CDM

eMAGAZINE

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

IN THIS EDITION:

Supporting the Mobile 5G Transformation

Ransomware Finds a Way - Best Practices

The Psychology of Ransomware Attacks

The Role of Identity & Access Management

The Most Serious Threats to eCommerce

Can We Ever Reclaim our Privacy?

Biometrics is Not Enough for Smartphones

Five Common Incident Response Problems

Learn How to Leverage SOAR

…and much more

SEPTEMBER 2018

MORE INSIDE

CONTENTS

@MILIEFSKY

From the Publisher…

CyberDefense.TV is live and growing with more interviews each month…

Dear Readers

I have just returned from CloudSEC Europe 2018 where I shared the stage with some brilliant panelists. We discussed the ever-evolving role of the CISO. One of the items we agreed would become very important, is the standardization of measurements for risk to organizations. There's a new standard on the block, called FAIR - which stands for Factor Analysis of Information Risk (FAIR) and is emerging as the standard Value at Risk (VaR) framework for cybersecurity and operational risk. It is hosted and managed by The FAIR Institute , a non-profit professional organization dedicated to advancing the discipline of measuring and managing information risk, located at https://www.fairinstitute.org/. Membership is free, just like subscribing to our eMagazines,so what are you waiting for?

FAIR provides information risk, cybersecurity and business executives with the standards and best practices to help organizations measure, manage and report on information risk from the business perspective. The FAIR Institute and its community focus on innovation, education and sharing of best practices to advance FAIR and the information risk management profession. I've always been a strong proponent of standardization in Information Security - from the CVE (common vulnerability and exposure) standard for documenting 'holes' in our computing equipment, software, hardware and networks to CWE (common weakness enumeration) - a way to better understand how to write great code - writing software with security best practices by avoiding leaving exploitable flaws in your compiled code. This standard is one to learn about and share in your organization.

Some of the areas I consider critical include looking for and measuring risk around People, Apps, Networks, Computing equipment, Code and Data (plus the databases where we find the data). I call this PANCCD – yes another acronym – this time I invented it and I'll share more about it in upcoming articles. There will absolutely be more to come on the topic of making cybersecurity measurable so stay tuned!

Gary S.Miliefsky, CEO
Cyber Defense Media Group
Publisher, Cyber Defense Magazine

Our Vision: To be the Global Leader of Cyber Defense Knowledge & Information

From the Editor...

While our Publisher is speaking at numerous conferences including CLOUDSEC UK 2018 this month, we are also hard at work on our October global print edition of our magazine coming out on October 3rd at the IPEXPO EUROPE 2018 event in London, UK. We hope you enjoy this September eMagazine edition with many more to come. We're seeing major changes in the evolution of the threat landscape. We will keep you informed so that you can stay one step ahead of the next threat. Enjoy!

To our faithful readers,

Pierluigi Paganini

Editor-in-Chief, Cyber Defense Magazine

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by Cyber Defense Magazine and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

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

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

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

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

PUBLISHER
Gary S. Miliefsky, CISSP®

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

WE'RE CELEBRATING

6 YEARS OF EXCELLENCE!

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

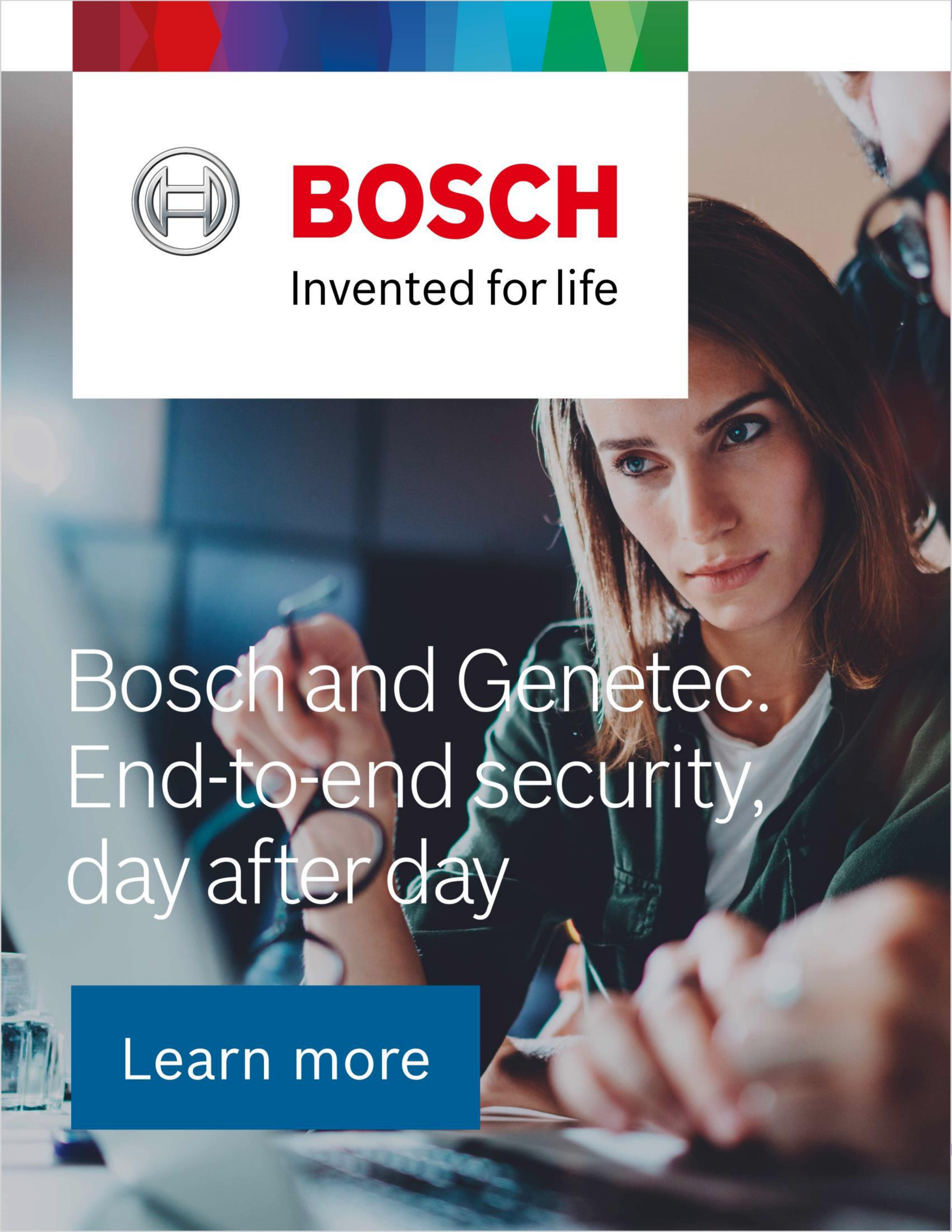
CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE **TV** **AWARDS**

SEE US IN OCTOBER AT...

