped countries to support the highest level health care through the funding of vital medical equipment, research, education, and the provision of items that impact comfort and care."

The hackers clearly assumed that people would be more interested in the fake job posting if they thought it was an opportunity to help people affected by Coronavirus. This is a realization many other cybercriminals have made as well, but they're soliciting money directly. To take just one example: Kaspersky Lab reports that a fraudulent email purportedly sent by the CDC asks recipients to donate to

help establish an "incident management system to coordinate a domestic and international public health response" to the pandemic.

While most people will immediately recognize that a federal agency would never send an email soliciting private donations – much less to a Bitcoin account – other cybercriminals are savvier. The Vasty Health Care Foundation website, for instance, uses a template based on a real charity (globalgiving.org) to convince visitors of its legitimacy. The FTC expects the number of phony Coronavirus charities to spike in the coming weeks, and it points out that "Some scammers use names that sound a lot like the names of real charities."

A recent press release by the office of Georgia's Secretary of State addresses the uptick in counterfeit Coronavirus charities and points out that "awareness is the first line of defense." This is NINJIO's core message, and it's more applicable than ever in the midst of a pandemic. If you want to help Coronavirus victims, visit the websites of well-known charities directly, never enter payment information in response to a solicitation email, and use resources such as GiveWell (which is conducting research on how to mitigate the effects of Coronavirus) and the Better Business Bureau to determine which charities are the most effective.

#5: Hackers are exploiting economic relief efforts

The economic impact of Coronavirus has been immense – the stock market saw its worst single-day drop since 1987 and workers are suffering from an explosion of layoffs. Governments are taking immediate action to stave off a potential recession – for example, the United States is developing a $1 trillion economic stabilization plan that would provide every American adult with a $1,000 check.

This provides even more fertile ground for cybercriminals who are doing everything they can to take advantage of the pandemic. In the coming weeks and months, we shouldn't be surprised if hackers launch a full-on disinformation assault, which will include emails, text messages, phone calls, and just about any other channel of communication that can be used as an attack vector. Government relief programs offer the perfect pretense for cybercriminals to deceive people and steal their information.

NINJIO recently received a direct report of a fraudulent text message that read: "As of March 18th you can qualify for the hardship program. Would you give us a quick call at [a number is listed here] now please to discuss your options?" These scams aren't limited to the United States, either. Mimecast discovered that an artificial email purportedly from the U.K. government has been circulating to "inform" people about a "new tax refund program for dealing with the Coronavirus outbreak." After being told what their "refund" is, victims are instructed to follow a link labeled "Access your funds now." Then they hand over their financial and tax information.

You should only provide sensitive information directly through the secure online resources provided by your government. Never click on a link in an email that's asking for money. If you have any questions about measures your government is taking to support unemployed or underemployed workers during the pandemic, reach out on the phone via the relevant agency's official phone number. And pay close attention to media reports on stimulus efforts, which will provide projected timelines and other important information.

At a time when cybercriminals are tirelessly developing schemes like these to leverage the mass fear, uncertainty, and desperation caused by the Coronavirus outbreak, we all have to be just as tireless in our efforts to repel their attacks and protect ourselves. While there are many technological defense mechanisms that can be deployed during the period of quarantine and social distancing – such as updating all your devices, using a VPN, and protecting accounts with multi-factor authentication – your most important cybersecurity resource is your own awareness.

About the Author

Zack Schuler is the founder and CEO of NINJIO, a digital security awareness company that empowers individuals and organizations to become defenders against cyberthreats. Prior to launching NINJIO, Zack was the founder and CEO of the IT services company Cal Net Technology Group. Cal Net was acquired by Olympic Valley Capital in 2013. In addition to his entrepreneurial pursuits, Zack is a member of the Forbes Technology Council and is on the board of governors for Opportunity International, an organization that provides microfinance loans, savings, insurance, and training to over 14.3 million people who are working their way out of poverty in the developing world.

Zack can be reached on Twitter @zschuler. Find out more about NINJIO at ninjio.com.

COVID-19: How to Take Advantage of Teleworking

By Pedro Tavares, Editor-in-Chief seguranca-informatica.pt

With the COVID-19 outbreak, companies and governments are taking preventive measures that include teleworking. This can be a turning point in the way we look at teleworking. Despite many advantages, it is important to be disciplined and follow a healthy doctrine so that everything can proceed smoothly and productively.

Teleworking has spread rapidly in recent years. It has been commonly adopted in some countries and not so much in others; it offers advantages and disadvantages for both the employee and the company.

If you feel a motivated person, I can share with you some advantages this mode of work:

Autonomy: This is the most probably and obvious advantage of teleworking (even more than the pyjamas and slippers advantage).

Savings on travel costs: In those large cities – and even the small ones- getting to the workplace can consume several hours each day.

The employee's opinion of the company will definitely improve: Since remote work has a number of important advantages, it is very common that this will influence the employee's assessment of both the company and his job.

Productivity can be increased: The advantages that teleworking offers should improve the worker's mood.

Nonetheless, you need to be a disciplined person, or teleworking can turn out to be a nightmare, bringing frustration to your professional life.

Some disadvantages that I can enumerate are:

- Sometimes it is not easy to disconnect, it might be a problem
- Work performance may drop, sometimes
- The worker could feel less identified with the company
- Some extra expenses are generated for the worker

In fact, this work away from the office can increase cybersecurity threats and vulnerabilities. These days, cybercriminals are taking advantage of the teleworking situation to put in place several cyber threats that attract users, such as phishing, online fraud, and disinformation campaigns.

In this sense, the protection of users must be reinforced in this new remote context motivated by teleworking, with four essential solutions: (i) virtual private network (VPN) connection, (ii) multifactor identity verification mechanisms, (iii) Cloud and DNS security, and (iv), device protection.

This is a time where many users are using video conferencing software to perform secure and online meetings.

Therefore, when using software from this nature, do not facilitate, and:

- Disable all functions that are not used, microphone, camera, screen sharing or file-sharing;
- Physically cover the webcam when not in use;
- During screen sharing, disable work-related notifications and ensure that it is okay to share content on the screen background or in other windows;
- Set passwords and do not reuse meeting codes; and
- Request approval from the meeting organizer for guests to access them and their recordings.

In general, here are enumerated some recommendations to protect yourself properly against cyber incidents:

- Use only devices authorized by your organization;

- Do not share these authorized devices with your family members;
- Make sure your home WI-FI has a strong password and, if you haven't already, take the time to change it;
- Make regular backups to an external device.
- Always use your organization's VPN;
- Do not open emails or SMS, or click on any unknown links or attachments (beware of phishing related to the COVID-19 pandemic); and
- Do not share professional information on social networks.

For organizations, I can enumerate some measures as well:

- Ensure that the devices are up to date and have an antivirus and firewall enabled;
- Provide a VPN for remote access of your employees to vital information resources;
- Provide secure authentication means for your employees;
- Ensure adequate support in case of incidents or doubts of your employees. Remember that this is a new situation for everyone; and
- Limit access to systems and folders with sensitive data.

Notice that in this unprecedented pandemic situation, teleworking and collaboration tools are crucial. Today, the priority should keep people safe and facilitate their work from anywhere, at any time and thought any device. With this mindset in place, companies remain connected to their teams and can continue their day-to-day operations safely.

About the Author

Pedro Tavares is a cybersecurity professional and a founding member of CSIRT.UBI and Editor-in-Chief of seguranca-informatica.pt. In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, malware, ethical hacking (OSCP-certified), cybersecurity, IoT and security in computer networks. He is also a Freelance Writer.

Segurança Informática blog: www.seguranca-informatica.pt

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

Twitter: https://twitter.com/sirpedrotavares

Contact me: ptavares@seguranca-informatica.pt

KPMG Recommends Steps to Bolster Cybersecurity in the COVID-19 Era

By Ton Diemont, Head of Cybersecurity at KPMG in Saudi Arabia

Hackers are jumping on the COVID-19 pandemic to exploit global uncertainty

Riyadh, 07 April 2020 : The outbreak of Covid-19 poses a challenge to many businesses across the globe, also impacting information security as ill-wishing threat actors actively seek to exploit the situation. With the increasing use of remote technology and employees working from home, it is crucial that cybersecurity is included in contingency planning and has the attention of the Board.

Since the worldwide outbreak of Covid-19, there has been an increase in malware using the virus itself as the bait. Cybercriminals try to take advantage of global uncertainty and disruption with additional phishing, online scams and malware installed via Covid-19 heatmaps and social media campaigns, according to KPMG in Saudi Arabia.

In light of these insights, Ton Diemont, the firm's Head of Cybersecurity in Saudi Arabia, recommends steps to best prepare for the current threat landscape for Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) in order to offer a solution to protect employees that are working from home.

- Ensure to inform your employees how they can work securely and safely, and how they should handle situations in case of doubts
- Make sure the employees are aware of what the protocol is in case of incidents or doubts
- Ensure your helpdesk is fully operational
- Be vigilant for phishing emails or whaling (i.e. phishing attacks which specifically target your CxO level)
- Ensure that you as CIO and CISO are included in business decisions related to the crisis. Therefore, be part of the crisis management organization and demonstrate your added value as a trusted advisor, as security measures will be challenged or relaxed during the crisis
- Above all, think in solutions, not in bottlenecks

"Organizations that want to protect themselves from these types of crisis must ensure to incorporate these types of scenarios in their periodic risk assessments at board and operational level. No one can deny that the likelihood of this threat is insignificant or nihil and that investments to deal with, or avoid, these risks will be wisely applied by senior management," asserts Diemont.

As a result of Covid-19, most of the increased spending for companies can be traced back to increased demand of infrastructure and tools/software to support staff that are working from home and has been implemented on short notice. Other cost centers are IT helpdesk facilities and staff.

These additional security measures that were implemented hastily may turn out to be more expensive than under normal circumstances, believes Diemont, adding that these measures can be re-evaluated when business returns to normal.

"While the Covid-19 pandemic will significantly impact businesses, the current view of, unfortunately, most senior management is that cybersecurity is merely seen as a cost center rather than a business enabler or business saver. Hence, cybersecurity is critical to collective resilience and must be considered foundational," he concluded.

About the Author

Ton Diemont, Head of Cybersecurity at KPMG in Saudi Arabia. Ton Diemont is a Director based in KPMG's Riyadh office with over 25 years of experience in cybersecurity, IT and Operational Risk Management and Financial Services. He worked over 21 years with leading financial institutions in the Netherlands, serving in the positions of CISO and Corporate Head of IT Risk in the last six years. He worked with many central banks, regulators and organizations within the financial services sector. He has a special interest in assisting financial institutions with their cybersecurity and risk governance customer centric transformation programs.

Modernizing Government Processes Requires Modern Cybersecurity Practices

By Anthony Bettini, CTO, WhiteHat Security

According to IDG, 89% of companies have recently adopted a digital-first business strategy or plan to do so. As part of this pattern, the government sector is increasingly relying on web-based applications and digitized forms--think the DMV, passport renewal, property tax payments, toll bill payments, election voting applications and more processed over the internet for both agency and citizen convenience.

By having forms and payments easy to complete online, this makes everyone's lives easier by speeding up, simplifying and storing information in databases. The modernization of these processes has not only made government and political involvement arguably more accessible, it also reduces the likelihood for human error or misconduct.

Although these applications have been proven to make the public sector more effective and efficient, they raise just as many concerns— some of which are integrity-related and many of which are cybersecurity-related. The public sector handles high-stakes events like elections and sensitive personal information, such as full names, addresses, social security numbers, financial details and more, which could easily be left vulnerable without proper cybersecurity measures in place.

Recent government-driven, technology-related incidents include but are not limited to: 1) this year's Iowa caucus in the United States, where coding and testing errors in the voting application delayed election vote counting and fomented doubt in the results and 2) the breach at the Defense Information Systems Agency (DISA), which put nearly 9,000 government employees' personally identifiable information (PII) at risk.

With government-related websites and applications becoming prominent targets for cybersecurity attacks, many are fearful that their data is not properly protected. This attention should push development teams and organizations to ask themselves: As these web and mobile applications are being produced and implemented, how are they being tested-- and are cybersecurity best practices being put into place?

How can this be avoided?

With a pivotal election year underway, all eyes are on the cybersecurity of the voting software, especially in light of reported interference in the last presidential election. As past voting breaches are being assessed, many are wondering if there was a way that these attacks could have been avoided. With healthier software development practices, modernizing government processes does not have to be a nightmare.

Working as a team is an efficient way to improve software development to push for increased security. One way to put this into effect is to implement a DevSecOps approach, which combines security into the DevOps process. This helps find and prevent vulnerabilities and other concerns earlier on in the process and better equips teams to make the necessary preparations and protections against potential breaches. By shifting security left and introducing security earlier in the development process, security professionals and engineers work in tandem to produce a more holistic and secure application.

Although identifying the need to work with a team is important, a great starting point for breach avoidance is appropriate planning and testing of the application with security as a focal point. Having a remediation plan and defined process prepared before a vulnerability is uncovered, quickens the process to correct it. After planning for potential vulnerabilities, a good practice is to perform penetration testing, which ensures that your plan is effective and highlights any cyberthreats.

Application security is becoming more important, not only because it protects companies from reputation damage, but also because as more processes are quickly becoming digital, more personal data is being put at risk without it. According to WhiteHat Security's 2019 Application Security Statistics Report, when 350 Android applications were analyzed, 70 percent leaked personally identifiable information.

If vulnerability testing is not prioritized throughout the development process, there could be ramifications, including extended timelines and increased expenses. In an ever-changing security field, automated testing platforms are beneficial because they keep developers akin to miscellaneous security flaws that may arise after the application is deployed.

Every year there is a positive trend of people using the internet and mobile devices, showing that more everyday activities may be made available digitally. Disenfranchised groups, including people with disabilities, are now able to participate in civic activities with little to no additional stress because of the increased accessibility from applications.

Although the modernizing of these processes has improved the quality of life for the public, and may add an extra layer of security from direct human tampering, the threat of application vulnerabilities is more prevalent. Once cybersecurity is prioritized while developing government applications, the move to computerized civic processes can live up to its potential.

About the Author

Anthony Bettini is the Chief Technology Officer for WhiteHat Security. Previously, Anthony ran Tenable Research where he joined via Tenable's acquisition of FlawCheck – a leading Container Security startup where Anthony was the Founder and CEO. Before FlawCheck and Tenable, Anthony was the Founder and CEO of Appthority, a leading Mobile Security startup and winner of the "Most Innovative Company of the Year" award at the RSA Conference. Anthony led Appthority to successful acquisition by Symantec in 2018. At WhiteHat, Anthony leads product management and development, engineering and threat research.

The Cyber Challenges of the 21st Century

By Emil M.Hasanov

The National Cyber Strategy demonstrates my commitment to strengthening America's cyber security capabilities and securing America from cyber threats. It is a call to action for all Americans and our great companies to take the necessary steps to enhance our national cyber security. We will continue to lead the world in securing a prosperous cyber future.

—President Donald Trump [1]

Nowadays, we are witnessing the increase of the cyber crime-attack related incidents and the impacts are becoming more damageable. This fact alarming about importance to improve security measures to mitigate the risks and impact in the area of critical infrastructure. Analyzing the problems related to the security of critical infrastructures we can see that human factor based on the level of awareness heavily affects cyber attacks and its consequences. The threat to critical infrastructure is becoming more real and severe and it is necessary to be aware about it and accordingly anticipate, predict and make appropriate actions to be fully equipped for a cyber attack. As it is mentioned above the main reason for the escalation of cyber attacks against the field of Critical Infrastructure (CI) is the fact that most control systems used for CI do not use appropriate protocols and software. And instead of that they adopt standard solutions that not applicable for all cases. As a result, critical infrastructure systems are more than before becoming vulnerable and uncover to cyber attacks.

[1] National Cyber Strategy of the United States of America, September 2018

Critical Infrastructure

Nowadays, there is a slight difference between countries and international institutions concerning their definition of critical infrastructure (CI) and sectors.

European Commission defines is the following: critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions; [2]

UNDRR (United Nations Office for Disaster Risk Reduction) defines is the following**:** The primary physical structures, technical facilities and systems which are socially, economically or operationally essential to the functioning of a society or community, both in routine circumstances and in the extreme circumstances of an emergency. [3]

NATO defines is the following: Physical or virtual systems and assets under the jurisdiction of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment.[4]

The US approach is more comprehensive and inclusive, and it has been particularly evolving since the attacks of September 11, 2001.

The United States defines is the following: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[5]

Homeland Security Act of 2002 established the Department of Homeland Security (DHS) and also formally introduced the concept of "key resources**"** "Key resources" are defined as "publicly or privately controlled resources essential to the minimal operations of the economy and government"

---

[2] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Article 2 a, Definition

[3] 2009 UNISDR Terminology on disaster Risk Reduction, United Nations international Strategy for Disaster Reduction (UNISDR), Geneva, Switzerland, May 2009

[4] Tallinn Manual on International Law on the International Law Applicable to Cyber Warfare, Michael N. Schmitt, March 2013

[5] The USA PATRIOT Act (commonly known as the Patriot Act) is an Act of the United States Congress that was signed into law by U.S. President George W. Bush on October 26, 2001.

Critical Infrastructure Sectors

Each national or international strategy and policy identifies different categories of sectors that are considered to offer vital services and thus require protection. A 2008 survey examined the policies of 25 countries and identifies as the most frequently mentioned the following sectors:[6]

- Banking and Finance
- Central Government
- (Tele-)Communication / Information and Communication Technologies (ICT)
- Emergency -Rescue Services
- Energy / Electricity
- Health Services
- Transportation / Logistics / Distribution
- Water (supply)
- Food (supply)
- Environmental Protection

European Definitions[7]

The EU directive identifies the following two **sectors** and their respective sub-sector:

I Energy

II Transport

UNDRR (United Nations Office for Disaster Risk Reduction)

Critical facilities are considered as elements of the infrastructure that support services in a society.[8]

US Critical Infrastructure sectors

There are 16 critical infrastructure sectors in the US whose assets, systems, and networks, whether‘ physical or virtual, are considered so vital to the United States that their incapacitation or destruction

[6] E. Brunner, M. Suter, International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies, A. Wenger, V. Mauer, M. Dunn (Eds.), CRN Handbooks, Vol. 4, no. 1, Center for Security Studies (CSS), Zurich, Switzerland, September 2008.