IPEXPOeurope

SPONSORS


BOSCH
Invented for life
Bosch and Genetec.
End-to-end security,
day after day
Learn more

Visuality Systems

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

Encrypted

SMB VERSION 3

Secured Access To Remote Files

REAL-TIME CONTINUOUS DIAGNOSTICS & MONITORING

SHINE A LIGHT ON THE DARKEST CORNERS OF YOUR NETWORK

STIGs & Configurations

Continuous audit of policies & controls.

Threats & Vulnerabilities

Real-time discovery of Threats & Risk.

Asset Discovery

Automatic inventory & tracking of assets.

User & Entity Behavior

Monitoring of risky & unsanctioned activity.

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

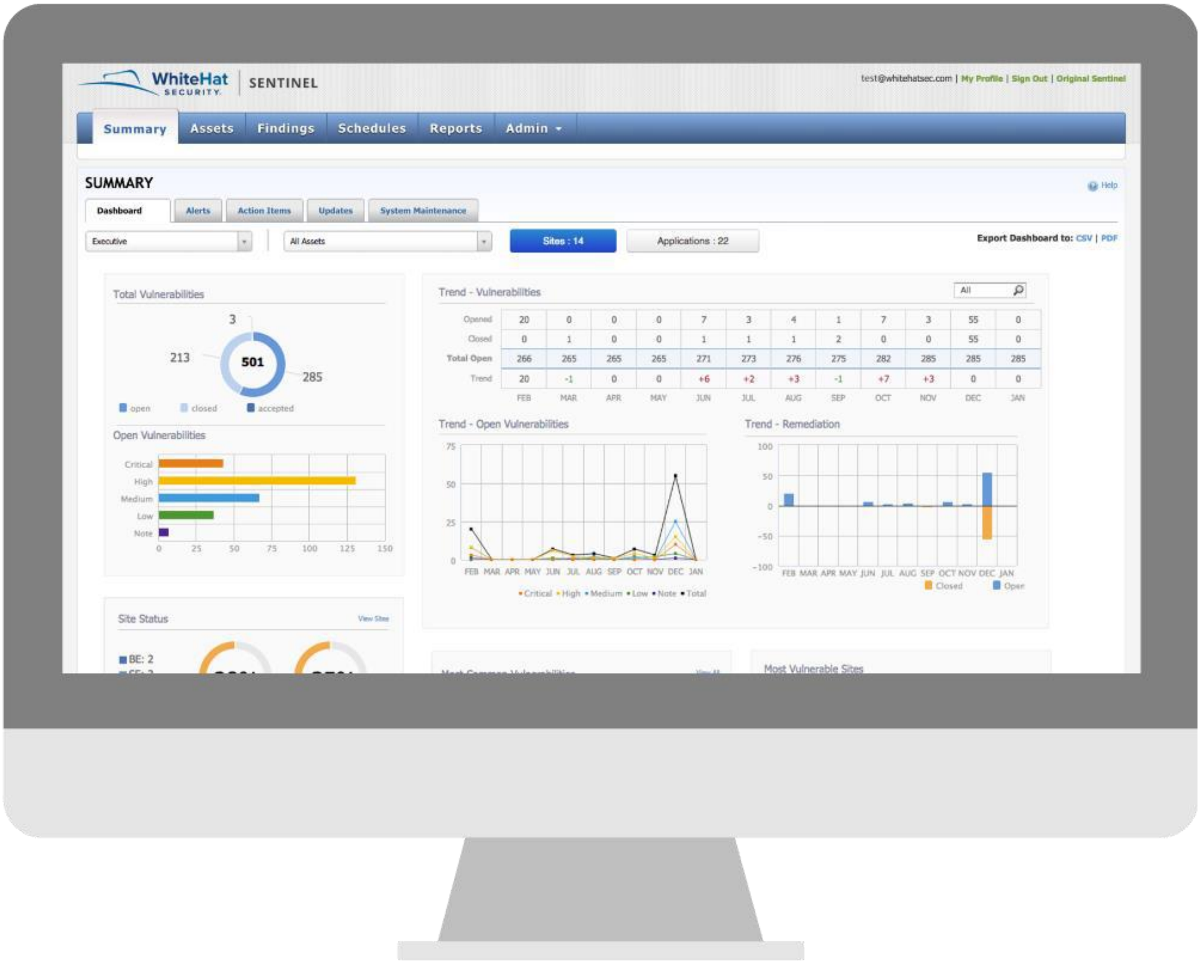
Look no further...

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

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

AristotleInsight®
— Identify | Remediate | Document —

AristotleInsight.com | Call us at 866.748.5227



	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN
Opened	20	0	0	0	7	3	4	1	7	3	55	0
Closed	0	1	0	0	1	1	1	2	0	0	55	0
Total Open	266	265	265	265	271	273	276	275	282	285	285	285
Trend	20	-1	0	0	+6	+2	+3	-1	+7	+3	0	0

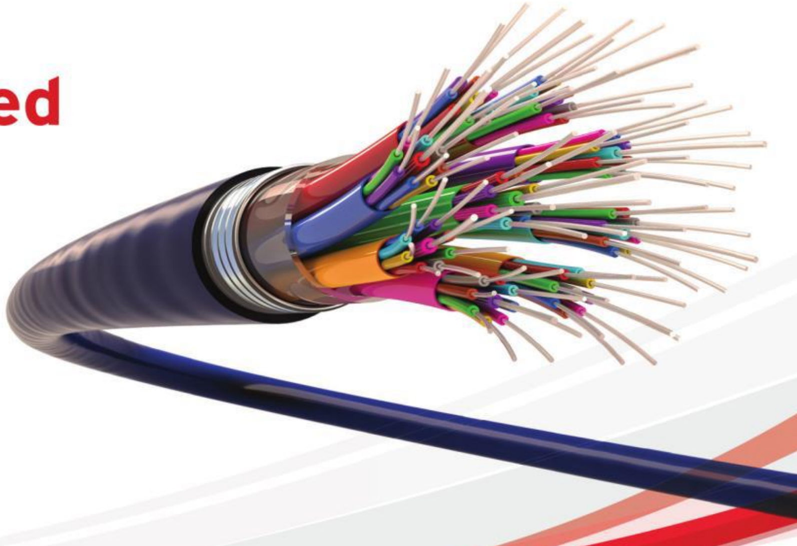
Your website could be vulnerable to outside attacks. Wouldn't you like to know where those vulnerabilities lie? Sign up today for your free trial of WhiteHat Sentinel Dynamic and gain a deep understanding of your web application vulnerabilities, how to prioritize them, and what to do about them. With 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 signup:
https://www.whitehatsec.com/info/security-check/

PLEASE NOTE: Trial participation is subject to qualification.