[7] Council Directive 2008/114/EC

[8] 2009 UNISDR Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction (UNISDR), Geneva, Switzerland, May 2009

would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.[9]

Cyber attacks

Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure.

In fact, every year malware from unlicensed software costs companies and governments worldwide nearly $359 billion a year, or $10,000 per infected computer.

According to Daniel R.Coats, (Director of National intelligence) China and Russia pose the greatest espionage and cyber attack threats, but US anticipated and equipped accordingly. These countries increasingly build and integrate cyber espionage, attack, and influence capabilities into their efforts to influence US policies and advance their own national security interests.

China

According to Daniel R. Coats China authorize cyber espionage against key US technology sectors. US expressed its concerns about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies. [10]

Russia

According to the United States Intelligence Community's report of 2019 Russia poses a cyber espionage, influence, and attack threat to the United States and its allies. Moscow continues to be a highly capable and effective adversary, integrating cyber espionage, attack, and influence operations to achieve its political and military objectives.

Following to the report Russian intelligence and security services will continue targeting US information systems, as well as the networks of our NATO and Five Eyes partners, for technical information, military plans, and insight into our governments' policies. [11]

Iran

Iran uses increasingly sophisticated cyber techniques to conduct espionage; it is also attempting to deploy cyber attack capabilities that would enable attacks against critical infrastructure in the United States and allied countries. Tehran also uses social media platforms to target US and allied audiences, an issue discussed in the Online Influence Operations and Election Interference section of this report.

[9] Homeland Security Presidential Directive 7,US December 17, 2003

[10] Statement For The Record Worldwide Threat Assessment Of The US Intelligence Community January 29, 2019, Daniel R. Coats, Director of National Intelligence, Senate Select Committee for Intelligence page 5

[11] Ibid.

Iran is capable to cause disruptive effect on companies' corporate networks for weeks that it was done for data deletion attacks against Saudi Arabia governmental and private-sector networks in late 2016 and early 2017. [12]

North Korea

North Korea has a capacity for the cyber threat to financial institutions. North Korean cybercrime operations included attempts to steal more than $1.1 billion from financial institutions around across the world.[13]

Another group of the cyber criminals can be attributed to non-state and unattributed Actors

Terrorists could obtain and disclose compromising or personally identifiable information through cyber operations, defacing websites or executing denial-of-service attacks against poorly protected networks—with little to no warning. [14]

In fact, every year malware from unlicensed software costs companies and governments worldwide nearly $359 billion a year, or $10,000 per infected computer. One study conducted last year showed that organizations now face a nearly one-in-three chance of encountering malware when they obtain or install unlicensed software.[15]

Analyzing the governmental expenditures we can see the increase for example the US FY 2019 President's Budget includes $15 billion of budget authority for cyber security-related activities, a $583.4 million (4.1 percent) increase above the FY 2018. US DOD was the largest contributor to this total. [16]

Worldwide spending on information security (a subset of the broader cyber security market) products and services exceeded $114 billion in 2018, an increase of 12.4 percent from 2017, according to Gartner, Inc. For 2019, they forecast the market to grow to $124 billion, and $170.4 billion in 2022.[17]

In April 2019 European Commission recommendation highlighted some points that the cyber security of the energy system, and the electricity grid, needs a dedicated sectorial approach.[18]

The EU has one of the most reliable electricity grids in the world, and possible vulnerabilities have not so

---

[12] Statement for the record worldwide threat assessment of the us intelligence community January 29, 2019, Daniel R. Coats, director of national intelligence, senate select committee for intelligence page.6

[13] Statement for the record worldwide threat assessment of the us intelligence community January 29, 2019, Daniel R. Coats, director of national intelligence, senate select committee for intelligence page.6

[14] ibid.

[16] 21 cyber security funding, federal budget authority, www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf , accessed 15 february 2020

[17] Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021, Cybersecurity Ventures' 2019 Cybersecurity Market Report sponsored by Secure Anchor Steve Morgan, *Editor-in-Chief, 10 June 2019*

[18]Cybersecurity of critical energy infrastructure, EPRS European Parliamentary Research Service. Auhor: Gregor

far been exploited to disrupt the energy supply on a large scale. [19]

The American and European approaches in this area present many differences. The United States has favored a strategy of 'security in depth' with strict and detailed regulations in specific sectors, which are implemented by institutions possessing coercive powers. The EU has adopted a more flexible and exhaustive approach covering a wide range of issues, leaving an important margin of maneuver for member states in the implementation of norms. No doubts the American system can serve as a model to improve certain weaknesses in the European approach, and vice versa, EU also can make its contribution as well.[20]

Nowadays, emerging threats are numerous: as all sectors of the economy rely on energy to operate, exploiting weaknesses in the grid's critical infrastructure has the potential to initiate a 'cascade effect' that hinders or halts operations in other sectors, such as transport, finance, and healthcare. Disabling the energy grid can provoke civil unrest, disrupt chains of communication, degrade military readiness, and generally impede a government's ability to respond quickly and effectively in a crisis situation. [21]

Notable incidents related to physical and cyber security of energy

Reports of hackers penetrating Russian and US power networks, 2019

In March 2019, the US grid regulator NERC warned[22] that a hacking group with suspected Russian ties was conducting reconnaissance[23] into the networks of American electrical utilities. In June 2019, the *New York Times reported* [24]that American 'code' had been deployed inside many elements of Russia's power network by US military hackers that were targeting Russian power plants. The claims were denied by President Trump and regarded with skepticism by cyber security experts.

---

[19] EPRS,European Parliament Research Service, Gregor Erbach, Jack O'Shea, Member's Research Service PE 642274, October 2019

[20] Ibid.

[21] Ibid.

[22] 'Most dangerous' hackers targeting U.S. utilities — report **Blake Sobczak**, E&E News reporter Energywire: Friday, June 14, 2019

[23] WIRED, The Highly Dangerous 'Triton' Hackers Have Probed the US Grid, Endy Greenberg,06.14.2019; https://www.wired.com/story/triton-hackers-scan-us-power-grid/ : accessed 16 February 2020

[24] The New York Times, U.S. Escalates Online Attacks on Russia's Power Grid, By David E. Sanger and Nicole Perlroth, 15 June 2019

Cyber-attack on petrochemical plant, Saudi Arabia, August 2017

Cyber-attack on a Saudi petrochemical plant attributed in August 2017 [25] was the first known attempt to manipulate an emergency shutdown system. The attack resulted in the plant shutting down and Cyber security experts from FireEye Intelligence reported of deployment of TRITON that attributed to the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM; a.k.a. ЦНИИХМ), a Russian government-owned technical research institution located in Moscow. [26]

Cyber-attacks on Ukrainian power grid, 2015 and 2016

In December 2015, hackers attacked the computer system of a western Ukrainian power utility, and cut off the electricity to some 225 000 people. [27] In February 2016, U.S. Deputy Energy Secretary Elizabeth Sherwood-Randall attributed the first attack on the Ukrainian grid to Russia at a meeting with U.S. energy industry executives. The experts drew the attention to the Sandworm Team that has targeted NATO, European governments, and industrial control systems generally. In February 2017, Ukrainian officials blamed Russian security services and the group behind the BlackEnergy3 malware.[28]

Baku-Tbilisi-Ceyhan oil pipeline explosion, Turkey, 2008

The Baku-Tbilisi-Ceyhan (BTC) oil pipeline in Turkey experienced a rupture and fire in 2008[29]. The Kurdish Workers Party claimed responsibility for the cyber attack on 6th August 2008 on the BTC pipeline that occurred inside of Turkey near the town of Refahiye. The physical rupture led to escaped product ignition and an explosion resulting in a fire that was extinguished by firefighters on August 7, 2008. The

---

[25] The New York Times, Hack of Saudi Petrochemical Plant was coordinated from Russian Institute, Christophe Viseux, 23 October 2018, https://www.nytimes.com/2018/10/23/us/politics/russian-hackers-saudi-chemical-plant.html :accessed 15 February 2020

[26] The New York Times, Hack of Saudi Petrochemical Plant was coordinated from Russian Institute, Christophe Viseux, 23 October 2018, https://www.nytimes.com/2018/10/23/us/politics/russian-hackers-saudi-chemical-plant.html :accessed 15 February 2020

Hackers behind Ukraine power cuts, says US report, BBC News, 26 February 2016, **https://www.bbc.com/news/technology-35667989**: accessed 14 February 2020

[28] Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks, Donghui Park, Julia Summers,Michael Walstrom 11 October 2017 , https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/#_ftn15 :accessed 16 February 2020

[29] A Cyber Attack May Have Caused a Turkish Oil Pipeline to Catch Fire in 2008,Ariel Bogle,11 December 2014, **https://slate.com/technology/2014/12/bloomberg-reports-a-cyber-attack-may-have-made-a-turkish-oil-pipeline-catch-fire.html** :accessed 17 February 2020

pipeline was out of commission till August 25, 2008.[30]

The investigations found that an elaborate cyber-attack caused the explosion, where the perpetrators turned off all the distress signals and erased 60 hours of surveillance video. According to Bloomberg, the main weapon of the attackers was a keyboard, as they hacked into the control room, cut off communications and maximized the pressure in the pipe lines.[31]

The incident occurred at a time when tensions between Russia and Georgia were building towards armed conflict. Russia officially deployed troops into the Russian-Georgian conflict two days after the pipeline explosion occurred. Cyber attackers accessed the control system of the pipeline via internet-connected security cameras and gained access to the industrial control systems to raise the pressure in the pipeline, causing it to rupture.[32]

Critical Infrastructure Protection Measures

EU

Cyber security Act: Regulation (EU) 2019/881 cyber security package (Cybersecurity Act), which is part of the 2017 and entered into force in June 2019, aims to strengthen the EU's response to cyber-attacks, improve cyber-resilience and increase trust in the digital single market. The Act empowers the European Union Agency for Cybersecurity (ENISA)– to improve coordination and cooperation in cybersecurity among EU Member States and EU institutions. It establishes an EU cybersecurity certification framework for specific categories of information and communication technology products, processes and services.[33]

Security of Gas Supply Regulation: Regulation (EU) 2017/1938 deals with gas supply shortages caused by a number of risk factors, including cyber-attacks, war, terrorism and sabotage. [34]

In April 2019, the Commission issued Recommendation (EU) 2019/553 that member states should take appropriate measures that includes cyber security risk analysis and preparedness when making decisions about infrastructure.[35]

---

[30] ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack, Robert M. Lee Michael J. Assante Tim Conway, ICS Defense Use Case (DUC), Industrial Control Systems, Dec 20, 2014, https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf :accessed 17 February 2020

[31] Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar *Jordan Robertson and Michael Riley,* 10 December, 2014, https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

[32] ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack, Robert M. Lee Michael J. Assante Tim Conway, ICS Defense Use Case (DUC), Industrial Control Systems, Dec 20, 2014, https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf :accessed 17 February 2020

[33]EPRS, European Parliament Research Service, Gregor Erbach, Jack O'Shea, Member's Research Service PE 642274, October 2019

[34] *Ibid.*

[35] Ibid.

United States of America

The 2005 Energy Policy Act in the United States was the first important legislation to address the growing challenge of cybersecurity in the energy sector. The mentioned legislative act was adopted as a response to the North-east blackout of 2003 that left 50 million North Americans without power. The act granted the Federal Energy Regulatory Commission (FERC) the ability to appoint an Electric Reliability Organization (ERO) responsible for reliable standards for all bulk power electric utilities in the country.

The North American Electric Reliability Corporation (NERC), a private non-profit organisation, was designated as the ERO for the United States and several Canadian provinces in 2006. The NERC is responsible for developing a list of Critical Infrastructure Protection-CIP standards (NERC-CIPs) that at the end should be reviewed by the FERC.

The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is designed to lead the Department of Energy's coordinated response to disruptions by partnering with the National Laboratory system, private sector coordinating organisations, and state and local governments. The cybersecurity risk information-sharing program (CRISP) is a public-private data sharing and analysis platform that facilitates the timely bi-directional sharing of unclassified and classified threat information among energy sector stakeholders.[36]

[36] Cybersecurity Risk Information Sharing Program (CRISP), Enhanced threat analysis with U.S. Intelligence insights for faster threat identification and mitigation, US Department of Energy, https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf :accessed 19 February 2020

About the Author

Emil M.HASANOV (L.L.M) studied Law in Baku State University (Azerbaijan), University of Geneva Switzerland. Completed programs in Cranfield University (Defense Academy)-Cranfield Mine Action (UK), Carlton University (Canada), George Washington University, Thunderbird School of Global Management", USEUCOM-US European Command (and other reputable int. institutions). Conducted lectures in Cranfield Academy, MFA of Azerbaijan (NATO winter school), MFA of Georgia.
Used to work for the Ministry of Justice (retired captain of Justice), provided advisory service for MFA of Azerbaijan, Germany and Slovenia. Used to work as a Head of Operations (Deputy Director of Agency) for UNDP/ANAMA- Azerbaijan National Agency for Mine Action, researcher/editor of Geneva-based Land Mine&Cluster Munitions Monitor (21 countries/ areas CIS/MENA), Regional Adviser of Slovenian International Trust Fund for South Caucasus (Slovenia-Georgia).Strategic Capacity Development Adviser of UN Peacekeeping Operations-UN Hybrid Operations for Darfur-UNAMID (Sudan)., Transition Manager/ Legal Advisor of US Dep. of State program to MoD Georgia, International Expert of OSCE-Ukraine and other int. organizations. Emil had different assignments with UN, NATO/NAMSA, EC-EEAS, OSCE. Co-founder of **Club de Geneve (Geneva-based think tank** www.clubofgeneva.org)

Emil had missions/assignments to armed conflict-affected countries/ areas: Georgia, Ukraine, Yemen, Turkish-Syrian, Turkish-Iranian, Tajikistan-Afghanistan Borders, Darfur (Sudan), Cyprus, Bosnia and Herzegovina, Iran.
The author of articles published in Azerbaijan and the USA. The charter member of the Rotary Club of Baku International- RCBI. Past President of RCBI, past Assistant Governor RI District 2430 (Azerbaijan)**.** 2430 RI District Assistant Governor (Afghanistan, Tajikistan, Turkmenistan and Uzbekistan).
Currently is working in Communication & External Affairs of International Energy company

Debunking the Top Myths in Vulnerability Management for A Safer Enterprise

By Dr. Deepak Kumar, Founder and CEO, Adaptiva

Cybersecurity is one of the most daunting challenges enterprises will face in 2020. According to IBM's 2019 Cost of a Data Breach report, the average cost of a data breach in the U.S. is $8.19 million, with companies averaging 206 days to identify breaches before even attempting to address them (a task that averages another 38 days).

These stats and hundreds of others on cybercrime are quite sobering. Cyberattacks are beginning to seem like an inevitability, another cost of doing business. Yet, a lot can be done to reduce risk, particularly when it comes to vulnerability management.

Top vulnerability management myths

The Importance of vulnerability management is often discounted or overlooked. Let's look at and debunk the top vulnerability management myths, so that enterprises may opt to change their practices in ways that make fortifying cyber defenses and reducing risks significantly easier.

Myth 1: Periodic scanning is enough

One common and dangerous myth to dispel is that periodic vulnerability scans are good enough. Not true. Even once a day is no longer enough. New apps and endpoints are added to corporate networks each day — and this does not happen in unison at 8 am. Changes are made throughout the day, which means network compromise can happen at any time. And it can take a mere 18 minutes for hackers to go from foothold to a full-on breach.

Companies can't just scan once per day, even if they fix a number of vulnerabilities every day. The rate at which new vulnerabilities appear is simply too high. Enterprises must scan continuously to be protected. Fortunately, new vulnerability management solutions make scanning at scale significantly faster and easier without impacting network performance, so there is really no good reason why enterprises should put networks at risk unnecessarily.

Myth 2: Vulnerabilities = patching

Many people equate vulnerabilities with patching. In reality, vulnerability management can be much more detailed and complex. For example, a configuration change might solve an issue, or if a company is running an old piece of software, a patch or configuration update might not be available. In this case, teams might need to put in a mitigating control, such as a firewall or routing change, to prevent certain types of traffic from getting to a port or application. In fact, sometimes mitigating controls work better than patches.

The bottom line is this: to think solely in terms of patching is short-sighted. Taking a broader view of vulnerability management will serve organizations better.

Myth 3: Fixing critical vulnerabilities ensures safety

The view that organizations have to fix Level 5 vulnerabilities first is outdated. Conventional logic goes that the most serious vulnerabilities demand immediate attention. The problem is that cybercriminals are aware of this mentality. As a result, they've begun attacking lower hanging fruit in middle-layer vulnerabilities. These are not as attention grabbing; they don't have people playing beat-the-clock to remediate them, which gives hackers longer to figure out a way in, and they can ultimately cause tremendous damage as they go undetected for long periods of time.

When it comes to vulnerability management, companies need to adjust their approach. They either need to adopt new considerations and ranking systems for how they address vulnerabilities or they should opt for a two-pronged strategy, leveraging automated vulnerability management solutions to immediately remediate lower level vulnerabilities while freeing up team members to fix higher level vulnerabilities simultaneously.

Myth 4: Vulnerability management is no big deal

There is a distinct lack of respect for vulnerability management. Whether it is from teams that adopt a certain arrogance about their abilities — a "my guys can fix anything manually" attitude — or those that operate under the assumption that vulnerability management is a low priority background task, the result is the same: vulnerability management has taken a back seat.

The problem is that there are simply too many vulnerabilities popping up too quickly. Even the most talented, best staffed teams are not equipped to deal with all of them. By viewing them as a lower priority or letting vulnerability management fall by the wayside due to a lack of time or resources, companies open the door to cyberattacks, ultimately making their jobs exponentially more difficult in the long run — not to mention potentially costing their companies millions of dollars if/when a breach occurs.

Some companies that hold cyber insurance policies may feel a false sense of safety. I would urge these organizations to take a look at Merck or Mondelēz, which held policies they perceived will protect them financially in the event of an attack. They were wrong. After NotPetya, their claims have been denied through a loophole that declared NotPetya an act of war. Today, these companies are hundreds of millions of dollars out of pocket and are tied up in legal battles with their insurance companies – battles that are expected to take years to resolve.

I would encourage all IT teams to prioritize vulnerability management, throw out their preconceived notions and myths. It may not be the sexiest task IT teams deal with but vulnerability management very well could be the biggest factor in preventing a serious malicious attack.

As first published in Help Net Security.

About the Author

Dr. Deepak Kumar is the founder and chief executive officer at Adaptiva. He is responsible for overseeing the company's ability to execute on its strategic product vision in the endpoint management and security space. He was the lead program manager with Microsoft's Systems Management Server 2003 team and program manager with the Windows NT Networking team. Prior to Microsoft, he was a group manager for IP Telephony products at Nortel. Dr. Kumar has received five patents related to his work on SMS 2003 at Microsoft and has written more than 50 publications, including a book on Windows programming. While at Microsoft, Dr. Kumar also authored the Think Week paper for Bill Gates that became Project Greenwich, now known as Microsoft Office Communications Server/Lync. Deepak is an avid outdoorsman and hiker. For more information, please visit https://adaptiva.com and follow the company on LinkedIn, Facebook and Twitter.

Practical Vulnerability Remediation Strategies

By Syed Abdur, Brinqa

Cyber vulnerabilities have a way of piling up. Vulnerability assessment and scanning tools report them in droves from every corner of the technology infrastructure – network, applications, cloud, containers, mobile, IoT, etc. Penetration testing programs proudly display vulnerabilities as the mark of a job well done. Threat intel sources generously send lists of them to you. Vendors send out notices and patches. It's overwhelming. Even with the best of intentions, you could easily build up a backlog of hundreds, if not thousands, of vulnerabilities to remediate. In larger companies, this number is frequently in the *millions*. You want to take care of them all, but some are more important than others.

Practical remediation strategies can help you deal with this daunting challenge. They give you effective, realistic ways to reduce your backlog of vulnerabilities intelligently and efficiently. These include strategies such as incorporating business context and leveraging threat intel to help you identify and prioritize the vulnerabilities that pose the biggest risk to your organization. By grouping vulnerabilities for remediation and integrating existing IT Service Management (ITSM) tools and processes, organizations can help reduce the overhead associated with tracking and remediating vulnerabilities, freeing up valuable cybersecurity resources. Strategies such as developing and enforcing rules and policies for SLAs and ownership assignment, and automating the validation of remediation efforts, can significantly improve the consistency and effectiveness of your vulnerability management program.

Overcoming the "Remediation Gap"

The backlog of un-remediated vulnerabilities is only partly a matter of numbers. Yes, there are a ton of them. However, structural issues can affect the remediation process as well. The time between a vulnerability being detected, i.e. discovered and reported to the right platforms, and the creation of a ticket that tasks a person with fixing the problem can stretch into months—during which time the system in question is exposed.

Manual processes are the major culprit here. Assessing the severity and impact of individual vulnerabilities manually is error-prone and can lead to inconsistent results. This problem is exacerbated by IT staffers lacking a complete, unified set of information about the nature and impact of a vulnerability. Even a well-organized team can work only so efficiently when they have to manually toggle between multiple systems to take care of remediation.

New solutions are emerging that address the remediation gap by automating key aspects of the vulnerability prioritization and remediation process. These solutions normalize and correlate the disparate data that defines vulnerabilities, presenting a complete picture to InfoSec professionals. For example, the information that fully describes the risk posed by a vulnerability affecting an ERP solution might be spread out across the vulnerability scanner, firewall logs, endpoint detection and response solutions, multiple threat intel feeds, and ticketing systems.

Seven Practical Remediation Strategies

The right approach to vulnerability remediation will give priority to the most pressing risks in the most efficient way possible. The remediation efforts will be validated, so all relevant stakeholders can be confident the matter was properly handled. The staffers doing the remediation work will be adequality informed about what they're doing so they understand the priorities and impacts of their processes. The work will be consistent, with clear ownership of tasks and responsibilities. The following seven practices help ensure these outcomes.

1. **Incorporate business context**—Not all vulnerabilities affect a business equally. In fact, the same vulnerability can pose very different risks to a business depending on where it exists in the technology infrastructure. Does a vulnerability impact the availability of a critical business function? Does it threaten to expose sensitive or confidential information? Does a vulnerability, if unpatched, put your organization at risk of failing compliance? These questions are impossible to answer by looking only at the technical aspects of a vulnerability instance. The good news is that the information needed to build comprehensive business context for vulnerability analysis already exists in your organization. Business continuity and disaster recovery initiatives measure the business impact of technical assets. Data protection programs keep track of where sensitive information resides in your organization. Audit programs monitor assets that determine compliance with various standard. By identifying and incorporating this information during vulnerability analysis and prioritization, you can drastically improve the effectiveness of your vulnerability remediation efforts.

2. **Leverage threat intel**—Just as business context helps you understand and communicate the internal impact of a vulnerability to your organization, threat intel represents the external, global implications of a

threat. Is a particular vulnerability being weaponized by a known malicious actor? Are there malwares and toolkits that leverage a vulnerability for exploit? Is there a spike in chatter around a vulnerability on the dark web? Updated much more frequently than vulnerability databases, threat intel can also help identify risks, e.g. “Zero Day” exploits, that may not yet be accounted for by vulnerability scanning systems. By incorporating threat intel in the vulnerability analysis and prioritization process, organizations can respond to threats faster, and proactively stay ahead of malicious actors.

3. **Consolidate vulnerabilities**—The backlog of vulnerabilities invariably contains multiple tickets that address the same issue. With a system that can identify comparable vulnerabilities and group them together, the volume of remediation work can be reduced dramatically. If you fix one vulnerability, that might automatically knock down dozens of other tickets that convey the same information.

4. **Develop and enforce SLAs and ownership rules**—It’s a good practice to be clear and consistent about the organizational aspects of vulnerability remediation. A Service Level Agreement (SLA) can help establish how promptly a particular vulnerability will be addressed. Ownership is the necessary twin rule to match the SLA. The IT organization needs to be able to say, “Yes, we will remediate this within 24 hours and John ‘owns’ the process.” That way, John knows exactly what is expected of him. To make this work, however, your vulnerability management program should provide mechanisms to codify this knowledge as rules or policies, and apply them automatically during vulnerability analysis and ticket creation.

5. **Use existing ITSM tools and processes**—Most organizations already have an IT Service Management (ITSM) platform such as JIRA or ServiceNow to track IT tasks, software bug fixes and the like. It’s wise to use this incumbent ITSM to manage remediation work. Adding another ticketing system adds to confusion and inefficiency. And, as often happens, remediating vulnerabilities aligns with other IT maintenance processes, so it makes sense for all tickets to be on the same system.

6. **Validate intelligently**—This may sound obvious, but a sound remediation strategy will include a validation step. You should make every effort to avoid turning validation into a second, backlog-ridden workload. One way to do this is to automatically update tickets by verifying vulnerability status on subsequent scans. To further shorten the loop, you can trigger micro scans that check for specific vulnerabilities on target systems instead of waiting for regularly scheduled scans to validate fixes.

7. **Automate**—Eliminating manual steps in the vulnerability analysis, prioritization, and remediation process is arguably the most significant way to overcome the remediation gap. Automation saves people time and helps reduce errors that occur as staffers toggle between systems and re-key data from one place to another.

These strategies work together synergistically. Applied correctly, they contribute to keeping the vulnerability backlog to a minimum and proactively closing the remediation gap. It is possible to get better at remediating vulnerabilities—reducing risk exposure in the process. All it takes are the right tools and the best practices outlined above.

About the Author

Syed Abdur, Director of Product Management
BIO: Responsible for driving product strategy and technical direction of the Brinqa product lines. Ownership includes development roadmaps, product design, feature design, strategic technical integrations.

A Guide to Firewalls: Best Firewalls for VOIP And Unified Communications

By Christopher Gerg, CISO and VP of Cyber Risk Management, Tetra Defense

The overwhelming popularity of VoIP Private Branch Exchange systems (PBX) in the modern workplace demonstrates that the benefits afforded to businesses over cost reductions, system flexibility and future growth are real, mainstream and very popular. Like any network-enabled infrastructure service, a phone system must be secured to best practice standards from security threats and vulnerabilities.

Introduction to Firewalls

The first line of defense for VoIP and Unified Communication systems is a perimeter firewall. It is designed to secure, manage and monitor ingress and egress network traffic based on a predefined security configuration.

The firewall controls the network packet exchange between the trusted internal network and untrusted external internet. telephone systems often incorporate VoIP firewalls, Session border controllers (SBC) and secured SIP trunking to create an assured telephone ecosystem.

Software versus Hardware Firewalls

Firewalls are available as physical hardware or software appliances that can be deployed into virtual or cloud environments. Deciding which flavor to deploy depends on the use-case scenario. For global organizations with large, multi-site call centers then hardware firewalls might be a more appropriate solution, simply because of the load and bandwidth requirements of many thousands of simultaneous voice operations.

Software firewalls are extremely popular in SMB environments, the firewall is virtualized which offers incredible flexibility for scaling and phone system management. Software firewalls make regular system upgrades significantly more straightforward and enables the capability to easily roll back in the event of errors.

Potential Threats to VoIP and Unified Communications

Information security specialists often group potential threats targeting VoIP and unified communications into three categories: *confidentiality*, *integrity,* and *availability*. This is sometimes referred to as the CIA Triad security model.

Confidentiality specifically relates to retained telephone data such as conversation content, voicemails and call history. Phone conversations can potentially be eavesdropped on if systems are incorrectly configured or inadequately protected. Confidentiality can also be violated unintentionally through human error, carelessness, or inadequate security controls.

The *Integrity* of telephone systems requires that data remains unaltered at all times and that the data is correct, authentic and reliable. Threats to data integrity can include caller identification spoofing, cases such as the incoming caller ID being deliberately altered to mimic a genuine organization - such as a credit card company. Hackers can potentially use this information to impersonate proxy telephone systems to reroute (hijack) phone calls, often with the intention to defraud.

Availability relates to the uptime of the phone system, the standard threats facing computer infrastructure can cause significant harm to telephone systems. Denial of Service (DoS) attacks can wreak havoc, with hackers flooding the telephone gateway or proxy servers to take down entire call centers and overload all the SIP trunks.

How Firewalls Protect Against Those Threats

Well-architected security firewalls can thwart and repel many of these threats. Implementing technical and procedural best practices can significantly reduce the risk and exposure of your business to outages and downtime.

At a technical level, diligent management of the telephone system must be mandatory, this includes system upgrades, patching, and infrastructure hardening. The firewall adds a secured gateway into the network, but if the rest of the network is running out of date software, then the entire system is at risk.

The firewall rules on the PBX must filter specific source IP address/domain combinations, including blocking out-of-scope open ports, implementing MAC address filtering, and blocking dangerous, suspicious or unauthorized network access.

Rules must be created that block untrusted web access from outside the specified IP address range, and the firewall policy must be configured to drop all the packets and connections sent from unauthorized hosts (IP blacklisting). Also, separating the voice and data traffic routing over the network will secure the trunks on the PBX.

To protect the *confidentiality, integrity,* and *availability* of data there are a number of countermeasures to be implemented. Strong access controls (ACLs), authentication mechanisms (MFA) and encryption of data in the process, transit and storage are a great start to help protect *confidentiality*.

To safeguard *integrity*, firewalls must incorporate strong authentication mechanisms and access control processes. Being protected by digital certificates and encryption of the network traffic enhances the security of data. Modern firewalls provide additional security features such as an intrusion detection system and enhanced SIEM logging capabilities.

System engineers can protect the *availability* of VoIP firewalls by creating a redundant and fault-tolerant network architecture. The easiest way to do this is to double down on the firewall investment by having an HA network stack.

Furthermore, many organizations are choosing to add an additional layer of protection by leveraging an external denial of service protection solution, often from third-party managed service providers that repel brute force DDoS attacks.

Best Firewall Software for VoIP and Unified Communications

In our opinion, the best software firewall for VoIP and Unified Communications is the Cisco ASA series adaptive security virtual appliance. It provides firewall functionality, as well as integration with context-specific Cisco security modules and can be scaled for enterprise-level traffic and connections.

Although licensing of Cisco products is quite expensive, the overall product experience and the level of granularity that can be implemented is staggering. Cisco is the global leader in unified communications and is the industry standard for software appliances.

The Cisco ASA series delivers advanced threat protection and integrated security features. It is perfect for network defense, vulnerability protection, and DDoS attacks and is widely used in VoIP solutions.

Best Firewall Hardware for VoIP and Unified Communications

In our opinion, the best hardware firewall for VoIP and Unified Communications is a physical Fortinet Fortivoice phone system firewall. These appliances are robust, secure and can accommodate up to 50,000 phone users.

Fortinet bundle a number of services internally which require no additional licenses including auto-attendants, music on hold and remote extensions. There are a number of built-in web-based management tools that enable real-time call monitoring, fax services, and call recording.

Firewall Administration and Management

Firewall administration is performed using a central administrative panel that incorporates management tools for the entire phone system suite. This will typically include SLA monitoring, call monitoring, call recording, hunt group configurations, and user privileges.

Additionally, there are a number of integrated security features that streamline the deployment of WAN services. Default features include user management settings, administrative passwords, voicemail password policies, extension filtering and tools to secure video/call conferencing services.

About the Author

Christopher Gerg is the CISO and Vice President of Cyber Risk Management at Tetra Defense. He's a technical lead with over 15 years of information security experience, dealing with challenges of information security in cloud-based hosting, DevOps, managed security services, e-commerce, healthcare, financial and payment card industries. He has worked in mature information security teams and has built information security programs from scratch, leading them into maturity in a wide variety of compliance regimes.

Don't Enable Hackers and Employees at The Same Time

By Dor Knafo, CEO, co-Founder, Axis Security

When work from home went from a luxury to mandatory overnight, that put a lot of pressure on already stretched IT teams. The magnitude of the challenge has been underscored by the difficulty that even the largest, most well-funded businesses in the world are having when it comes to delivering services quickly in this new environment. Many organizations are struggling to scale their legacy VPN infrastructure because of licensing and limits to the hardware-bound infrastructure that prevents them from quickly scaling capacity. For users, these network-based, legacy access solutions are leading to a frustrating experience as they are being overrun with *all* employees (not just some) going remote 24x7.

For the average enterprise without unlimited resources, the situation is especially acute. Now it's not some, but all employees who require secure access to private business applications, anytime from anywhere. Not only that, but as always, a multitude of third parties, suppliers, and subcontractors also interact with the company daily and they continue to require remote application access.

IT teams need to provide this access immediately, or the gears of the business will grind to a halt. The challenge they face is scaling with speed, *and* security.

While this massive infrastructure and access shift is happening, malicious actors are living down to their reputation, targeting hospitals and healthcare institutions. They're also targeting weak home-based

infrastructure because that is where the workers are, and that infrastructure is assumed, rightly, to be easier to breach than an enterprise environment. Make no mistake, they know the changes that are happening to enterprises right now, and they are acting.

Providing remote, secure access to critical business applications is an extremely difficult proposition using traditional network-based access solutions. Most work from home employees are familiar with Virtual Private Network access. From a user perspective, this was a slow, clunky process even *before* there was an explosion of people trying to use the service.

What does this mean from a security perspective? Network-centric access approaches are based on trusted devices, and only have a single binary access decision at the beginning of each session. Once a session has begun, the VPN approach reveals another security shortcoming by bringing the user onto the network all the way to the application itself. What if that user has malicious intent, be they a hacker, a third party with access, or perhaps, an insider. They're now on a flat network, with access to extremely vulnerable legacy applications. Essentially, what businesses are being forced to do using legacy network-based access solutions is provide a dangerous level of access to inherently insecure and vulnerable applications, representing a massive security risk to the organization.

Application Access Security Without Compromise

There is a better way to enable access to critical business applications. You don't have to mess with the network. You don't have to bring every user on to the network right to the front door of highly vulnerable legacy applications. You can keep everyone off your network and you apps isolated...while actually making access easier.

The new way forward, now more than ever, is to leverage a secure application access cloud that acts as a broker between the end user, the network, and the application. The benefits to this approach are immediate and broad based both from a security and access perspective for end-users, it is rapid deployment and a familiar web interface, not that clunky VPN experience we've all grown tired of. This increases business agility and user satisfaction

For IT teams, the beauty of a cloud approach is that they're no longer required to make cumbersome network changes. They can deploy and scale users rapidly and integrate application access with existing identity solutions using a simple API.

From a security standpoint, the application access cloud allows the organization to implement a true zero trust approach to application access. Everyone is an untrusted user, separated from the network and the application itself. With a VPN, there is a binary yes/no decision point at the beginning of the session, and then the end-user is on the network, free to roam and interact with highly vulnerable legacy applications.

By leveraging an application access cloud, IT teams gain enhanced security by separating the user from the application, essentially upgrading legacy applications to the latest secure communications protocols without ever having to touch them. In addition to enhanced security are greater visibility, control, and analytics. Every user is tightly managed, every action is tightly reported and recorded. A dashboard

provides visibility into exactly what's going on across all users, at all times. This is the future; this is zero trust application access.

About the Author

Dor Knafo is co-founder and CEO of Axis Security. Axis Security was founded to solve the problem of secure application access for employees, partners, and other stakeholders. Axis Security delivers a purpose-built zero-trust cloud native security and analytics platform for fully controlled and managed access anywhere, solving one of the most vexing challenges for security teams.Prior to co-founding Axis Security, Dor was a senior security researcher at Fireglass, a leader in web isolation and later by acquisition, at Symantec. Dor is a five year veteran of the elite Unit 8200 of the Israeli Army Intelligence Corps as a senior software engineer for advanced cyber security, and earned a Bachelor of Science degree in Computer Science from IDC Herzliya, graduating cum laude.

For A Fully Rounded Defence, Automate

By Karen Levy, Vice President, Product and Client Marketing, Recorded Future

Cyber criminals are now running their operations in a way not dissimilar to modern legitimate businesses. Criminal groups have organisational structures, with various threat actors taking defined roles and using common business tools, such as lead generation apps, like Lead411 and UpLead. But to streamline operations and achieve higher pay-outs, automation has become a game changing tactic. Automation can be used in any part of the cyber kill chain, from reconnaissance, to infiltration, privilege escalation or data exfiltration. In response, legitimate organisations need to move beyond manual techniques to combat these new methods, otherwise they will find themselves outgunned, outmanoeuvred and out of luck.