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

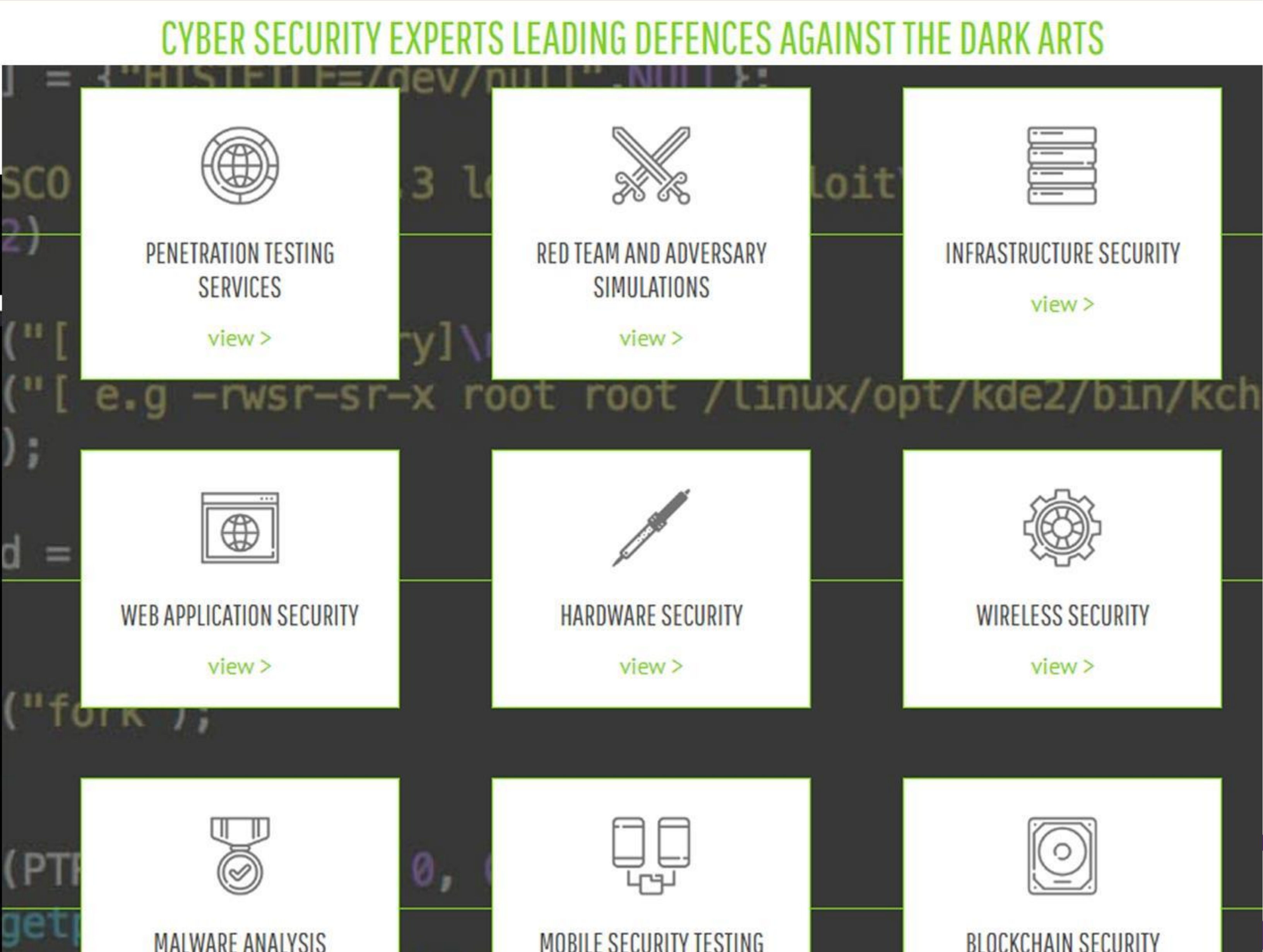
ZERO DAY INITIATIVE

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

www.trendmicro.co.uk/xgen-cyber

Hacking Experts

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



CYBER SECURITY EXPERTS LEADING DEFENCES AGAINST THE DARK ARTS

PENETRATION TESTING SERVICES
view >

RED TEAM AND ADVERSARY SIMULATIONS
view >

INFRASTRUCTURE SECURITY
view >

WEB APPLICATION SECURITY
view >

HARDWARE SECURITY
view >

WIRELESS SECURITY
view >

MALWARE ANALYSIS

MOBILE SECURITY TESTING

BLOCKCHAIN SECURITY

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

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

THIS IS 100% POSSIBLE WITH

GOANYWHERE®
Managed File Transfer

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

Dropbox

Google Drive

VOTIRO SECURED.

salesforce

SharePoint

Jenkins

Microsoft Dynamics 365

zendesk

Simplify Your Processes and More with Secure Cloud Integrations

Request a Demo: www.goanywhere.com/demo

ARTICLES

5G – Supporting The Transformation of European Mobility

5G will be more than the next mobile network evolution, it is set to be a real game changer for citizens and industry alike, addressing societal challenges and meeting the connectivity needs of new innovative services and businesses. Compared to previous generations, 5G will provide a significantly improved performance, handling up to a thousand times higher data volume with a similar increase in device density.

Thanks to this improved performance, 5G will be in a position to deliver enhanced mobile broadband services to support the digital transformation of European industry, including the automotive industry. 5G will also support the deployment of Iot with billions of connected devices over the next decade. 5G will be a key element in an industrial revolution across all sectors, leading towards distributed production management, low-energy processes, cooperative robots, and smart manufacturing and logistics. The transport sector, in particular, will become highly automated and provide new mobility business models for the transportation of persons and goods.

C-ITS continuity of service

Cooperative ITS (C-ITS) in Europe requires continuity of service, so it will be deployed concurrently with future wireless technologies, such as 5G for instance. Continuity of service will prevent vehicles equipped with earlier connectivity technologies from being excluded from the C-ITS eco-system. “Whatever the technology, safety applications will always require guaranteed uninterrupted communication. 5G is a promising mobile communication technology that can provide C-ITS communication. Considering the potential for reducing the number of fatal accidents, Dynniq anticipates the immediate implementation of C-ITS technology,” said Cees de Wijs, CEO of integrated mobility and energy solutions provider Dynniq.

Connected and automated driving concepts address key societal mobility challenges, in particular safety and quality of life in urban and densely-populated areas. Connected vehicles are able to learn from each other to gather and maintain a complete and reliable picture of the driving environment. For instance the presence of other road users, including pedestrians and cyclists, and also new road hazards, dangerous crossings or hidden corners will be made known to the entire fleet thanks to the Internet of Things.