Businesses need to fight fire with fire and use automation across their security operations. Security Orchestration, Automation and Response (SOAR), which integrates security orchestration and automation with security incident response platforms (SIRP) and threat intelligence platforms (TIP) is just one part of the puzzle. For a fully rounded defence, businesses must also automate other elements of their security operations such as decision making, intelligence, blocking, and alerting.

Managing External and Internal Threats

The relationship between an IT security team and those threat actors focused on infiltrating their network is like a game of chess, each trying to out manoeuvre the other. However, threat actors have the advantage of setting the timeline of attacks and conducting research and recon to figure out how best to achieve their objective. This research can involve using the lessons learned from past attacks, as well as talking to other actors to discover their secrets and tools used.

From this information threat actors develop their game plan for what they want to target and the most effective attack vector. For example, if they hear a rumour that an organisation doesn't do much in the way of cybersecurity training, a phishing campaign might be most effective. Or they may find that a firm's remote desktop protocol is unsecure and use that as a method of infiltration.

Intelligence about the external threats it faces is invaluable to an organisation. If a company knows it is being targeted and has an idea of the threat actor's intended tactics, techniques and procedures (TTP), then effective defensive measures can be put in place.

However, trying to gather, analyse and then act upon intelligence manually is resource heavy and ineffective. For instance, an organisation might decide to integrate a threat data feed into its security information and event management (SIEM) solution. Such a feed could include a stream of data on suspicious domains, lists of known malware hashes, IP addresses associated with malicious activity or code shared on pastebins. Anything that is flagged as a concern with the internal telemetry of an organisation's security infrastructure will be sent to the IT security team as an alert, without any context.

This is further complicated by security teams receiving alerts from actions carried out within the organisation too. The issue is that alerts can be triggered by almost any activity that an organisation's monitoring system might find suspicious, particularly if the alert parameters are not well defined.
Each of these alerts have to be triaged, which takes up huge amounts of time, diverting IT security professionals away from other tasks, as well as making it near impossible to determine which threats to act upon first.

The total number of alerts generated by internal and external threats can often overwhelm security teams, resulting in alert fatigue. This can be a serious issue for the integrity of an organisation as it can lead to security professionals simply ignoring alerts. Research from Cisco found that 44 percent of the alerts security teams receive each day are not even looked at, which could equate to many genuine threats to the network going unnoticed. Of the remaining 56 percent of alerts that are looked at, only 28 percent are deemed legitimate threats, meaning that there will be a significant number of false positives.

Automation can help address this issue by collecting unstructured data from disparate open, closed and technical sources, then connecting the dots by providing context on indicators of compromise (IoCs) and the TTPs of threat actors. This creates actionable security intelligence that is timely, provides context, and is easily understood by security decision makers.

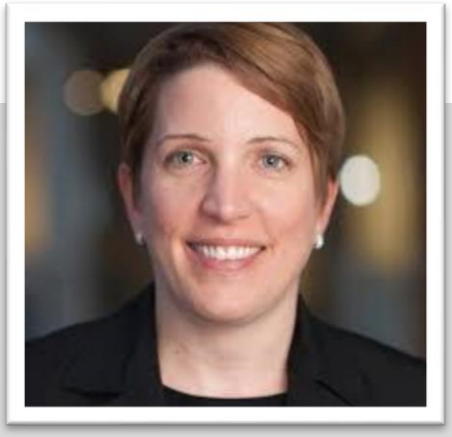
Furthermore, automated security intelligence tools provide security teams with access to contextualised internal alerts that not only help them to prioritise those that need human intervention, but also reduce the number of false positives. This enables the security team to focus on what really matters as well as keep an organisation safe.

Improving Workflows and Responses

An internal cybersecurity ecosystem is complex, with many different workflows to monitor, such as SIEM, SOAR, and firewalls. Moving from one to another to correlate different information sources to discover the reason behind certain suspicious activity is time consuming and stressful. This stress is due to the time pressure of having to try to quickly and accurately resolve an issue. For example, is a spike in an organisation's bandwidth due to someone sharing a very large file or the start of a DDoS attack? The last thing a security operative wants to do is either prevent the CEO from sharing the latest annual report video with a prospective client or let an attack unfold due to their inaction. Therefore, it comes by no surprise that research by the Ponemon Institute found that around 65 percent of IT security staff considered quitting their roles due to various stresses. The stress surrounding IT jobs are also likely to impact decision-making abilities, meaning they could potentially miss a significant threat. Further, the cyber-skills shortage means that no organisation can afford to lose a seasoned IT security professional.

Using automation to feed the information from all these intelligence sources into existing tools limits the need to change and disrupt workflows and streamlines efforts. This makes life much easier for security professionals to have the rich context they need for making timely decisions, while also helping to reduce the stress they are under.

Eventually, as automation becomes more popular in the cyber criminal underworld, businesses wanting to effectively repel infiltrators will have to likewise deploy automated security solutions. Failure to do so will leave them exposed to sophisticated threat actors who are ready and able to use such technology for their own illicit gains.



About the Author

Karen Levy is Vice President, Product and Client Marketing at Recorded Future. Karen Levy is the Vice President of Product and Client Marketing at Recorded Future with responsibility for go-to-market strategy, product positioning and client programs. Her more than fifteen years in marketing at cyber security technology companies includes leadership roles at RSA, CyberArk and Recorded Future. Karen holds a Bachelors in Chemistry from the University of Pennsylvania and an MBA from Boston University

Our company website is https://www.recordedfuture.com/

Secure Remote Active Directory Logins

By François Amigorena, CEO and founder, IS Decisions

Organizations across the world have seen their way of working changed from face to face to remote working. This big change is a golden opportunity for hackers. So many new remote connections mean so many access points that they can exploit.

Active Directory (AD) is used by organizations all around the world. In fact 95% of fortune 1000 companies use AD. Knowing that, the best way to achieve security for your remote users is to ensure the remote use of these AD credentials is secure.

Targeting the most vulnerable

New phishing email campaigns have surfaced with the coronavirus outbreak. Like the illness itself, the attacks are focused on the most vulnerable – your new remote employees. Attackers are using public fear to tempt their victims with links or downloads of safety instructions and infection maps. The likelihood that employees will click on a link or open an attachment is higher than ever.

Their objective is to be able to compromise corporate credentials so that they can access the network and start moving laterally to look for anything valuable to exploit. The problem is that, like with the coronavirus, you may not even know you have been infected. The average discovery time for a data breach is 191 days, according to the Ponemon Institute.

A threat surface bigger than ever

Generally speaking, insufficient security of Active Directory logins can be a high risk for your company. Now that most companies have recently moved to remote work, this threat surface is bigger than ever.

Most companies didn't have any time to prepare for remote working which increases the risk even more. They just rushed to allow Microsoft remote desktop (RDP) access so that their users would be able to access work resources without being physically at the office.

Understandable enough, most companies have prioritized the continuation of operations, leaving little attention for IT security.

Securing Active Directory logins

Remote desktop access is a great way to implement remote working but it's not fully secure. It is often only protected by a single password. To make sure those remote connections are better secured, here are three recommendations:

- Strengthen passwords
- Use a Virtual Private Network (VPN) for all remote sessions
- Enable two-factor authentication on these remote sessions

With this, you will significantly improve the security of your employees working remotely.

In order to fully minimize the risks, here is list of recommendations written by experts:

1. Clear device policy for remote users: Use the device available, secured and managed by your organization whenever it's possible. If it's not possible, give clear usage and security rules to your employees working from home equipment.
2. Make sure external access is secure: First, use a VPN (Virtual Private Network). Then, if possible, you should limit VPN access to only authorized machines to strengthen security. If a person tries to login from an "unauthorized" machine, login should be denied.
3. Strong password policy: All passwords must be complex, long enough and unique. To address the vulnerabilities of passwords, you need to enable two-factor authentication on your remote connections, especially for the ones to the corporate network.
4. Security updates policy: It needs to be strict. You have to deploy them on all devices as soon as they're available. External threat actors can quickly exploit such vulnerabilities.
5. Backup of data and activities: If you are victim of a cyber-attack, backups might be your only chance to recover your data. Perform and test them regularly to ensure they work.
6. Use professional antiviral solutions: They can keep your company safe from viral attacks, but also sometimes from phishing and ransomware.

7. Log activity: Logging of all access and activities of your workstations and devices will help you understand a cyber-attack and how to remedy it.
8. Monitor the activity of external access: Monitoring your remote connections and shared file and folder access will help you detect an unusual behavior which could be a sign of an attack. If you can have real-time alerts and immediate response in place, you can act before damage is done.
9. Users' awareness: It is important to give clear rules to your remote users on what they can or can't do. They often constitute the first barrier in avoiding/detecting attacks.
10. Get ready to suffer a cyber-attack: Whatever your size, you're not fully protected against cyber-attacks, no business is. By evaluating the possible cyber-attack scenarios, you can estimate the measures to take to secure your company.
11. The Manager's responsibility: Managers' involvement and responsibility must be exemplary when it comes to security policy to make employees adhere to it.

About the Author

François Amigorena is the founder and CEO of IS Decisions, and an expert commentator on cybersecurity issues.

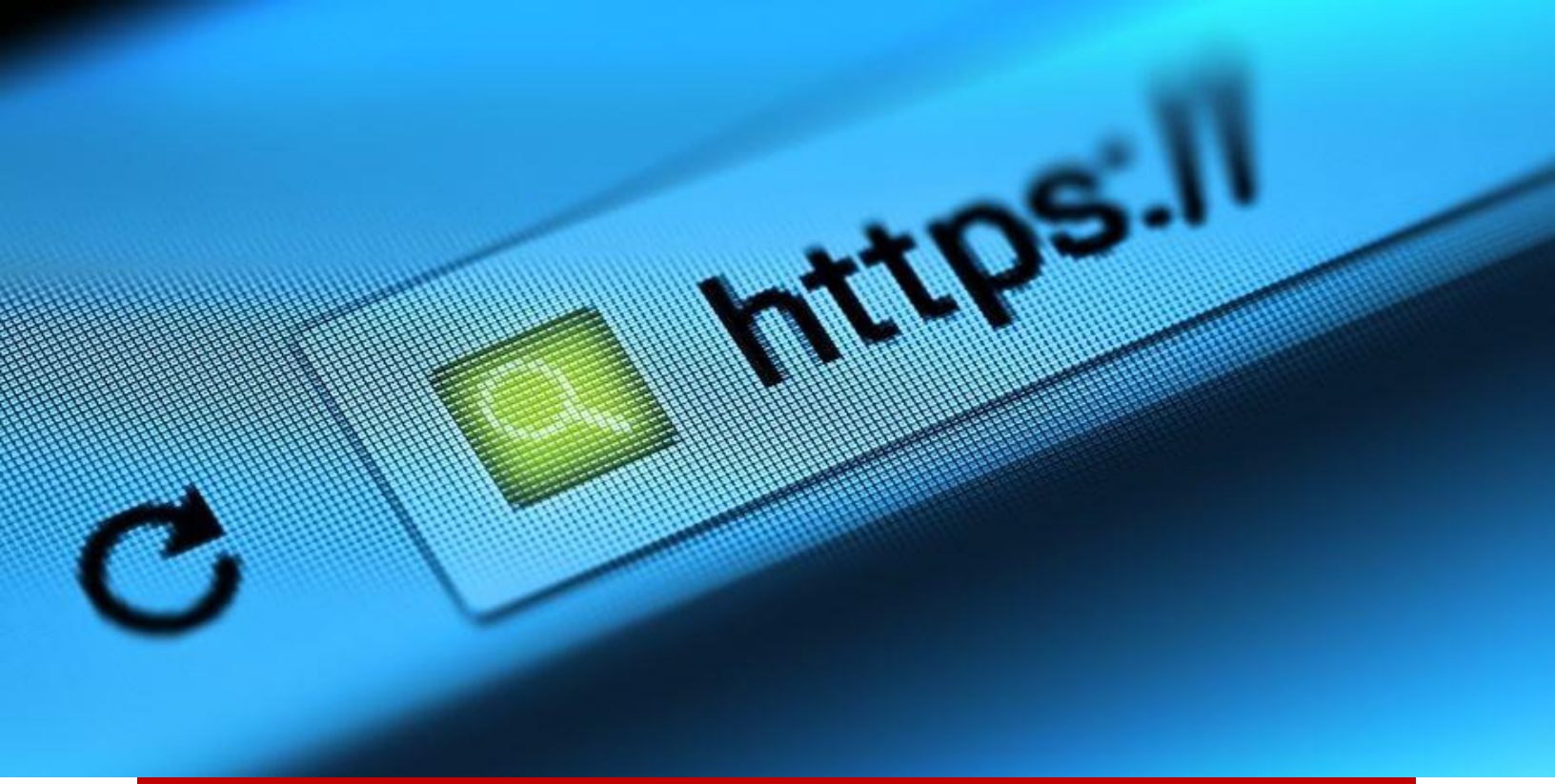
IS Decisions software makes it easy to protect against unauthorized access to networks and the sensitive files within.

Its customers include the FBI, the US Air Force, the United Nations and Barclays — each of which rely on IS Decisions to prevent security breaches; ensure compliance with major regulations; such as SOX and FISMA; quickly respond to IT emergencies; and save time and money for the IT department.

Twitter: https://twitter.com/IS_Decisions

Linkedin: https://www.linkedin.com/company/is-decisions/

Facebook: https://www.facebook.com/ISDecisions/



Not All Secure Certificates Created Equal

By Cal Evans, Developer and SiteGround Ambassador

Data security is essential for every person who uses the Internet, but if you have your own site, the stakes are even higher. If your site isn't encrypted, not only will your SEO suffer, but you put yourself and your site visitors at risk.

There are two types of secure certificates, free ones that you create yourself, and then have them signed by a trusted authority, or the ones you purchase or get directly from an SSL store or your web hosting provider. No matter the size of your audience or the type of site you run, you'll want to ensure that your data is encrypted. Mostly, anything you wouldn't tell a stranger should be protected this way.

Having that padlock symbol next to your domain not only builds trust with your visitors but protects their personal data from attack. The key to deciding how to procure that certificate is to determine what benefits you need most from having one.

So how do you know if you need to purchase a secure certificate or use a self-signed one? Each offers its own unique benefits – security, support and validation.

Paid secure certificates primarily offer two things, validation and support. Validation that Google will not diminish your SEO and that customers will know that your site is trustworthy. Support from your certificate provider throughout the process of obtaining and maintaining the certificate. The more support and validation you are looking for, the higher the cost of the certificate will be. Buying an SSL certificate guarantees that the certificate will work with 99 percent of browsers, ensures the site is HIPAA and PCI compliant, offers a lifetime of reissues and provides 24/7 support. These considerations are key for sites that handle large medical and financial information.

Using a self-signed certificate, on the other hand, can be a daunting task for less tech-savvy individuals. Mostly developers working in special cases use self-signed certificates. Also, the authority that they are signed by is VERY important. It has to be signed by an entity that has their root certificate ALREADY embedded in a browser. This is how the browsers recognize a certificate as valid. Unless self-signed certs are signed by a trusted authority, they will ALWAYS throw a warning to the user asking them if they want to continue. That's why self-signed certificates are not recommended for the general public, even low-traffic/low-risk sites.

LetsEncrypt certificates are the middle ground that solve the dilemma of a paid vs. self-signed certificate easily and freely for everyone. SiteGround - and many other reputable web hosts - now gives users the option to install a LetsEncrypt cert directly from the admin portal with a single click.

It's worth noting; the ability to create a certificate and have it signed by a trusted authority is key in ushering in the era of ecommerce. The opportunity to sell products to visitors easily and securely encouraged more business owners to jump into the industry.

Whether you're a master coder or a novice blogger, the right secure certificate is out there for you. When you prioritize the data security of your site and your audience, you will provide not only a better customer experience but a safer Internet for all.

For more detailed information about the types of SSL certificates, you can check out the Geek2English podcast episode on SSLs.

About the Author

Cal Evans, Developer and SiteGround Ambassador.For the past 15 years Cal has worked with PHP and MySQL on Linux, OSX, and Windows. He has built a variety of projects ranging in size from simple web pages to multi-million-dollar web applications. He enjoys building and managing development teams using his widely imitated but never patented management style of "management by wandering around". He is currently a member of the SiteGround Ambassadors program and in addition to building and managing dev teams enjoys speaking at conferences on various topics. Cal can be reached at www.linkedin.com/company/siteground-web-hosting-company/.

Social Engineering in Getting Competitive Advantage

By Milica D. Djekic

Our world is full of wonders. You would never be aware of how beautiful and adorable something can be unless you do a deep dive to discover its most fascinating secrets. The environment at any time includes many predators and prey that fight hard to survive in nature. It's similar with the never ending game between the security professionals and cyber criminals that also fight for their territory in cyberspace. Nature will always apply its rules, and any animal that wants to obtain the food for itself and its family must adapt to the surrounding conditions.

Never forget the story about the mice and cats. The cats need to eat the mice in order to get fed, but the mice would never be safe being syurrounded by so many cats. Also, the mice could be the good food for snakes that have fast reflexes like cats, and also such a good appetite for mice. In any case the mice are the prey either for cats or snakes and even if they multiply themselves following the geometrical progression, they would not live long in a place full of their predators. Apparently, in the environment being populated with the mice, cats and snakes there would not be enough food for both predators. They would need to compete very hard just to assure their survival.

In other words, just try to imagine what would happen if the number of mice in some spot would drop and there would still be a lot of cats and snakes that would need to survive in that territory. The analogous case is with the marketplace players. They would try to exploit some marketplace as long as there are the resources and reserves, so once they get no clients somewhere – they would simply change the strategy. Well, if there are fewer mice and more snakes – the cats would need to leave such a place and attempt to find the better opportunity somewhere else. The new environment would mean the new rules and does not matter how the process of the adaptation could get challenging – the cats would need to deal with this situation in order to remain alive. In our tale, the cats are the hunters that would take advantage of the mice that would also learn how to survive in the world by being aware of the predators. They would use so many camouflage tactics in order to protect their offspring as well as their own lives and if necessary they can also try to change their location in order to stay safe. So, in our story both predators and prey would have to make accommodations to survive. It would appear that in the nature everything is about getting the resources so critical for the life. The mice would eat the seed, while the cats and snakes would hunt the mice. Basically, that's how the nature works.

On the other hand, what can we learn about human beings and their societies? Modern economies deal with the marketplace and there are so many competitive suppliers for the purchasers or, in other words, for the sales. If there are not enough clients one of the competitors would need to withdraw from the competition or if the clients lack purchasing power – they would not be in a position to pay for the good or service being offered by competitive suppliers, so they would rather choose to purchase the offerings from someone else. In other words, if there is no enough seed for the mice – they would need to eat something else in order to get fed. Only if they show the flexibility and capacity to adapt they would survive in any time and any place. That's how evolution goes and that's how their genetic code would get improved making them being capable to live under any conditions. Apart from that the predators would stay in the race for the food as well and if the mice get that smart to avoid to become the catch – the cats and snakes would either change the territory or some of their habits simply making a decision to lower their requirements and eat what they can catch in such an occasion.

So, if you cannot sell your good for a competitive price, either you would move to a new marketplace accepting the risk from the new surrounding and its rules, or you would simply lower your price to sell what you have for a smaller amount of income. If that new situation would not give you a chance to survive – you would need to adapt your strategies to new circumstances and try to think how to take offer something new for that demand.

In other words, the communities of predators would not collapse if they decide to exploit the different reserves of the food and the prey would also stay safe and sound if they learn to change some of their habits. Talking in the language of the modern people, the marketplace players would not need to shut down their businesses if they, for instance, decide to give their products some other market alternative such as barter. If you cannot sell your beef for the money in the Middle East take the barrels of petrol instead the funds and you would definitely re-sell such a good product somewhere else. Maybe your business partners would not accept the alternate goods, but they would get something of value – so, that's how you would survive as long as your area has the resources that can get used.

The Game of Thrones

Social engineering is still one of the biggest cyber defense challenges of today, because modern hackers exploit various techniques and tactics in order to obtain IT privileges and permissions through the art of deception as well as confusion. The common social engineering scheme could include the social engineer being supported by cyber tracker that would analyze open-source intelligence as well as traced data carefully choosing a moment to attack his victim for some kind of competitive advantage and benefits. So, what would the common schemes look like? The social engineer is someone counting on communications skills and the cyber tracker is the guy who would do the surveillance of someone's email, social media and information exchange accounts trying to figure out what's going on with someone being from the specific interest for that duo.

Also, it's possible that the hacker would utilize some kind of phone calls and text messages monitoring solutions and he would then provide those information to the social engineer whose role is to engage the third party into a conversation based on the stolenm data. This information would be the basis to sell some credible, but disturbing story to your victim – then you would undoubtedly win the game. Your target would get confused and lose concentration after such a psychological operation and you would accomplish what you wanted – to gain access to the victim's resources.

People are Nice and Helpful, Right?

So many people are very kind and supportive and it may appear they simply cannot say no. Well, that's the gravest vulnerability of all of us and the social engineer would get familiar with that, so he would usually try to put the victim into a disadvantageeous position. Even if such a team makes the phone calls, send text messages or use skillfully composed emails – their goal is the same – they want to break your concentration and drag your attention to something else while they extract more information from the victim. Sounds silly, but it works in the practice!

The Usual Schemes

The social engineer is someone who uses great eloquence in both verbal and written context, so that person can use such a skill to distract, misinform or outplay you in such a communication in order to conduct some sort of espionage and collect some type of competitive intelligence. If some business is still so new in the marketplace – the competitors would get awareness about its presence. As it grows and raises the competitors would get curious who are the principals of this new busines. At the beginning they may offer some kind of support trying to convince you that you should trust them and let them get close to you. The final goal of every competitor is to destroy his competition and that's why anyone dealing with some activities should be careful about responding to inquiries.

We All Are the Citizens of the Planet

As long as there are competitive players in the marketplace there will be corporate espionage. The strong competitors use all possible means to obtain sensitive information and even steal some of the ideas from their competitors. Many people love to play monopoly as a business game; if you want to survive such a merciless game you need to fully open your eyes and camouflage your trade secrets and proprietary business information. Well established competitors have experience on their side, so if you are still new in your area of business – just be careful.

Some Deception Techniques

Social engineering commonly uses some kind of psychological campaign relying on deception techniques and tactics. Those kinds of strategies aim to make the target being mistaken about something and they take advantage of uncertainty, so our advice here is to be patient and avoid giving your competitors the chance to see everything about your business. The best way to destroy your competition is to make it work for you, and many experienced organizations and individuals know that, and they engage in such a practice.

Conclusions

If you say to anyone that you are his new best business friend, and that person is inexperienced, he could drop his guard. On the other hand, anyone clever would harbor suspicions about such a claim and not take those words literally. In other words, do not be naive and believe that your competitors would just help you for nothing. They would work hard and sometimes play dirty in order to get someone under their

control. There are no free favors and you cannot get something for nothing, so never offer your trust blindly.

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. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU) and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

Best Practices for Better SOC Analysis

By Chris Calvert, co-founder, Respond Software

Security analysts are a breed apart. They work long hours, using their intelligence and attention to detail to sort false alarms from real threats. However quick their reaction time, though, and however experienced they may be, they cannot possibly monitor every security alert, or even a tiny subset of them. The consequences are missed incidents and long attacker dwell times.

This obviously lowers an organization's security posture. It takes most organizations 197 days to identify that their IT environment has been compromised, according to the findings of the Ponemon Institute in its 2018 "Cost of a Data Breach" study. The total cost of containing, investigating and repairing the breach averages $3.86 million, or $148 per lost or stolen record.

Typically, the amount of time that a breach goes undetected determines the cost of the breach. Incidents that are fully resolved within 30 days cost an average of $1 million less to remediate than those taking more time. Unfortunately, the trend is moving in the wrong direction, as it's taking companies longer to identify and contain the data breaches they're being confronted with than it did last year.

Lack of Visibility

Here is an all-too-common occurrence: Security Operations Center (SOC) analysts receive multiple alerts about the activity in their environment, only to have failed to register these alerts' true significance –

resulting in a breach. Very likely, the analyst(s) never even saw the alerts, since they didn't match any of their simple rules. Most network security monitoring programs collect plenty of sensor telemetry data, but only a fraction of that data is currently being analyzed or reviewed and even then, it's not being considered in depth.

A SOC analyst may console themselves with the notion that all this data that has been collected will be available for forensic analysis in case of a breach. However, the sad truth is that using endpoint or network monitoring this way does little or nothing to thwart attackers. From the perspective of prevention, detection or even deterrence, it's totally ineffective and surprisingly expensive. And as long as organizations continue in this current approach to this problem, they are not going to see better results.

Security Operations: Barriers and Best Practices

What keeps security analysts from being able to make instant decisions as data is streamed in real time? There are three primary barriers. They include insufficient memory – of the human kind. Most people can't recall details from two hours ago, let alone days, weeks or months earlier. There's also the issue of volume; there's just too much information and data to process. The third barrier concerns a lack of context or meaning. Analysts don't always understand what the data is telling them, and the log files often don't contain useful information.

To overcome these barriers, here are seven best practices organizations can use to

maximize their security operations:

1. Ask better questions.

Irrespective of how large an organization is or how much money and resources it has invested in security technologies, some attacks will always succeed. Information security leaders often produce metrics that demonstrate how hard they're trying to prevent breaches—which is not really relevant anymore. And chief information security officers (CISOs) often use threat metrics to justify their (traditionally underfunded) budgets. Instead, leaders need to ask more penetrating questions about the value they derive from their investments in security operations.

2. Make use of autonomous analysis.

If you're not using data to inform decision-making logic, it's not doing you any good. With today's security operations software, autonomous analysis is possible, and this can give you the opportunity to make a revolutionary change in how you use log and sensor data. What's important is how well you monitor, employ and analyze it to recognize malicious activity in your environment.

3. Become a data minimalist.

Just because you can collect lots of data doesn't mean you must or even should. Some SecOps teams collect more than a hundred data sources—monitoring everything from endpoint operating system events to router status logs. But more than 99.99% of this data is never put to any use. This dramatically increases your costs without appreciably improving your security posture. A better method is to collect only what you need and then actually use it, rather than being buried under it all.

4. Enable honesty and success.

Failing to disclose known vulnerabilities, concealing operational failures or creating a dishonest organizational culture only makes a hard job harder. Instead, make your SOC a place where employees can be honest about what they find without worrying about getting fired or ignored. And incorporating automation and security analysis software into places in your SOC where human failures commonly occur can greatly improve its overall operational efficiency and effectiveness.

5. Remember the real threat.

It's time to rethink the words you use for cyberattacks. For instance, it's not actually a "virus"—a rapidly multiplying microscopic organism—that's on your network. And it's not just "malware"—something inanimate—that's in your environment. There are human criminals taking deliberate action, via malicious code, with the intent to do you harm. Recognize the seriousness, gravity and human origin of the threat.

6. Adopt an active and anticipatory approach.

By and large, the workflows and procedures you are using to safeguard your business are simply not working. Much of the thinking—and benchmarking—that your fellow business leaders do centers around the concept of having reasonable protections in place. This is seen as a tool to justify the inevitable failure that results in a breach. Instead, you must reimagine what it means to defend yourself in a digital world. Successful defense requires you to take an active and anticipatory approach to the attacks you will experience.

7. Learn to anticipate the unknown.

What is your mega-breach response plan? Attackers will often exploit vulnerabilities that they know are considered low-priority risks. These are so numerous, and so often unexpected, that it's nearly impossible to anticipate all the attacks that can be launched against them. Tabletop exercises and red teaming can be tremendously valuable in this area, so your leadership is prepared for the unexpected.

Proactive Improvement

As long as there is data, there will be cybercriminals trying to get at it. In this never-ending battle, organizations can empower their SOC analysts with modern security analysis capabilities. This will help them overcome the barriers of too much information, not enough memory and lack of context. Implement the best practices detailed above to improve the lives of your SOC analysts so that they won't be overwhelmed by irrelevant data and can focus their intelligence and skill on the alerts that matters.

About the Author

Chris Calvert, vice president of product strategy and co-founder of Respond Software, has over 30 years of experience in defensive information security, 14 years in the defense and intelligence community, and 17 years in the commercial industry. He has worked on the Defense Department Joint Staff and held leadership positions in both large and small companies, including IBM and HPE. He's designed, built and managed global security operations centers and incident response teams for six of the global Fortune 50. As he often says, if you have complaints about today's security operations model, you can partially blame him. It's from his firsthand experience in learning the limitations of the man vs. data SecOps model that Chris leads product decision and strategy for Respond Software.

Your Passwords Have Already Been Hacked

Time to Remove the Ticking Time Bomb From Your IT Security Strategy

By Shahrokh Shahidzadeh, CEO, Acceptto

There was a time where dozens of stolen passwords or digital credentials would send paralyzing fear into the hearts of IT Security professionals as they, better than most, understand that it only takes just one to access sensitive data and extort millions.

Unfortunately, recent headlines announcing 500 million and now even 773 million credentials stolen signal a new level of "normal on the war against cyber criminals. It means that attacks are even more frequent than we realize. The two largest data breaches of the past decade alone resulted in over half a billion compromised user records, a statistic that should frighten any IT professional. And the problem is getting worse. Of the top 14 largest data breaches, only one - Heartland Payment Systems' 2008 data breach - happened before 2010.

Passwords: A Human Problem?

It's clear that an adherence to outdated models drives cybersecurity concerns. 81% of security breaches in 2017 were due to weak or stolen passwords. Due to the frequency of data breaches, we all must now operate under the assumption that it's not a matter of 'if', but 'when' we become aware of the fact that our credentials and personal information are compromised.

The continued prevalence of passwords ignores all we know about how behavior drives cybersecurity. According to a study of a 2018 data breach by web security expert Troy Hunt, 86% of involved users were relying upon already previously leaked passwords. Meaning not only are users creating weak passwords in the first place, they're continuing to rely on weak passwords which are already sitting in databases available to any hacker or cybercriminal willing to look or pay. Even when attempting to make unique passwords, users are forced into symbol and character restrictions that drive users towards more common, easier to remember passwords. Further, those popular password meters don't always pick up on obvious password character patterns (names, nouns etc.) that are obvious to hackers, resulting in users feeling a false sense of security and bad advice.

Passwords: Will They Ever Be Replaced?

When it comes to security incidents, the most relevant of them is credential hijacking which accounts for the majority of attacks. Because of this past focus on password complexity, organizations have increased the total cost of ownership (TCO) associated with password resets and Helpdesk calls. Unfortunately, none of this has been proven to improve overall security.

Industries are past due in acknowledging that the use of the password is taking away valuable resources from other strategic IT investments. This hyper focus on passwords alone has compounded the security risk on a year-over-year basis, it is now a reality that most organizations are going to be breached because of the lack of security work done on other fronts.

To decrease dependency on passwords and remove them altogether requires initiative from executive leadership and sponsorship and ultimately retiring the 60 year old architecture of user directories. There has been solutions offered over the years to address the challenge but oftentimes the associated TOC has made passwordless solutions - such as smart cards and tokens such as Yubikey and use of biometrics (e.g. fingerprints, voice, retina detection etc.) - which are either cost prohibitive for most organizations, vulnerable and often suffering from the same shortcomings of good old binary passwords.

However, the good news is that in the last few years the security industry has responded to this challenge with various low cost, easy-to-manage passwordless solutions such as those deploying passwordless continuous authentication — where a solution constantly tracks the activity of the user pre-auth and post-authorization, to determine how likely the current user is actually authorized. Not only do these types of solutions address the cost associated with passwords by removing them altogether, but they improve the overall security posture of any organization, pre, during and post authorization.

Defusing a Ticking Time Bomb with a Continuous Approach

Cybersecurity professionals, whether tackling mass password breaches or a targeted phishing campaign, are working against a ticking timebomb trying to outmaneuver and foolproof the constant variable of human behavior. It's time to adapt systems to human behavior, not the other way around. Digital behaviors - things like how and when you access applications, devices you use, where you are, what your data and application usage signature looks like, time you are doing specific things - can all be part of a collection of key attributes that can establish legitimacy of claimed identities and validity of authentication.

Investing in a passwordless continuous authentication technique is the way forward. This is a technique that not only makes sure you are who you say you are when you log in, but also tracks that accuracy through your full online session (pre-, during- and post-session):

> *For example, let's say you have an employee that uses two unique workstations, a laptop and a desktop, three locations with distinct IP addresses, certain set of applications, and then logging in at certain fixed hours that all can be derived as the user habits. If someone tried to take over their account from an unknown device, at an unknown location and wrong time with a different digital hygiene than the known normal, a solution using continuous behavioral authentication would alert your system to a possible breach.*

> *At that point, whoever was attempting to use that person's account could be locked out, preventing them from getting into your company's files. You could then look into the situation to determine if a breach occurred or there was a more benign explanation.*

Getting rid of passwords and securing the access at the authentication state and continuously post-authorization is the key step forward to protecting against data breaches and is a paradigm shift that is available now.

About the Author

Shahrokh Shahidzadeh is the CEO of the Acceptto. He is a seasoned technologist and leader with 27 years of contribution to modern computer architecture, device identity, platform trust elevation, large IoT initiatives and ambient intelligence research with more than 20 issued and pending patents. Prior to Acceptto, Shahrokh was a senior principal technologist contributing to Intel Corporation for 25 years in a variety of leadership positions where he architected and led multiple billion dollar product initiatives. Shahrokh can be reached online at https://www.linkedin.com/in/shahrokh-shahidzadeh-1187062/ or on twitter @AcceptoCorp and at our company website http://www.acceptto.com/

The Journey to Universal Privilege Management

By Karl Lankford, Director – Solutions Engineering, BeyondTrust

Almost without exception, today's threat actors leverage readily available automated tools — automation increases the speed and probability that the attacker can find and exploit that initial weak link that gives them a "hook" into an environment.

The good news is that organizations increasingly recognize that to maintain a level playing field, they need automation and purpose-built solutions to protect privileges, and PAM has become a cornerstone of an effective, modern cybersecurity defense. The bad news is that many organizations mistakenly presume that privileged password management alone will solve the problem, when it's only one part of a necessary, comprehensive PAM solution.

Universal Privilege Management (UPM)

The Universal Privilege Management model allows enterprises to start with the PAM use cases that are most urgent to the organization, and then seamlessly address remaining use cases over time. Each use case, once addressed, will give enhanced control and accountability over the accounts, assets, users, systems, and activities that comprise the privilege environment, while eliminating and mitigating multiple

threat vectors. The more use cases that are addressed, the more PAM synergies emerge, and the more impact organizations will realize in reducing enterprise risk and improving operations.

So here are the 10 use cases on your journey to UPM.

Accountability

While not mandated, many organizations find discovering and securing privileged accounts the logical starting point for improving privilege security controls. But this demands a privileged credential management solution that automatically discovers and onboards the ever-expanding list of privileged accounts/credential types and brings those under management within a centralized password safe. This includes both human (employee, vendor) and non-human (functional, service, application, software robot, etc.) accounts in the environment.

The solution should allow control over which accounts are being shared, by whom, when, where, and why. It should provide mechanisms to find hardcoded credentials and deliver options to replace them with managed credentials. Critically, the solution should monitor, manage, and audit every privileged session regardless of where it originates.

Least privilege on desktops

Another important step to achieving Universal Privilege Management is implementing least privilege on end-user machines. Least privilege is defined as, “the minimum privileges/rights/access necessary for the user or process to be fully productive.”

With a least-privilege approach, users receive permissions only to the systems, applications, and data they need for their current roles. Rather than being enabled, persistent, and always-on, the privileges are only elevated on an as-needed basis and only for the targeted application or process. This is the basis for a just-in-time (JIT) PAM model.

Least privilege on servers

Having superuser status is important for administrators and some authorized users to do their jobs. Unfortunately, this practice also presents significant security risks from intentional, accidental, or indirect misuse of those privileged credentials.