Promoting automated driving with IoT is the main objective of the EU-funded Autopilot project, coordinated by ITS Congress organiser ERTICO. ERTICO will also participate in the EU-funded 5G-DRIVE Research and Innovation Action, for developing and validating key 5G functionalities and services, including network planning through pre-commercial testbeds for eMBB and V2X services, in collaboration with a twinned Chinese project led by China Mobile.

Breakthrough mobility concepts

"5G will enable the digital transformation of the transport sector towards a global Digital Smart Mobility paradigm, providing breakthrough mobility concepts and new innovative applications and services matching user needs and societal challenges," said François Fischer, Senior Manager Connected and Automated Driving at ERTICO.

Automated driving is a safety and time critical application with stringent connectivity requirements, in particular concerning latency. 5G will provide low-latency (<5 ms) connectivity that meets autonomous driving requirements. Fully automated driving will only be possible by providing all connected vehicles with a virtual picture of the driving environment in cloud and edge computing architectures, for which 5G network slicing features will be a major requirement.

Creating and maintaining a reliable virtual representation of the driving environment will also require the collection of data from billions of connected sensors. The challenge of this high density of connected objects will be addressed by 5G's massive Machine Type Communications (mMTC). Finally, Artificial Intelligence will be the ultimate enabler of driverless vehicles, particularly through deep learning and computer vision.

Join the 5G conversation at ITS World Congress

Reflecting the transformative potential of 5G, a number of sessions at this year's ITS World Congress are dedicated to this topic. The increased cybersecurity threat that goes hand in hand with the multiple new uses and applications offered by 5G is also dealt with in a number of related sessions.

5G-related sessions

ES09: Delivering Effective Cooperative, Connected and Automated Mobility (CCAM)
SIS17: Evolution from Current Automotive Connectivity and its Deployments to 5G and 5G C-V2X
SIS31: 5G with Satellite – Delivering Resilience and Reach
SIS55: Fusion of Road Infrastructure and Vehicle Sensor Data for Automated Driving
NS9: 5G /G5 Opportunities and Telecom Connections with C-ITS

At the congress, ERTICO will also host an informal workshop with a focus on: 5G for Automated Mobility.

Cyber security-related sessions

ES11: Enhancing Cybersecurity & Resilience of Transport Infrastructure
SIS10: Assessing Next Generation Technologies for Emerging Future Transportation Environments
SIS36: ICT Serving Automated Road Transport
SIS60: Cybersecurity For Public-Facing ITS Systems

To take part in the 5G and cybersecurity discussion at ITS World Congress, register here. To view the full programme click here, and for more information about the ITS World Congress 2018, please visit www.itsworldcongress.com

Ransomware Finds a Way - Best Practices to Minimize Negative Impact, Downtime After a Ransomware Infection

by Jim Varner, President and CEO, SecurityFirst

Ransomware has become a scourge to businesses around the globe and always manages to find a way to infiltrate even the best defenses. Whether it was a well-known recent outbreak from WannaCry or Petya/NotPetya, which spread worldwide in a matter of minutes, or a more random incident on a small business, school district, city, or healthcare provider, any one of these can be detrimental to an entities infrastructure and business operations.

After getting hit with ransomware, companies may lose data and have to spend money as they try to recover their sensitive assets, either through paying a ransom or a solid recovery process, or risk disrupting business continuity. Beyond any monetary figure, it's also possible they'll damage their reputation in the eyes of their clients and customers due to downtime and potential data loss, which can be even more detrimental to the business. By better understanding the threats ransomware presents, there are several essential preventative measures that can be done early to mitigate the impact, minimize potential disruption to business operations and more importantly – loss of critical data.

Ransomware – Preparation is Key

The growth and sophistication of ransomware variants has caused many companies to anticipate a potential infection, regardless of whether they're actually hit. Having a contingency plan in place is essential to both minimize the potential risk and the impact of ransomware.

Ransomware's attack vector is typically through email attachments, hijacked websites and adware, making it nearly impossible to protect against everything. However, there's a common thread linking all of these: the human touch. You can prepare and educate everyone in an organization to be wary of suspicious emails, downloads, content and websites, but sometimes even the best prevention simply isn't enough. And that's not all. Ransomware variants are spreading, with many slipping past even the best and most up-to-date defenses so it's important to remain vigilant, regardless of your role in an organization.

You might ask, "What about paying the ransom; it's not that much and it seems a lot easier and cost effective?" That's one way to go, but there is no guarantee you'll get access to your data again just like there's no guarantee you'll rid yourself of malware or viruses that are now on the network.

The fastest and safest way to recover is through strong preparation and a quick reaction to isolate the infected computer or server and shut it down before implementing your recovery plan. The complexity and speed of recovery relies on advanced planning and preparation including data backups.

Take a Layered Approach to Ransomware Prevention

There are several steps companies can take to prepare themselves if they're hit with a ransomware attack:

- **Updates are essential**: Update all systems, anti-malware and firewalls, and ensure all operating systems and software is up-to-date with the latest patches. This is basic security hygiene any company should do on a regular basis.

- **Practice data governance**: Determine what data exists across your organization and the stakeholders who are responsible for it. Data governance makes a difference - greater accountability including executing access policies and reinforcing best practices across the board will significantly narrow the potential attack.

- **Limit the attack surface**: Narrow the attack surface with more stringent access controls, advanced encryption, key management and real-time access monitoring. This also helps improve overall company operations while preventing other data losses and potential issues.

- **Encrypt your data**: If your files are compromised in a ransomware attack, strong data encryption ensures the data cannot be decrypted and exfiltrated without the proper authentication and authorization. It's a small but simple measure that goes a long way to protecting your assets.

- **Access controls matter**: Companies should limit data access to only those roles that absolutely need the data to perform their job functions by implementing role-based access controls (RBAC) and privileged access management (PAM).

- **Whitelist your applications**: Isolate workloads whenever possible by using a process of default-deny "zero trust" and whitelisting, which only allows access to decrypted data through a specific application or process. Put systems in place to always monitor who is accessing the data and when, so you aren't left surprised when unauthorized access attempts occur.

Data Backups Help

Back up data, specifically sensitive data, as a standard practice. A 2016 alert from the U.S. Department of Homeland Security (DHS) suggested data backup as a key element of any ransomware recovery:

"Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Note that network-connected backups can also be affected by ransomware; critical backups should be isolated from the network for optimum protection."

Having a backup and recovery strategy is a best practice, but the enormous amount of data organizations generate can be challenging to back up and if backups are stored on the network it can still be compromised. That is why DHS also suggests data be backed up offsite and air gapped from the network, which is where cloud, and specifically object storage, come into play.