Organizations must limit, control, and audit who has access to superuser accounts and privileges, without impairing productivity. Organizations must be able to efficiently and effectively delegate server privileges without disclosing the passwords for root, local, or domain administrator accounts. They should record all privileged sessions to help meet regulatory compliance. This is conceptually like the removal of administrative rights on desktops, but with the added requirements of supporting server-class operating systems in Tier-1 regulated environments.

Application reputation

Application control is essential to preventing advanced malware attacks, such as ransomware. Whitelisting, blacklisting, and greylisting offer application control strategies that enable organizations to restrict applications to only those approved to execute, with the correct privileges, within the appropriate context.

Another application reputation capability involves empowering organizations to make better informed privilege elevation decisions by understanding the vulnerability of an application or an asset with which it interacts. Applying real-time risk intelligence to privilege delegation and elevation not only stops exploits from becoming a privileged attack vector, but it also blocks drive-by social engineering threats that can leverage vulnerabilities within the environment. Similar to application control on Windows, command filtering on Unix and Linux is a critical security, compliance, and reliability control. For both application control and command filtering, a full audit trail of everything, attempted and allowed, is important.

Remote access

The vast majority of remotely launched attacks come from threat actors who are not specifically targeting the organization, but rather through remote contractors, vendors, and, even remote employees, who have themselves been compromised.

The ideal defense is to extend PAM best practices beyond the perimeter. This ensures only the right identity has access to the right resources in the right context. It eliminates “all or nothing” remote access for vendors by implementing least-privilege access to specific systems for a defined duration of time, potentially requiring a chaperone when appropriate.

Vendor credentials should be managed through the solution with policies, mandating rotation or single use passwords, and utilizing credential injection in sessions so that passwords are never exposed to end users.

Finally, session management and monitoring should be enforced to audit and control all vendor/remote access activity. This approach is far more secure than traditional protocol routing technologies like VPN.

Network devices and IoT

Many PAM tools lack the ability to extend granular privileged access controls to non-traditional endpoints, such as medical or industrial-connected devices and control systems.

Organizations need a solution that delivers the capability of least privilege to those endpoints by allowing fine-grained control over the commands sent and the responses received over SSH sessions. This offers the ability to control the operation of functions like tab completion, restricting access to only those aspects of the endpoint that are appropriate for the user. Administrators and vendors can be constrained within their area of responsibility without impacting their productivity.

Cloud and virtualization

With the accelerated use of virtualized data centers and cloud environments for processing, storage, application hosting and development, organizations have opened new avenues for threat actors to access sensitive data and cause disruption.

From a privileged access management perspective, the options to secure these assets are like traditional desktops and servers as described earlier. However, here are a few unique privileged security use cases for the cloud:

Utilize a password management solution to manage the passwords and keys that are unique to the cloud environment, like the hypervisor, APIs, and management consoles.

Implement a PAM solution with session monitoring for all administrative or root access into cloud providers, regardless of whether they are SaaS, PaaS, or IaaS-based.

When performing RPA or variations on DevOps, utilize a password management or secrets store to protect application-to-application secrets used in the cloud

DevOps and DevSecOps

DevOps delivers condensed development and deployment cycles through automation, frequently leveraging the scale of the cloud. The downside is that DevOps processes can also "automate insecurity," creating massive risks as well as compliance and operational gaps.

The right solution can discover all privileged automation accounts (including for CI/CD tools, service accounts, RPA, etc.) and replace the credentials with trusted API calls. The automatic retrieval and injection of the proper tool credentials helps protect developers, operations teams, and applications from attacks when privilege accounts are used for automation.

Privileged account integration

Modern PAM solutions must communicate with the rest of the IT security environment. By unifying privileged access management and other IT and security management solutions, IT teams benefit from a single, contextual lens through which to view and address risk by activity, asset, user, identity, and privilege.

Identity Access Management (IAM) integration

Access to an organization's resources is ideally managed through an IAM solution, which offers capabilities such as single sign-on, user provisioning/deprovisioning, role-based user management, access control, and governance. But managing a heterogeneous environment that contains silos for Unix,

Linux and macOS, plus a Microsoft or cloud environment, leads to inconsistent administration for IT, unnecessary complexity for end users, and a vast sprawling of alias accounts.

The ideal solution is to centralize identity management and authentication and provide single sign on across Windows, Unix, Linux, and macOS environments by extending a directory store like Microsoft's Active Directory with single sign-on capabilities to non-Windows platforms.

By evolving PAM capabilities using this UPM model, organizations will not only reduce the threat surface, eliminate security gaps, improve response capabilities, and ease compliance, but will also deter many attackers, who are still largely opportunistic in seeking to exploit the easiest prey.

About the Author

Karl Lankford is the Director, Solutions Engineering, for BeyondTrust, where he has worked for 5 years. A highly capable security leader, Karl has acquired a wide range of security experience and knowledge over the last decade, working across multiple industries. Karl is a regular speaker at industry conferences, delivering disruptive technical and strategic thought-leadership insight to the international cybersecurity community.

Why Finance Should Bank on Automating Security

By Faiz Shuja, co-founder & CEO at SIRP

Challenger banks such as Monzo and Starling are shaking up the finance sector. Traditional bricks and mortar institutions are eyeing their success in offering customers quality services on a modest budget and wondering if they could do likewise. The big difference is that the fintech start-ups exclusively offer their services online rather than on the high street. To catch up, traditional banks are now investing huge sums to digitalise their services and operations. Figures from IDC suggest that such investment will grow 20.4 percent each year to 2022, making finance the fastest growing sector for digital transformation.

This transition to digital infrastructure, however, corresponds with an increase in the total attack surface, putting banks at greater risk from threat actors. As such, improved security measures are a vital part of any digital transformation strategy.

The modern-day bank jobs

Financial institutions are, not surprisingly, some of the most attractive targets for cybercriminals. Today's digital robbers have the same motives as their masked and armed forebears, to get in and out quickly with as big a pay out as possible. The cash and safety deposit boxes of yesteryear have been replaced by vast troves of valuable financial and personal data held in digital vaults. The IMF has acknowledged

that such quantities of sensitive information makes financial institutions “one of the most highly targeted economic sectors for data breaches”.

The nature of these threats means that not only are financial institutions at risk from cyber criminals, their customers are too. Further, an attack can come from anywhere, either from external actors or rogue insiders. This has been long recognised by regulators. Hence the banking industry has some of the strictest and most mature data security laws. These are now being applied to the digital realm. For example, regular audits are now being carried out on behalf of the European Central Bank to ensure financial institutions have robust firewall policies.

The value of time

One of the greatest menaces that banks face is from advance persistent threat (APT) groups, which can be made up of either well-organised gangs or actors working on behalf of nation states. APT groups are aggressive, often well-resourced and will stop at nothing to achieve their goals. To counter the cyber criminals, financial institutions need to be able to detect an attack is taking place at the earliest opportunity and have ready access to tools to stop it in its tracks.

However, all too often banks’ adherence to traditional manual processes hampers incident response times. For instance, it is estimated it can take a security analyst up to an hour to investigate and respond to a single threat alert. Meantime, a cyber criminal could achieve their objective.

This situation is further exacerbated by the fact that security analysts typically receive more alerts than they can handle, particularly if alert parameters are not clearly defined. In fact, security teams do not even look at nearly half of the alerts they receive according to research from Cisco, meaning that many genuine threats could be slipping through the net.

The smart money’s on automation

To help them cope with the growing speed, sophistication and volume of attacks, IT security teams at financial institutions need to automate as many of their processes as possible. Doing so will enable them to focus on those complex cases that need human intervention, while leaving the bulk of alerts and clear IT policy violations to be dealt with by Artificial Intelligence/ Machine Learning (AI/ML).

As an organisation becomes more sophisticated in its use of automation, more and more complex issues can be handled by the system. Security Orchestration, Automation and Response (SOAR) provides a risk-based approach based on an organisation’s unique structure and objectives. This can then be combined with the SIEM to create a single pane of glass through which tens of thousands of daily alerts can be monitored and prioritised.

Financial institutions’ race towards digital transformation is likely to become ever more business critical. As it does there will be a corresponding rapid increase in the volume of risks and associated alerts. Automation can help security analysts better handle the mountain of alerts they receive each day,

improving the odds that the culprits will get caught in the act before they have a chance to open the virtual cashbox.

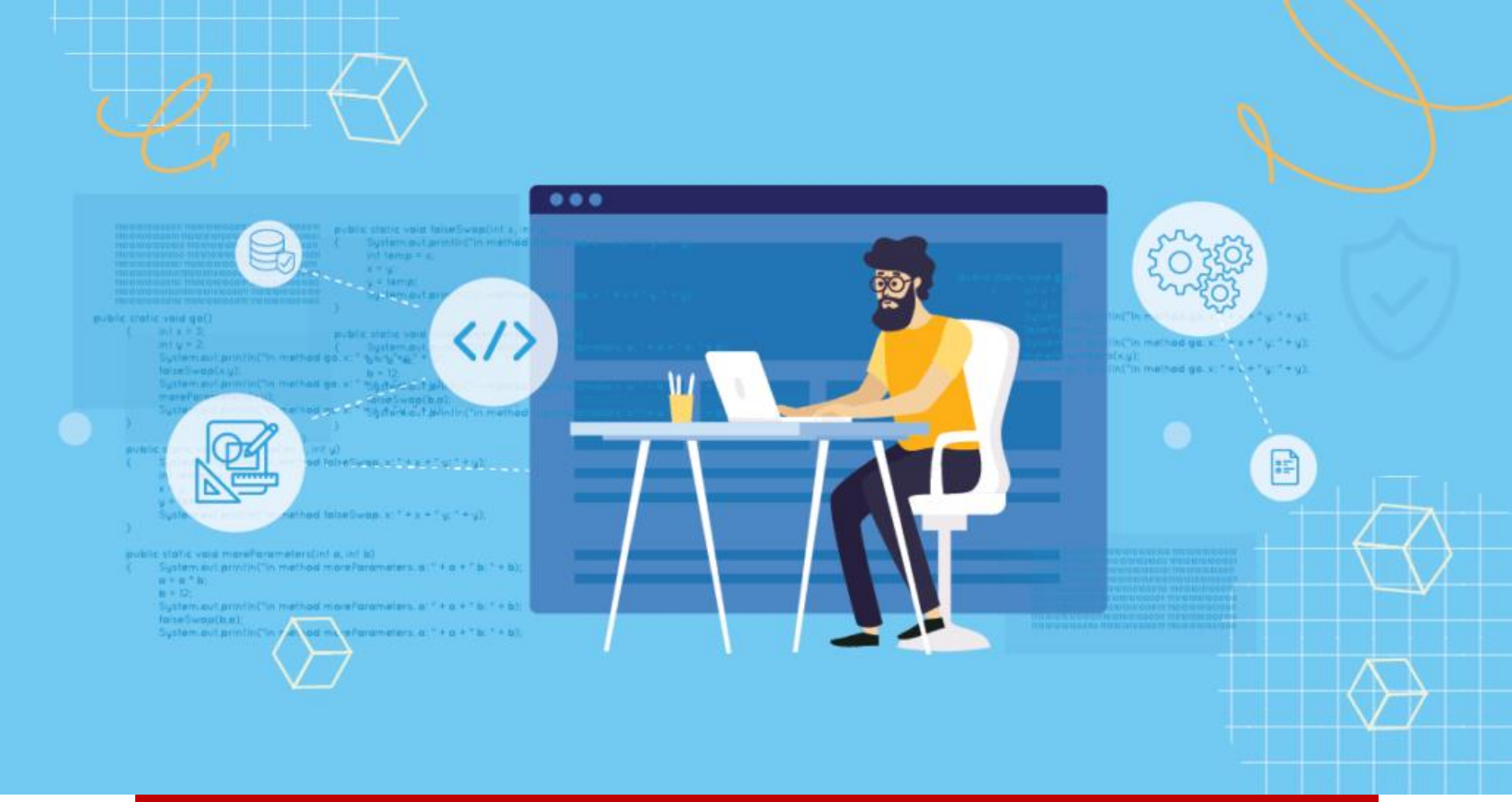
About the Author

Faiz Shuja, CEO, SIRP . Over sixteen years of experience in designing, implementing, and managing secure technology infrastructures. Has been involved in information security management, enterprise security operations, honeynets, penetration testing, incident handing, and forensics analysis.

Currently Co-founder & CEO for SIRP. SIRP is a Risk-based Security Orchestration, Automation and Response (SOAR) platform that fuses essential cybersecurity information to enable a unified cyber response. Through a single integrated platform, it drives security visibility, so decisions can be better prioritised and response time is dramatically reduced. With SIRP, the entire cybersecurity function works as a single, cohesive unit.

Also, CEO of The Global Honeynet Project, a non-profit, all-volunteer organization dedicated to Honeynet research. The Honeynet Project's goal is to learn and raise awareness about the motives and tactics of the Black Hat community. Its aim is to share and dissipate knowledge about the various tools and hacker practices in use on the Internet today.

https://www.linkedin.com/in/faizshuja/



Lifecycle Assurance for Platform Integrity and Security

By Tom Garrison, Vice President and General Manager of Client Security Strategy

Today's supply chains are global, complex and often lack transparency. This creates a variety of challenges, from design and responsible sourcing to deployment and secure retirement. Most platforms change custody, ownership and physical location several times over the course of assembly, transportation and provisioning. To help ensure the integrity at every stage of the compute lifecycle, there needs to be a security-first approach when designing, architecting and building these technologies. To help address this problem, Intel is working with an ecosystem of customers and partners on a new Compute Lifecycle Assurance Initiative designed to provide an end-to-end framework that includes tools and solutions for increased platform integrity, resilience and security.

To understand where this initiative is going, it is important to first look at what has been done historically. The call for assurance across the supply chain landscape has been evolving for decades. In fact, several examples have revolved around social responsibility and sustainability. For instance, The Responsible Business Alliance was formed in 2004 to help address key challenges around the rights and well-being of worldwide workers and communities. More recently, policymakers have begun to focus on supply chain risks in new ways. The 2018 SECURE Technology Act gave U.S. federal agencies new authority to consider supply chain risks when procuring products.

Technology companies have been doing their part as well. For example, over the past several years, Intel has taken several important steps toward supply chain transparency, including being one of the first to deliver Intel® Transparent Supply Chain (TSC) tools – a set of policies and procedures implemented at factories to provide visibility into the critical components that were used to manufacture the Intel-based PC or server.

Today, Intel TSC is available to customers across a variety of our platforms, including Intel® Core™ based PCs, Intel® NUC, Intel® Xeon® SP systems, and Intel® solid-state drives. In addition to our own platforms, we have enabled ecosystem partners with Intel TSC tools, including Hyve Solutions, Inspur, Lenovo (client and server), Mitac, Quanta, Supermicro, and ZT Systems.

While these have been great initial steps toward transparency and integrity, more can be done. This is the goal of Intel's Compute Lifecycle Assurance (CLA) Initiative. A fundamental principle of this initiative is health of device hardware and firmware across the system – not just on day one, but across all stages of the compute lifecycle. The initiative establishes an end-to-end framework that can be applied across the life of any platform to substantially improve platform integrity, resilience and security.

As a side note, the industry working group National Telecommunications and Information Administration (NTIA) has already created a Software Bill of Materials with an initial set of deliverables that address similar challenges in the software supply chain. Similar to the way Intel is approaching the compute platform lifecycle, their work is complementary and is driving meaningful change across the software ecosystem.

To address industry concerns, Intel is committed to investing in tools and processes that improve the integrity of computing products across every lifecycle stage, building on the Transparent Supply Chain tools we have today.

We see four key stages of the Compute Lifecycle Assurance Initiative: Build, Transfer, Operate and Retire, designed to provide better insight on the state of a platform at each stage:

- **Build** – This phase includes the architecture and design of the Intel components, with the goal of utilizing the latest in security research findings and world-class security techniques to minimize attack surfaces. We include the manufacturing of the platforms (PCs, servers, SSDs, etc.). We believe this build phase must start from the component level and extend all the way to platform manufacturing to provide a comprehensive picture of the platform's inception.
- **Transfer** – This phase extends from the manufacturing facility dock to when the device arrives at the customer site. In this phase it is important to detect tampering, modification or changes within the hardware, firmware and software since the device was manufactured. We will also put mechanisms in place designed to establish who should or should not have rights to modify the platform throughout distribution.
- **Operate** – The operate phase starts with provisioning of the device and extends over the remainder of the device's useful life. We aim to improve confidence that a system is operating in a known and trusted state at any point. One example of our goals is to provide visibility into the functional or security updates that have been applied to the platform and report whether the device is fully updated.
- **Retire** – This phase starts when a device is being decommissioned either permanently or for repurposing to a secondary customer/market. We will develop tools to help assure all data was confidentially wiped from the drive and the platform.

To see how Compute Lifecycle Assurance will ideally work in practice, let us look at a procurement example. When procurement places an order and receives the device on their dock, they have

comprehensive visibility into that device. Under the new framework this includes ensuring the device includes the required components that were ordered (such as processor type, SSD type, etc.) and does not include any blacklisted components from vendors that are high risk from a security or quality standpoint. Further, assurance will be provided that the device state has not changed unexpectedly from the time of manufacturing including key hardware components and firmware versions. Finally, there would be access to management tools capable of reporting on and assessing the fleet security posture with data read from each device.
Tackling assurance is critical for the industry, and collaboration is key to creating a successful CLA Initiative. Worldwide, policymakers have already begun to focus on supply chain risks in new ways.

Commercial enterprises around the world should find value in this improved level of assurance as well for validation, compliance and governance. In the next 12 to 18 months, our teams at Intel expect to see growing interest from customers, partners and government oversight organizations in transparency beyond just the manufacturing supply chain to include transportation, provisioning, attestation and in-field updates. Our journey with CLA is just beginning and we invite the broader ecosystem to join us as we build a more trusted foundation for all computing systems.