What About the Cloud?

The cloud is growing in popularity as a viable option for data storage, allowing for easier data recovery since not all data is kept in the network and at risk for attack. However, just because data is in the cloud, doesn't mean it is secure. Without the right data security that encrypts data before it is sent to the cloud, cloud storage is just an open extension to your network and can be vulnerable as well. You should also control all aspects of access and visibility once the data is in the cloud.

Additional benefits to cloud storage come from using object storage and geographic dispersal to provide the redundancy and resiliency needed to quickly recovery from ransomware.

While only about 10 percent of an organization's data is used on a regular basis, companies may need to store the other 90 percent, sometimes for several years at a time, due to various regulatory requirements and processes. Object storage, especially when leveraging public cloud tiered pricing, can be a highly cost-effective answer for this issue, keeping the data stored away, but readily available for recovery. Since object storage connectivity is via API, it provides potential cost savings and air-gaps backup data from the operational network.

Geographical dispersal can be as simple as sharing the same encrypted copy to multiple cloud providers or locations to ensure if there is an issue on one platform, data can be easily recovered from another source. Other options available in the market today can split the data with resiliency across multiple cloud locations or providers – giving you an extra layer of security and speedy recovery when needed. Whether that's a ransomware or malware attack, or even in the event of a natural disaster, companies can be assured that their protected data is safe and recoverable.

Keep in mind with object storage, there are unique challenges, particularly privacy. While cloud service providers (CSPs) provide secure environments or even protection through encryption, you can only ensure proper security of the data in object stores of any cloud, when you are in control.

With the right approach, object store dependency and privacy concerns can be alleviated. Organizations must have technical and operational processes in place to explicitly block CSPs from accessing that data. The right approach is to use client-side access controls, encryption and encryption key management as a standard part of the organization's data protection strategy. By securing the data before it goes to object storage you won't sacrifice data security.

The Aftermath of a Ransomware Attack

Ransomware enables cybercriminals to take command and control of systems and business operations for quick financial gain or other malicious intent. Once a successful attack begins, companies often no longer have control or access to their most valuable assets: its data.

Getting back up and running after a ransomware infection, with minimal impact to time and resources, is essential to all organizations, regardless of their size. This necessitates making data protection with secure backup and recovery an essential part of any security process.

Remember the basics when you're recovering from a ransomware attack:

- Identify the infected machines and remove them from the network
- Determine if any other areas are impacted
- Examine your backups to ensure they are not affected
- Patch and scan devices on the network
- Bring new machines online as needed

By employing these best practices and taking a layered approach to ransomware prevention, you can ensure your data is protected. That way, if a ransomware attack still occurs, you'll be in the best position to regain control of your data so that you can get back online much faster, avoiding business disruption and data loss.

About the Author

Jim joined SecurityFirst in 2014 with over 36 years of experience in silicon technology, server development,telecom, security systems, and software management solutions at IBM and BLADE Network Technologies. He assumed the role of President and CEO of SFC in January of 2017. Jim is well respected as a subject matter expert in the areas of data security, server systems and management
solutions. Jim earned a degree in Engineering from Youngstown State University and currently splits his time between North Carolina and Southern California, typically close to the beach and the waves.For more information, visit https://securityfirstcorp.com

Psychological Operations Behind Ransomware Attacks

By Milica D. Djekic

The ransomware attacks could cause the sabotage of your entire IT infrastructure and you would agree with us that it's not pleasant at all to get your files or machines being locked and seeking from you some sort of the fees in order to stop that incontinent situation. In so many cases, you would not be sure if those campaigns could promise you that your data would get saved even if you pay for the ransom. On the other hand, this sort of attacks would give you the time limitation for paying for the fees and that could indicate some sort of psychological operations being directed to the common people.

Why would we believe that the ransomware attacks could get correlated with some sort of the psychological operations? First, if you need to pay for any sort of the blackmail within the restricted period of time – you would cope with the higher amount of anxiety, stress and even paranoia. This is quite unsuitable, right? It would appear that such an application would terrorize you trying to make you fulfill its demands. Here we come to the crucial words – being terrorized! We know quite well that any timing requirement being the part of a security solution would only assure your defense. Further, if anyone would blackmail you with any sort of sabotage giving you the limited time to pay for your security – you would undoubtedly get in position to deal with the psychological operations.

The ransomware products are the new generation malware and they would cause the quite frightening effects. So, if you would feel anyhow anxious, scared, stressed and even paranoid about this sort of the threats – you should think twice about the background of such a project. It's well-known that in defense mainly the terrorist organizations would show the intent to conduct some sort of psychological operations. So suddenly, your computer would put you under the pressure and you would feel so powerless in front of such a threat. That's exactly the effect so many terrorist groups would want to make. In this article, we would talk a bit more how the ransomware attacks could get correlated with the secret terrorist projects and why it is important to develop the strong countermeasures for this type of scenario.

The today's black market would offer a plenty of new technologies including the ransomware solutions. This sort of the product would get developed as the part of some cybercrime project that could get sponsored by so many malicious actors' organizations. The point of this effort is not to claim anything, but rather to try to provide a rational discussion dealing with the deep logical flow. In the other words, we would not make any suggestions on for a reason that could be speculative only and as the purpose of this effort; we would see the quite critical review of the ongoing circuitstances. So, we would get aware of that the black market is the place that could offer you the heaps of goods and services. The well-paid projects are those being accomplished by so skillful malware developers.

These guys would work so hard independently or as a team in order to create the new piece of the code that could cause harm to someone's IT asset. Next, it's also well-known that someone would pay for such a project and from the current perspective; it may appear that the cybercrime underground would develop such a malware for a reason to make a profit over the victims' vulnerabilities.

So, if the situation is as getting indicated – it could get quite clear that his new innovation in the area of a cybercrime could be the handy method for making the money on. On the other hand, we would notice that there would be some side effects with this project targeting the people's mind and psyche. In the other words, all of these could get correlated with the psychological operations. Our idea is that the terrorist groups could stand behind those projects. Maybe they would not develop the entire code, but they would define the requirements how such an application should work. If you are running out of the time, you would feel uncomfortable at least and in the case of the ransomware attacks when you are aware of that your entire business could go to waste, your level of anxiety, stress and paranoia would only go up and up. The ransomware projects got launched on the black market and it's quite logical that the cybersecurity experts would investigate these malicious codes and try to find the adequate resonse to such a threat.

The terrorist organizations would be more than happy to see the western people suffering such a sort of the attacks and we would not get surprised if they would sponsor those projects. In this effort, we would only make the linkage between the ransomware solutions and terroristic psychological operations. We would not try to convince anyone to believe into these suggestions, but rather try to warn the authorities to get such an idea in mind – once they make a decision to investigate such a case deeply. Apparently, the fact is someone would get the idea to develop the piece of the malicious code that would terrorize the people in order to make them suffer the wide spectrum of negative emotions and feelings. The modern cyber defense has developed some countermeasures to these situations, but that's not enough – because the black market would get flooded with the new and new technological offerings. The main question here would be who would stand behind these intelligently designed weapons. We would call these offerings the weapons for a reason they would literarily serve as the tools for making the profit on and conducting the psychological campaigns as well.

The main question here would be if the new generation threats would serve as the cyber weapons which role would be to raise our blood pressure on. The fact is that we are living in the quite turbulent part of the history and we should get aware of so many adversaries that would wish to cause harm to the majority of common people. The role of a defense should be to try to resolve such situations and we think there is still a lot of time and hard work to get invested into this sort of challenges in order to get tackled.

About the Author

Milica D. Djekic is an Independent Researcher from Subotica, Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the book "The Internet of Things: Concept, Applications and Security" being published in 2017 with the Lambert Academic Publishing.

Milica is also a speaker with the BrightTALK expert's channel and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Her fields of interests are cyber defense, technology and business.

Learning from our Oversights: Banking, Phishing, and Cyber-Insurance; Oh my!

by Mr. B3N3; Cybersecurity Lab Engineer

A bank robber, after being apprehended, years ago was asked: “Why did you rob the bank?” The simple and direct response was, “That’s where the money is.” There is no difference today. Organizations will be targeted due to an asset the attackers want access to. This may be data or information, or the familiar cash.

An incident happened in Virginia to a bank and within eight months, the same issue presented itself. These illustrate the importance of relevant, regular training for phishing attacks and review of cyber-insurance policies by the appropriate personnel.

Incidents

The target was The National Bank of Virginia located in Virginia. The bank was compromised twice in eight months. The total amount stolen between these was an estimated $2.4M. The first was on May 28, 2016. This attack continued through Monday (Memorial Day), and was subsequently detected. The focus of this and the 2nd successful compromise was cash. Once compromised, the money was stolen through hundreds of ATMs across North America with cards whose magnetic strips had been the true user’s data placed on them. The ATMs initially with the first incident had stolen $569,648.24.

Once detected the bank contracted with Foregenix to complete the forensic review. In June 2016, the bank put in place the additional security protocols recommend. Curiously, the bank was breached again, allegedly by the same group, in January 2017. The attackers through this attack were able to steal $1.8M.

Methodology

The two rather deeply probing and expensive attacks were successfully completed with simple phishing emails with attachments. Typically, the user opens the email, clicks on the link or opens the attachment, and potentially the IR (Incident Response) Team and other operation teams subsequently have a long day and/ or weekend ahead of them. With the first attack, the initial compromised computer connected with and compromised another computer within the bank. This second computer accessed the STAR Network. This is managed by First Data and is used to manage the debit card, transactions, customer accounts, and the use of ATM and bank cards.

With the compromised computer, the attackers had the ability to disable and modify the anti-theft, and antifraud protections that normally are in place for the banks clients. This included the bank clients PIN, withdrawal limits for the individual person, daily usage, maximums for the debit cards, and fraud score protections. The bank clients were pwned.

The interesting twist is either by luck or learning from the 1st attack, the attackers also gained access to Navigator in the second attack. Navigator was used by the bank to manage their customers debits and credits.

During the compromise #2, the attacker credited the bank ‘s client accounts for $1,833,984 from several hundred ATMs. The second compromise also occurred over a weekend, between January 7-9, 2017. To make matters worse, the attackers updated for their needs or removed the bank‘s critical security controls.

Cyber-Insurance

The bank did have cyber-insurance in place and in force at the time of the attacks. The insurance company was Everest National Insurance Company. Once the claim(s) had been filed, the insurance did not want to pay. There were two exclusions, and the insurance company claimed this fell under their Debit Card rider. The bank then filed a lawsuit in the Western District Court of Virginia, Roanoke Division (Civil Action No 7:18CV310).

Lessons Learned

Cybersecurity presents a new environment for the enterprise to thrive in. One aspect that is particularly new is cyber-insurance. The insurance industry is still working to detail the working, interpretation, and the method on how to apply this. In purchasing this service and insurance, the business needs to be wary and complete the due diligence, so senior management is aware of the coverage, as much as they are able to.

One aspect to fully explore are the exclusion riders. These, when possible, should be minimized in number. Where these are required, any ambiguity in the wording should be explored and detailed, while being documented. With this, any ambiguities should be limited. Notwithstanding a section to the contrary, the emails and other documents should fill in the gaps.

With the exclusions, this would work to limit the insurance company’s exposure to certain attacks. The industry may not know of a certain attack or one that had not been published yet. The attack vector may not be known yet. The business may be waiving their right to coverage for an unknown attack, or one that had not been created yet.

The business should actively consider consulting with an attorney specializing in this area with regard to the cyber-insurance policy and rider. The agreement and insurance rider are written with the insurance company’s interests in mind. The sections and riders may be vague where needed, and be able to apply exclusions where they may need it.

Insurance works, in theory, and practice, by pooling risk. The pool consists of individual policies. The insurance companies use large mathematical formulas to determine what factors to take into account. The larger the pool, assumptively the less overall risk, fewer claims, and subsequently larger profits. If there are too many claims, the insurance company’s profits will be lower. As this is relatively new, the pool of clients purchasing this type of insurance is not massive. As this is the case, a few compromises certainly could affect the operational and net income for the insurance company. The insurance organizations are profit driven, and not an altruistic entity.

Even if the organization follows industry standards and recommendations, there may be issues. The InfoSec environment is ever-changing. There are new attacks, updated old attacks, nuances, or old issues never fixed. To anticipate every issue and attack angle is not possible.

Phishing continues to be a rather viable attack vector, with attacks increasing in numbers and believability. These can be skillfully crafted, with the business symbols and graphics. All it takes is one person in the right department (e.g. accounting, finance, tax, or Human Resources) clicking on one link and the business operations can get very interesting, very quickly. The phishing training needs to be regular, and relevant.

About the Author

Mr.B3N3 began coding in the 1980's. Presently Mr. B3N3 is a Cybersecurity Lab Engineer at a Tier One supplier to the automobile industry. Mr. B3N3 has completed the PhD (IT and System Engineering) and interests include cryptography, SCADA, and securing communication channels. He has

Signs That Indicate Your WordPress Site is Hacked

Discovering a website hack on time is very important; if you detect it late, it would already have caused you great damage. Here, in this article, we'll be discussing WordPress website hacks and how to know if your WordPress website has been hacked.

Why hackers love WordPress websites...