About the Author

Tom Garrison is a vice president of Client Computing Group and general manager of Security Strategies and Initiatives (SSI) at Intel Corporation. He leads the team overseeing Intel's efforts to enhance client security and to help customers and manufacturers deploy tooling and processes for greater security assurance and supply chain transparency. Garrison is responsible for coordination and execution of Intel's response to matters involving product function or security for client platforms. Garrison joined Intel in 1994. Prior to assuming his current role within SSI, he spent two years managing the Desktop, Commercial and Channel (DCC) team, which included Intel's desktop, business client, and workstation businesses, as well as the Intel® Unite collaboration solution and the client channel business for the company. Prior to his role in DCC, he spent three years as the general manager of the Business Client Platforms group. Earlier in his career, he spent 17 years in the Datacenter Group leading the Datacenter Engineering and Datacenter Strategic Planning organizations. Garrison holds a bachelor's degree in electrical engineering from Portland State University in Oregon.

How Pizza Can Be the Recipe to Understand Cloud Security

By Yohanan Berros, Customer Operation Managers, XM Cyber

It's not always easy to wrap your mind around the various layers of cloud security and how they differ from conventional on-premises computing. Fortunately, we've formulated a simple (and delicious) metaphor for your consumption: A pizza dinner.

First, think of conventional on-premises computing as the "at home" version of a pizza dinner. You manage the entire cooking environment: The pizza ingredients, the oven, the electricity or gas, the beverage and the dining table. Nothing is outsourced, everything is made and hosted at home. That's the "on-prem" version of a pizza dinner.

Now let's look at the Infrastructure-as-a-service (IaaS) version of the pizza dinner. In this case, you still manage the dining table, the beverage, the oven and the gas or electric, but a vendor takes care of the ingredients: The dough, sauce, toppings and cheese. This is the "take and bake" version of cloud security; part of it is managed onsite, and part of it involves a vendor.

Platform-as-a-Service (PaaS) offerings take the process of making a pizza dinner even further out of the kitchen and off your premises. It's the equivalent of pizza delivered right to your door. You take the pizza, place it on the dining table and grab a beverage, while the vendor takes care of everything else. It's a largely off-site, vendor-managed experience.

Finally, we have Software-as-a-Service (SaaS) offerings. Here, the vendor takes care of it all: Toppings, drinks, oven, table, electricity, etc. It's the cloud security equivalent of dining out — everything is handled off-prem.

To extend this metaphor a bit further, "dining out" has never been more popular in the enterprise realm. Cloud migration continues at an aggressive pace, as organizations seek to move forward with digital transformation initiatives.

According to a recent research report cited by *Forbes*, 83% of enterprise workloads will be either in a public, private or hybrid cloud by the end of 2020, while on-prem workloads decline sharply.

Yet while these projections (and the adoption that has already occurred) leave little doubt about the future primacy of cloud computing, organizational security leaders have one significant reservation: Security. That same research report showed that two-thirds of IT leaders cited security as their greatest concern when pursuing a cloud strategy.

If one reads the headlines, that concern seems well justified. It seems like new, high-profile cloud security breaches come with alarming consistency. Today's organizations are racing to migrate in order to stay competitive and relying on their security professionals to maintain robust security during this typically challenging period of migration.

Compounding this challenge, cloud environments are growing more complex, attackers are growing more sophisticated, and even one small misconfiguration or endpoint security lapse can endanger the assets that an organization holds most precious.

In other words, dining out for pizza has never been more popular, but you're going to navigate a few potholes on the way to the restaurant.

Fortunately, defenders have a powerful new tool that helps even the pavement (and the playing field): Breach and attack simulation (BAS) platforms.

How Breach and Attack Simulation Helps Mitigate the Risk of Cloud Cyber Attacks

Here's the truth about any security environment, cloud or otherwise: Over a long enough timeframe, attackers will be able to defeat it. Perfect security does not exist. To deal with this challenge, organizations deploy cloud penetration testing and other tools to determine whether their cloud environments security is up to the task.

Red team/blue team testing is another entrenched approach to maintaining security. These are exercises where ethical hackers (the red team) pose as attackers and attempt to breach an environment, while an opposing group (the blue team) works to defend the environment. By simulating these attack-and-defend scenarios, red and blue teams can work together to provide a clearer picture of organizational security.

This approach has drawbacks, however: It's manual, reliant on human skill and resource intensive. This means these exercises can only be run periodically. In the absence of continuous coverage, undetected vulnerabilities can arise and compromise cloud security.

Breach and attack simulations are designed to take the benefits of penetration testing and red teaming and enhance them by making them automated and continuous. A BAS platform can launch and run attack simulations continuously and identify the defensive measures/remediation steps needed to close any vulnerabilities. BAS platforms allow defenders to shed their reactive posture, assume the mindset of the attacker, and probe for vulnerabilities on a 24/7 basis, making them the gold standard for securing cloud environments and safely managing migration periods.

Simulate Attacks on Amazon Web Services (AWS)

Organizations need a fully automated BAS solution for hybrid cloud environments, as it can simulate attacks on Amazon Web Services, the dominant player in cloud computing.

A BAS simulation solution for AWS cyber security addresses one of the critical gaps in cloud security: assessing cloud and on-prem security in a vacuum. To fully protect critical assets, it's imperative to assess the risks cloud and on-prem pose to each other, and identify and recommend remediation for hybrid environment risks, closing this crucial gap.

AWS public API layer is the layer below the AWS entities which in most cases has broad authorization permissions, a sophisticated attacker can leverage them to exploit resources over the cloud.

The right platform must audit AWS configurations via API and use this data to calculate possible attack vectors. By simulating attacks on AWS infrastructure, misconfigurations and other problems — many of the same vulnerabilities that have unleashed a torrent of high-profile cloud security breaches in recent years — can be rooted out.

In Conclusion

In the language of our pizza metaphor, you need to be protected not only when you're dining out but also while you're traveling to the restaurant.

Creating a simple pizza dinner may be the key to understanding cloud security, but learning how to protect your "pizza" from thieves requires a few added ingredients: automation, continuous monitoring and AWS integration. Find a cloud security solution that offers this unique recipe.

About the Author

Yohanan Berros is a Customer Operation Manager, at XM Cyber. He has extensive knowledge of network security and customer security project experience, with 3 years of high-level customer management at Check Point, and lot of experience in the cyber field, security operations, vulnerability assessment and mobile security. To reach him and learn more, visit https://xmcyber.com/

Moving Beyond Honeypots to Next-Generation Deception Technology

By Wade Lance, field CTO, Illusive Networks

When security professionals hear the word “deception,” they tend to immediately think of honeypots. That association needs to be updated. The concept of honeypots goes back a long way; IT security researchers began using honeypots in the 1990s. Their goal was to trick an attacker into interacting with a fake system. Honeypots were designed to capture and analyze attacker behavior in a safe environment, not to detect threats. The deception technology landscape has evolved considerably since then.

Honeypots vs. deception technology

It turned out that honeypots aren’t very effective at detection – they tend to be limited in scope and easy for professional bad actors to identify. As detection methods have advanced, attackers responded by focusing their attention on remote hosts where their beachhead has had a historical interaction. So the value of honeypots plummeted as detection tools as attackers abandoned network scans in favor of using the history they found on the beachhead. Production users don’t interact with honeypots, so attackers don’t either. When an attacker does stumble over a honeypot they pretty quickly figure out they aren’t real systems.

Deception technology holds a lot of promise, especially for early and efficient threat detection. However, to fully realize that potential, deception needs to go well beyond the honeypot.

Honeypots are difficult to distribute widely, and require significant resources to maintain and implement, so security teams can usually only deploy a limited number. That means there are never enough to effectively detect threats. Any value a honeypot strategy has for detection is based on a fairly specious hope – that an attacker will accidentally trip over or be lured into it.

That hope has grown increasingly thin over the years as cybercriminals have gotten wise to the honeypot ruse. Experience, crowdsourcing, and widely-available tools now help attackers distinguish honeypots from real systems containing the valuable data they are targeting. To be an effective detection tool, deceptions must be inevitable, undetectable and inescapable. Even today's more advanced honeypots are none of these things.

As mentioned, honeypots in a decoy role were originally intended to allow the defender to observe attacks in progress. As such, they still serve an important purpose in threat research. They can be used effectively for forensic analysis, threat hunting, and developing responses to malicious behavior. Honeypots may still prove useful, but not as the centerpiece of a modern deception technology strategy focused on threat detection.

What does next-generation deception technology offer?

Next-generation deception technology gives defenders the earliest and most effective method for detecting and halting an attacker's movements once inside the network. At the same time, deception dramatically increases the effort and costs for the attacker.

Automation and machine learning support rapid deployment and touch-free refreshes to maintain deception authenticity. Intelligent deception systems can recommend and craft customized network, system, application, server and data deceptions that appear native to the environment.

Currently, honeypots gather data in isolation. Next-gen deception technology moves the focus of deception beyond the honeypot to the endpoint, server, and device. This approach gathers information across the production environment, provides previously unimagined visualization of the attack surface, and offers highly efficient detection of cyber threats at the attack beachhead.

Evaluating next-gen deception technology

When it comes to selecting a next-gen deception technology solution, here are some best practices to make the evaluation process easier:

Make sure it SMAQs: an effective next-generation deception solution must be Scalable, Authentic, Manageable, and Quiet. These traits would seem to speak for themselves, but we are often surprised to find deception products that are hard to deploy, easily recognized as fake, require extensive handholding, and still produce unacceptable levels of false positive alerts. Caveat Emptor.

Focus deception on the production system: Honeypots focus on diverting attackers away from the production system, but this is no longer enough. As mentioned above, next-generation deception

methods needs to focus on the production systems themselves. When evaluating a potential solution, it's important to make sure the focus is on the production environment and not just aimed at diversion. This is especially true in larger environments.

Getting value out of your deception platform beyond detection: When it comes down to making an investment in deception technology, it's important to choose a solution that offers you aspects beyond threat detection. A well architected deception-based solution will offer enhanced visibility, attack surface reduction, precision forensic data to speed response, as well as threat hunting and intelligence gathering.

Moving from a reactive/passive defense to an active defense: Cyber criminals will continue to evolve and become more sophisticated in their approaches. That's a fact. Organizations cannot afford to take a purely reactive or passive approach to defense. Being proactive will make a world of difference in protecting your organization from damaging breaches and attacks. The best approach provides so much false data to attackers on production hosts that they can't orient themselves or make effective decisions. Never underestimate the power of creating frustration for the attacker. They are people too, and quickly move out of environments where it is just too difficult to operate.

Integrations are also important: Next-generation deception technology should also integrate comfortably with other security solutions. That includes Security Incident and Event Management (SIEM,) Endpoint Detection and Response (EDR) and Security Orchestration, Automation and Response (SOAR) systems. Having these integrations helps ensure the threat detection capabilities can enhance the resolution capabilities of other technologies as well.

A new day in network security

Honeypots were a novel invention in their time – but that time has passed. They still have their usefulness but have been overshadowed by a better, smarter option for the purposes of quick threat detection: the new breed of distributed deception technology. Today's deception technology is scalable and automated, providing true early detection to shut down attacks quickly. IT professionals must vet potential solutions carefully to ensure the organization gets the active network defense it needs.

About the Author

Wade Lance, field CTO of Illusive Networks, has been productizing new technologies in education, healthcare and information security for over 20 years. He has diverse experience in solution design for global 1000 cybersecurity teams, an extensive background in advanced cyber-attack detection, and a specialty in cyber deception methods and platforms. Prior to his career in information technology, Lance was a professional mountain guide. As program director at Appalachian Mountaineering he developed a new method for technical rock and ice climbing instruction that is still used today to teach advanced skills for the most dangerous environments.


EVENTS

REUTERS EVENTS™ INSURANCENEXUS

INSURANCE AI AND INNOVATIVE TECH USA 2020

MAY 12-13 | RADISSON BLU AQUA | CHICAGO USA

Cyber Defense Magazine has secured a VIP upgrade, quote 5106CyberDefenseVIP when you register online at: https://events.insurancenexus.com/analyticsusa/register.php

Harness the Power of Tech

Maximize AI Integration and Data Efficiency to Empower Technology-Led Insurance

500+	60+	175	150	45+
ATTENDEES	SPEAKERS	DATA AND ANALYTICS EXPERTS	INNOVATION AND TECH EXECUTIVES	CASE STUDIES

Join the leading strategic insurance event in the US

Data and Analytics

Drive business value with data and analytics: Implement AI and advanced analytics to achieve core business objectives and customer satisfaction at scale

Turn your vision into reality: Develop a strategy for successful AI implementation to ensure a robust business intelligence infrastructure, data integrity and a 360 view of the customer

Boost the power of your insurance product: Discover how AI is changing existing products and services in order to improve customer service and increase efficiency

Innovative Tech

Become innovative at your core: Discover the true value of innovation to your core processes, accelerate underwriting, fast-track claims and product development

Maximize innovation impact: Find the maximum value for each disruptive technology and transform your culture to be more innovative

Move beyond single technology implementation: Discover how to implement multiple technologies to infuse the whole value chain and stay ahead of your competition

Speaker Line-Up of Visionaries and Senior Leaders

Adam Kornick
Chief Data Technologist
Allstate

Jim Tyo
Chief Data Officer
Nationwide

David T. Vanalek
Claims Chief Operating Officer
Markel

Vineet Bansal
SVP, Chief Technology Officer
Swiss Re

Dong Li
Chief Data Officer, VP of Group Technology Center of Intelligence
Sunshine Insurance Group

Will Dubyak
VP, Analytics for Product Development and Innovation
USAA

Jeff Briglia
Chief Insurance Officer
Metromile

Richard McCathron
Chief Insurance Officer
Hippo

Insurance AI and Innovative Tech USA 2020 is bringing together over 500 senior innovation and business unit executives to uncover the rewards of embedding technologies such as AI, IoT, blockchain and automation into their working processes and operations.

Cyber Defense Magazine has secured a VIP upgrade, quote 5106CyberDefenseVIP when you register online at: https://events.insurancenexus.com/analyticsusa/register.php

IFSEC INTERNATIONAL

19-21 MAY 2020
EXCEL LONDON UK

SECURITY IS CRITICAL
IFSEC IS ESSENTIAL

Europe's leading integrated security event

Meet **450+** leading exhibitors

Network with **34,500+** security professionals

Attend **65+** seminars and workshops

Register for your free ticket at www.ifsec.co.uk/Defence

Co-located with

FIREX INTERNATIONAL | INTELLIGENT BUILDING EUROPE | FACILITIES SHOW | SAFETY & HEALTH EXPO | WORKPLACE WELLBEING SHOW

CTX COUNTER TERROR EXPO | WORLD COUNTER TERROR CONGRESS | AMBITION EPRR CONFERENCE & ZONE | FORENSICS EUROPE EXPO

By Informa Markets

IFSEC INTERNATIONAL

informa markets

The only security event you need to be a part of

IFSEC International returns to ExCeL London on 19-21 May 2020

IFSEC International, Europe's leading integrated security event, is critical to today's changing landscape. Running for the first time alongside *Counter Terror Expo* and *Smart Buildings Expo,* IFSEC is your unmatched opportunity to showcase your security technologies to a global network of installers, integrators, end-users, consultants, distributors and government officials.

"IFSEC has been transforming over the years. It is a must attend show for any stakeholder in physical and converged security."

CTI/CISO
Virtually Informed

"It was our first time exhibiting in the UK and Europe, as we wanted to expand our markets. There was a good quality of visitors and foot traffic – we would definitely exhibit again."

Business Development Manager, **Telaeris Inc**

"We came to broaden our security portfolio, we wanted to explore the markets and understand ROI. It has been a really successful show with excellent networking opportunities."

Business Manager
Siklu

For more reasons to exhibit and to book your stand visit: www.ifsec.events/international

Co-located with:

FIREX INTERNATIONAL
SAFETY & HEALTH EXPO
FACILITIES SHOW
SMART BUILDINGS EXPO

Plus:

CTX COUNTER TERROR EXPO 19-21 May 2020 ExCeL, London
FORENSICS EUROPE EXPO 19-21 May 2020 ExCeL, London
AMBITION THE EPRR EXPO 19-21 May 2020 ExCeL, London

intelligent insurer **Underwriting Innovation**

June 22-23, Hilton Magnificent Mile, Chicago

CLICK HERE TO GO TO THE EVENT WEBSITE

Accelerate Underwriting Profitability in a World of Changing Risks

Capitalize on Cutting-Edge Data Analytics, Automation, AI and IoT to Drive Efficiency, Make Better Decisions and Become the Underwriter of the Future

1. **Harness External Data and Advanced Analytics to Drive Efficiency and Make Better Decisions:** Deploy AI, robotics and automation to work smarter, deliver maximum value and boost profitability
2. **Identify Opportunities for Emerging Risks:** Cyber, cannabis, autonomous vehicles, climate change... Utilize data to price intelligently and deliver innovative products and services to new customer segments
3. **Become the Underwriter of the Future:** Achieve the right blend art and science, human and machine and upskill in statistics, analytics and AI to maintain relevancy and retain talent
4. **Accurately Assess Risk Through Emerging Technology and Catastrophe Models:** Evaluate IoT, aerial imagery and location data to provide tailored cover, more accurate prices and mitigate against risk
5. **Respond to the Evolving Distribution Landscape:** Build a strategy for engaging with brokers, aggregators, insurtech and MGAs to access profitable markets and reduce friction along the value-chain

30+ Speakers from the world's biggest insurance brands:

- David Perez, *Chief Underwriting Officer,* **Liberty Mutual**
- Dean LaPierre, *Chief Underwriting Officer - Global Property & Marine,* **Berkshire Hathaway Specialty**
- Jane Peterson, *Chief Underwriting Officer,* **Markel**
- Erik Nikodem, SVP, *Head of Property,* **Everest Insurance**
- Matt Junge, *SVP Head of Property Solutions, US & Canada,* **Swiss Re**
- Robert Curtis, *SVP,* **SCOR Alternative Solutions**
- Matteo Carbone, *Founder & Director,* **IoT Insurance Observatory**
- Jonathan Charak, *VP and Emerging Solutions Director,* **Zurich North America**
- Blake Konrardy, *VP of Product,* **Kin Insurance**

A two-day event dedicated 100% to underwriting

150+ Attendees | 30+ Speakers | 20+ Hours of Networking | 16+ In-depth Sessions

SAVE $600 - REGISTER BEFORE MARCH 6TH

CLICK HERE TO GO TO THE EVENT WEBSITE

1,100+ ATTENDEES

85+ SPONSORS

50+ CONFERENCE SESSIONS

90+ SPEAKERS

THE INDUSTRY'S LARGEST INDEPENDENT AI GOVERNMENT EVENT

2nd Annual

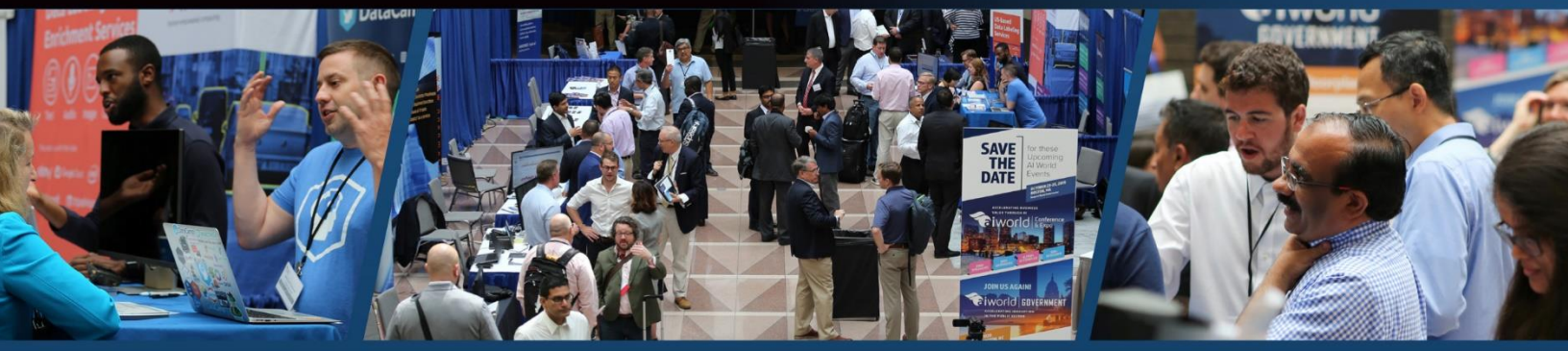
aiworld GOVERNMENT

JUNE 22-24, 2020 | WASHINGTON, DC

RENAISSANCE DOWNTOWN HOTEL

Save $200 with discount code CDM2020

Accelerating Innovation in the Public Sector



AI World Government provides a comprehensive three-day forum to educate and inform public sector agencies on proven strategies and tactics to successfully deploy AI and cognitive technologies.