Hackers, as we know, are always after things that are popular on the internet. WordPress is definitely the most popular among all CMS platforms and powers over 60 million websites today. Hence, it's quite natural that hackers target WordPress websites; statistics are that every single minute there are over 90,798 hack attempts that are being made on WordPress websites.

What kind of WordPress websites are attacked?

This is an irrelevant question. Hackers can target anyone and anything. Any person, any network or any website can be hacked. But still, to make it simpler, let's put it this way. Hackers are always looking for common security errors that website owners make and vulnerabilities that websites have. In other words, a hacker always targets a website that is weak. The key, hence, is to fortify your website against hacking attacks. Still, if by any chance, there happens to be some vulnerability or error and a hack happens, it's always good to spot it on time. For that, you need to be aware of the hack signs that you have to be on the lookout for. Here we go, discussing WordPress website hack signs that could help you take timely action and avoid incurring big losses:

1. You get the “This Site May Be Hacked” message

If, while going through the search engine results, you happen to see the message "This Site May Be Hacked" right below the link of your website, it's a clear indication that your website is hacked. You should act immediately because any user who's perhaps searching with a keyword for which your website is ranking would come across this message and would avoid your website.

2. Spam emails that are sent from your website

If there's any indication of anyone getting spam emails from your website, you should think of taking some precautionary measures. Hackers, when they get control of websites, especially those with a clean record, they use it to send spam emails to unsuspecting people. You should always remember that email servers have security measures in place that would detect websites sending out spam emails and then blacklist them. So, if your website is sending spam emails, it could also end up being blacklisted and that could cause you much loss.

3. Your website becoming slow and unresponsive

Whenever a website becomes slow or unresponsive, it could be a sign that it has been hacked. But there could be other reasons as well. The website would have had a sudden increase in traffic and that too would cause such an issue. At the same time, if your WordPress website has been hacked, it would definitely become slow and unresponsive as hackers would most probably be using the website server to carry out malicious activities.

4. Visitors to your website get redirected to some other site

If any visitor to your website complains of getting redirected to some other website, it could be an indication of a website hack. Hackers would hack your ranking WordPress website and redirect users to some other website that they are using for executing some other purposes. This would also lead to a massive fall in traffic for your website.

5. When an antivirus flags your website as unsafe

When an antivirus software starts flagging your website as unsafe, you need to do the checks and see if it's hacked. Antivirus tools are designed to protect users from websites that are hacked and hence infected with malware. This is to protect the users from getting their systems infected.

6. You discover themes or plugins that you haven't installed

If your website administrator finds themes or plugins that weren't initially installed on your website, then it's best to check if the website is hacked or not. Hackers, in order to create backdoors on a website that they have hacked, sometimes install plugins on it. This would help them later to have an access to the website even if it's cleaned by a security expert and the infected is removed. So, if ever you find any plugins or themes that you hadn't installed on your WordPress website, then it could probably have been hacked.

7. When your web host disables your website or issues warning

If you get a warning mail from the web host or if your web host disables your WordPress website, then it's almost certain that your website has been hacked. Sometimes the web host would send you details of the exploit and also give you a deadline to fix the issue failing which your website would be suspended. Shared hosting providers, who host multiple websites on the same server, would be extra cautious and may straightaway disable your website so that others don't get affected. Take quick action and repair the issue so that you don't incur huge losses.

8. When your website gets blacklisted by search engines

Search engine crawlers always check websites to find out if they are compromised in any way. On finding a compromised website, the search engine would immediately blacklist it. So, if under any circumstance, your website gets blacklisted by a search engine, you should immediately look into it and confirm if it's hacked.

9. When you detect new admin accounts that you hadn't created

If ever you detect new admin accounts that you hadn't created for your WordPress website, it could be an indication of a website hack. Of the many roles assigned by WordPress to website owners, the administrator has access to all the areas of the website. The others (editor, author, contributor, SEO editor etc) may have limited access only. So, hackers who compromise your website would quietly create admin profiles so that they can later start handling your website as per their requirements. So, if ever you find a new admin account that you hadn't created, do the needful and get things mended on time.

10. If your website comes up during searches for illegal medicines

This is something that shouldn't be happening! If your WordPress website shows up during searches for illegal medicines- Nexium, Viagra etc- you should take it as an indication of a hack. Your website might have nothing to do with these medicines, but users searching for those medicines would find your website listed with descriptions mentioning these medicines appearing below the website link on the search engine. This would affect the traffic greatly and you could end up suffering great losses. Take action immediately and fix the hack.

About the Author

Julia Sowells is a security geek with almost 5+ years of experience, who writes on various topics pertaining to network security. Julia frequently writes for us here at Cyber Defense Magazine on very interesting and well timed cyber security related subject matter.

How Automation Can Ensure Speedy, Successful PAM Deployment

In today’s operating environments, where threats are increasing in volume and sophistication on a daily basis, security and IT leaders are forced to balance protecting an organization’s critical data to ensure business continuity and enabling users and administrators to be productive at work.

Years ago, companies aimed to prevent hackers from gaining access to their systems by erecting firewalls and perimeter defenses focused on keeping bad actors out. However, this approach has grown outdated and ineffective. Organizations no longer have the luxury of automatically trusting anything *inside* or *outside* its perimeters, and instead must now focus on verifying and protecting the devices and privileged users already inside an organization from being exploited.

Today, controlling and monitoring which system users need privileged access to accomplish specific tasks is extremely important to mitigating the risks posed by insider threats, preventing data breaches and meeting compliance requirements. A privileged user is someone who has administrative access to critical systems, and privilege should only be extended to trusted users. Privileges include the ability to change system configurations, install software, change user accounts or access secure data, which is why only responsible users should be trusted with these privileges.

Privileged access management (PAM) is a suite of functionality that protects privileged user accounts from compromise by providing a safe environment in which users with privileged access may access target systems with credentials managed by the PAM system on behalf of the user.

The bigger and more complex an organization’s IT systems get, the more privileged users they have. These privileged users could include employees, contractors, remote or even automated users, and some organizations have as many as two to three times as many privileged users as employees.

With today’s operating networks evolving at such a rapid pace, countless organizations have lost track of the endpoints, devices and infrastructure attached to their network. Organizations are also behind on rolling out protections to their critical infrastructure.

Unfortunately, for many organizations, this all means it is not a question of *if* but *when* a breach will occur. However, PAM aims to keep organizations safe from accidental or deliberate misuse of privileged access by offering a secure, streamlined way to authorize and monitor all privileged users for all relevant systems.