AIWorldGov.com


ISAF CyberSecurity
9th International Cyber Security, Information & Network Security Exhibition
OCTOBER 08th-11th, 2020
Istanbul Expo Center (İFM) - Turkiye
ISAF
"smart exhibitions"
www.isaffuari.com
T. +90 212 503 32 32 - marmara@marmarafuar.com.tr
MARMARA
TANITIM FUARCILIK
www.marmarafuar.com.tr
/marmarafuar
/isafexhibition
/company/marmara-fuar


1,100+
ATTENDEES
85+
SPONSORS
50+
CONFERENCE
SESSIONS
90+
SPEAKERS
THE INDUSTRY'S LARGEST
INDEPENDENT AI
GOVERNMENT EVENT
2nd Annual
aiworld
GOVERNMENT
NEW DATES:
OCTOBER 28-30, 2020 | WASHINGTON, DC
RENAISSANCE DOWNTOWN HOTEL
Save $200
with discount
code CDM2020
Accelerating Innovation in the Public Sector
AI World Government provides a comprehensive three-day forum to educate and inform
public sector agencies on proven strategies and tactics to successfully deploy
AI and cognitive technologies.
AIWorldGov.com

QUBIT CONFERENCE SOFIA 2020

3rd Cybersecurity Community Event

29 OCTOBER/ SOFIA, BULGARIA

- Excellent speakers
- Educational session
- News & networking
- Practical workshops

REGISTER YOUR INTEREST AT

sofia.qubitconference

EURONAVAL

THE WORLD NAVAL DEFENCE EXHIBITION

OCTOBER 2020

EXHIBITION
20/23
LE BOURGET

CONFERENCE
19
PARIS

www.euronaval.fr

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

EGYPT DEFENCE EXPO

7-10 DECEMBER 2020
EGYPT INTERNATIONAL EXHIBITION CENTRE

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

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

EGYPT INTERNATIONAL EXHIBITION CENTRE
7-10 DECEMBER 2020

400 + EXHIBITORS

30,000 + VISITORS

FULLY-HOSTED VIP DELEGATION PROGRAMME

Media Partner

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Supported by

Ministry of Defence

Egyptian Armed Forces

Ministry of Military Production

جهاز مشروعات الخدمة الوطنية

Organised by

CLARION EVENTS

RSAConference | Where the world talks security

Ensuring the security of your organization is always challenging, even in the best of times.

We created an **online resource center** to help you find the answers you may be looking for. It includes relevant content such as interviews with CISOs dealing with today's realities, preventing ransomware attacks, tips on how to improve your virtual presenting skills, and much, much more.

Browse our specially curated resources today, and keep checking back as new information is added regularly.

rsaconference.com/cyberdefense-2020

You don't need to be next in line for a data breach.

Put on your thinking hat and step into the shoes of a hacker.

Cyber incidents are on the rise. While most organizations play defense--creating plans that tell them what to secure and how to react if their security settings fail--it's not enough to respond to a data breach.

What if you looked at cybersecurity from a different point of view?

In our guide, "How to Think Like a Hacker and Secure Your Data," you'll discover how to go on offense with your data by:

- Diving into modern data breach statistics
- Exploring hacking terminology and techniques
- Walking through seven strategies for data protection

Are you ready to put yourself in the shoes of a hacker?

Visit **https://www.goanywhere.com/think-like-a-hacker**

to get a free copy of our cybersecurity guide.

GO ANYWHERE®
Managed File Transfer

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

“Amazing Keynote”

“Best Speaker on the Hacking Stage”

“Most Entertaining and Engaging”

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

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

CYBER DEFENSE TV

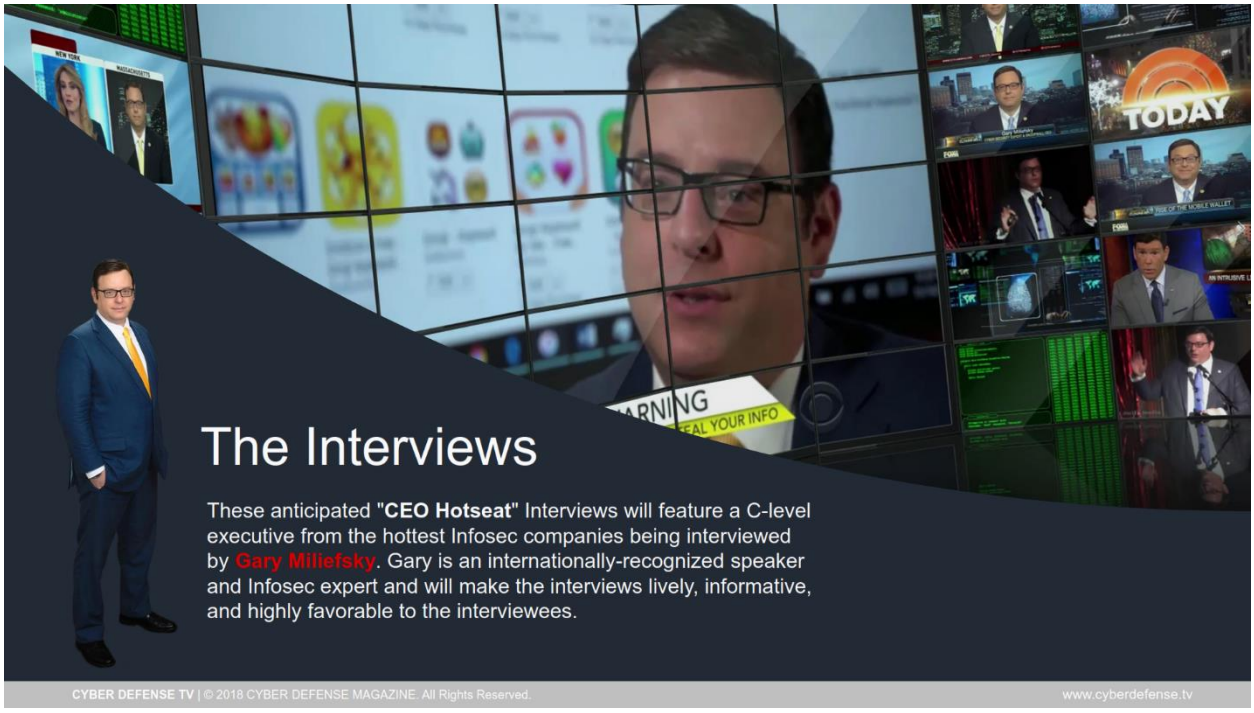
INFOSEC KNOWLEDGE IS POWER

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

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

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

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



Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine

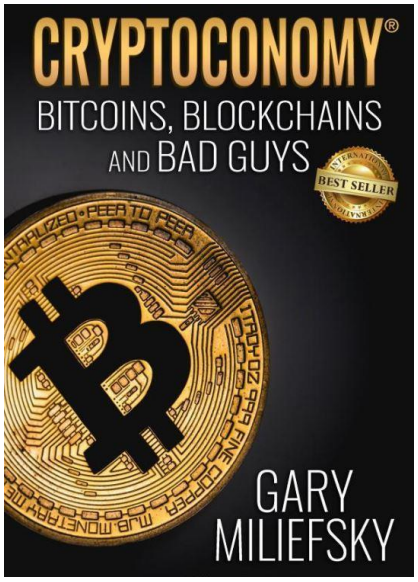
276 Fifth Avenue, Suite 704, New York, NY 1000
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)
Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 05/01/2020

TRILLIONS ARE AT STAKE

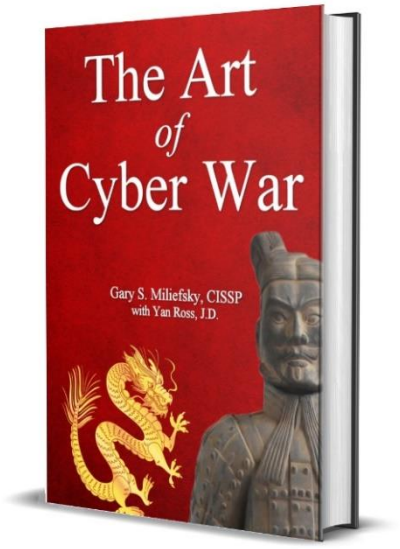
No 1 INTERNATIONAL BESTSELLER IN FOUR CATEGORIES

Released:



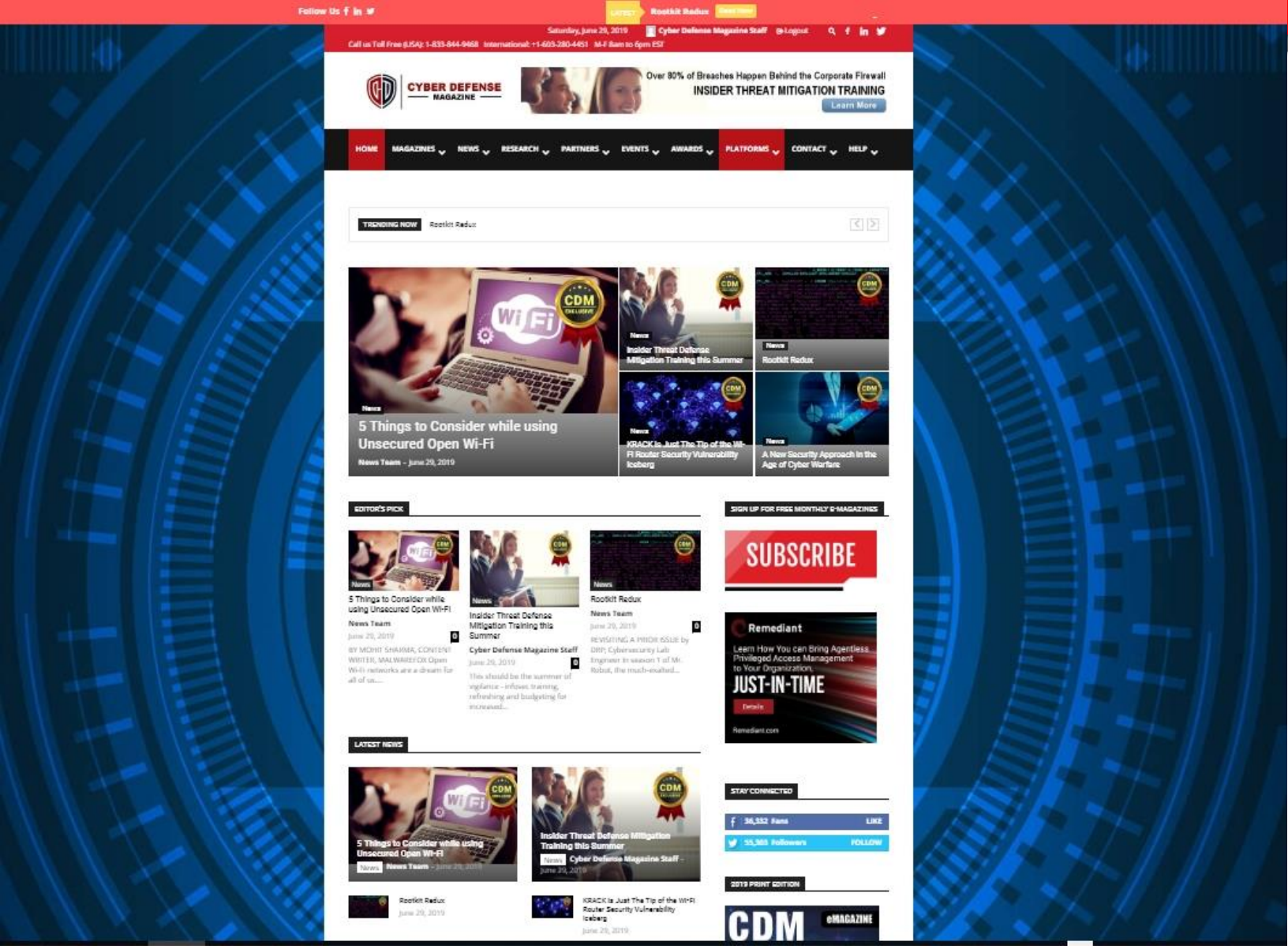
https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH

In Development:



To learn more:
Call +1.512.372.1004, Visit www.brinqa.com

brinqa



8 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're shooting for 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS.

Millions of monthly readers and new platforms:

www.cybersecuritymagazine.com *www.cyberdefensewebinars.com*

JUNE 2–4, 2020
David L. Lawrence Convention Center | Pittsburgh, PA

SMART MANUFACTURING EXPERIENCE

the path to the connected world of manufacturing

Greater Connectivity = Greater Need for Cybersecurity Solutions

- **Thousands of buyers.** Engage with qualified attendees searching for the best ways to secure their data and their business
- **Exclusive opportunity.** Only open to companies that can demonstrate a connection/application to smart manufacturing
- **Active participants.** Demonstrate your solutions and educate manufacturers on the most effective methods to safeguard their valuable data

The Event is Focused on These Transformative Technologies:

- Cybersecurity
- Additive Manufacturing (AM) & 3D Printing
- Artificial Intelligence/Machine Learning
- Augmented Reality (AR) and Virtual Reality (VR)
- Automation & Robotics
- Data Analytics
- Industrial IoT (Internet of Things)
- Workforce Transformation

Be Part of the Experience!

Call **800.733.3976** or visit **smartmanufacturingexperience.com**

sme AMT

HERJAVEC GROUP

Celebrating Over 15 Years of Cybersecurity Operations Excellence

At Herjavec Group, information security is what we do.

You may know me from making deals on television, but my passion lies in innovating technology - yes, cybersecurity.

Over 15 years ago we started the business selling commercial firewalls to IT buyers. Over time we've seen a monumental shift towards what we are all familiar with - the cybercrime epidemic. Now our customers are challenged to address compliance requirements, incident response plans, nation state threats, security awareness, malware detection…the list goes on. In response, we have advanced our cyber capabilities and attracted world class talent.

Today, Herjavec Group is a global leader in cybersecurity with expertise in comprehensive security services including **Managed Security Services** (SOC Operations, Threat Detection, Security Technology Engineering) & **Professional Services** (Advisory Services, Identity Services, Technology Implementation, Threat Management & Incident Response). Herjavec Group is over 300 people strong, with offices and Security Operations Centers across the United States, United Kingdom, Canada and India. At Herjavec Group, we realize that in cybersecurity change is constant, but we are driven by a steadfast goal: to make enterprises around the world more secure.

To your success,

Robert Herjavec
Black Unicorn Awards Judge
Star of ABC's Shark Tank
Founder & CEO of Herjavec Group

Recognized Industry-Wide

- MOST INNOVATIVE IAM PROVIDER — Cyber Defense Global Awards 2018 Winner
- SECURITY SERVICES LEADER — IDC Analyze the Future
- LEADER IN MANAGED SECURITY SERVICES — Cyber Defense Global Awards 2018 Winner
- SECURITY COMPANY OF THE YEAR — CDM Cyber Defense Magazine
- #1 ON THE CYBER SECURITY 500 — World's Hottest Security Companies
- TOP 10 ON THE 2018 TOP 100 MSSPs — MSSPAlert.com/Top100

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefensemagazine.com

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

Gary S. Miliefsky, Publisher & Cybersecurity Expert

ALWAYS FREE
NO STRINGS ATTACHED

RSAConference | Where the world talks security

Ensuring the security of your organization is always challenging, even in the best of times.

We created an **online resource center** to help you find the answers you may be looking for. It includes relevant content such as interviews with CISOs dealing with today's realities, preventing ransomware attacks, tips on how to improve your virtual presenting skills, and much, much more.

Browse our specially curated resources today, and keep checking back as new information is added regularly.

rsaconference.com/cyberdefense-2020

Lucio Frega, Threat Researcher
Deutsche Telekom - Cyber Threat Intelligence

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

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

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

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

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

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

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

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

About the Author/Disclosure

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

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