FAILED PAM DEPLOYMENTS

The first challenge in proactive cybersecurity is gaining ―situational awareness,‖ or a solid picture of the network environment — even the ―invisible‖ portion. To see users, network devices and connections, security teams are required to collect significant network information and assemble it into a model of the network. Combing through all of this data is difficult, especially when the only resource may be a spreadsheet of device inventory data created months ago that is likely both out of date and missing information.

Unfortunately, there have been a significant number of failed PAM deployments in recent years as IT systems grow bigger and more complex. When deploying PAM, organizations often run into challenging issues, including two incredibly difficult steps. First, it‘s very hard to detect every device and privileged user on a network. Then, its excruciatingly difficult to put all of those users and devices into a PAM system and deploy everything needed for PAM.Many organizations don’t expect PAM deployment to take as long or cost as much as it ultimately does in many cases. Consequently, countless companies either give up or can’t continue to invest — and their deployment fails.

As a result, too many companies have no idea which assets and privileged users are connected to their networks, presenting both security risk and complexity when deploying countermeasures. Fortunately, automated discovery tools can help to get handle on assets, ensuring they’re managed securely and that PAM is being deployed on time and on budget.

HOW AUTOMATION HELPS

Increasingly, a critical component of a robust cybersecurity program is automation. Hackers and bad actors are progressively developing and deploying automated attacks in order to scale more effectively and to reduce the amount of direct support and instruction that many traditional cyberattacks require. To effectively compete against this level of sophistication, organizations need to combat automation with automation.

Before companies can effectively manage privileged access, they have to identify and catalog devices, assets, configuration data, access paths and security policies. Automation makes this process faster, easier and more accurate than ever before.

DISCOVERY

While some companies have a solid inventory of critical assets, many do not. And for those that don’t, an automated discovery tool can be incredibly helpful. Today, advances in automation technologies allow organizations to detect privileged users and devices on the network quickly and more efficiently than ever before.

After an automated discovery tools reveals the privileged users and devices on a network, the real fun begins. The information provided during automated discovery offers insight that powers automated orchestration tools to provide complete coverage with the PAM deployment.

ORCHESTRATION

Automated orchestration technologies enable users to arrange and manage the myriad of security technologies in place at most companies (i.e. firewalls, IDS/IPS, sandboxes, endpoint security agents, ticketing systems, deception technologies, vulnerability scanners, behavioral detection tools, etc.), eliminating the manual effort that comes with managing assets in an identity security platform. With most PAM vendors, users would have to go out and manually configure servers one at a time or figure out how to script the servers themselves.

Orchestration is vital as it directs all activities relating to an organization’s standard operating procedures, delivering consistently predictable results and optimal utilization of available resources. High-tech tools reduce the once time-consuming orchestration of hundreds of servers from months of work down to just a few moments, significantly reducing the time it takes to deploy PAM solutions.

IN THE END…

Talented IT staffers are fighting an uphill battle as cyberthreats appear more frequently and grow ever more sophisticated in today's increasingly complex IT networks. In fact, 2017 set the record for both the most breaches and the most data compromised in a year. In order to claim victory in this environment and adequately secure critical assets and data, IT security teams must plan for PAM as a core preventative and monitoring technology.

Automation reduces or completely removes the friction associated with PAM deployment. It levels the playing field by keeping servers, devices and infrastructure up to date, limits or prevents lateral movement in a breach and prevents insiders from damaging complex critical IT infrastructure. In today's public-private cloud environments, servers are added rapidly to an environment. Automated discovery and orchestration tools allow PAM components to be deployed in just a few minutes, not hours or days, to protect new cloud servers. While many companies may be able to fuse copious amounts of security tools to protect their IT infrastructure, it still requires a significant amount of manual effort.

Data breaches are not going away anytime soon, and as the threat of cyberattacks continues to increase, organizations need to reconsider how security is managed. In the era of constant connectivity, it's vital that companies leverage available tools and technologies. The best tools are all-in-one security platforms that revolutionize the speed at which PAM can be deployed by automating the discovery of assets as well as the onboarding of all target systems into the platform, providing continuous protection against identity-based breaches in even the most dynamic environments.

Cameron Williams is the founder and CTO of OverWatchID, the industry's first Converged Identity Security Platform, comprising Privilege Account Management, Cloud Access Security Brokering, Identity Access Management and MultiFactor Authentication in a multi-tenant SaaS platform.

Going Beyond HIPAA Compliance: A Case Study

A Case Study on how Black River Memorial Hospital Improved Security Posture

HIPAA compliance is a big piece of any healthcare organization's cybersecurity process. However, the goal of any compliance audit is to ultimately improve security posture. In healthcare, this requires measures such as monitoring vulnerabilities and tracking privileged user rights to not only document compliance but remediate threats.

"AristotleInsight has been a significant tool in helping me accomplish data mapping all the information into, within, and out of our organization. Tracking the flow of data in a healthcare organization is a challenging project, but I feel like we now have proof of control over the systems."

Ideally, a healthcare organization will implement a single solution capable of this. At Black River Memorial Hospital, that solution is AristotleInsight®.

Proving Compliance at Black River Memorial Hospital

Celebrating their 50th year of assisting patients, Black River Memorial Hospital provides key services such as:

- Occupational Health
- Diagnostic Imaging
- Dialysis
- Emergency and Urgent Care
- Homecare
- Hospice
- Medical/Surgical Inpatient Care
- Nutrition Services
- Obstetrics
- Pain Clinic
- Rehabilitation
- Respiratory Care
- Home Medical Equipment and Supplies
- Surgery

In Black River Falls, Wisconsin.

The task of overseeing Black River Memorial Hospital's security posture along with ensuring compliance with frameworks, including HIPAA, belongs to Brett Spafford, Information Security Specialist. Spafford credits AristotleInsight as a large help with accomplishing her job.

“I feel that using AristotleInsight, I have more proof of control over the network and that I’m better equipped to handle HIPAA security compliance and documentation requirements.”

AristotleInsight is an Integrated Visibility platform that provides Continuous Diagnostics and Monitoring of security functions such as Configurations, Vulnerabilities, Privileged User Management, Asset Inventory, and Threat Analytics.

The system collects and reports on vast amounts of data from users, devices, applications, processes, and endpoints.

“Having one solution with so many capabilities and tools has helped so much through several risk assessments because of how many security areas the product covers,” says Spafford.

“Being able to make recommendations supported by the analytics and metrics in the system has helped our leadership teams make informed decisions about where to focus resources for our security program.”

Improving Security Posture

In addition to documenting compliance with security frameworks, it is imperative that healthcare organizations are continuously monitoring their security posture and making improvements.

“IT Departments need tools like this to automate processes, set alerts and provide an “at a glance view” of the details all the way through trends.”

One area that traditionally troubled organizations is vulnerability management. Without a continuous monitoring solution, organizations are left facing questions such as ‘who applied this patch? or ‘why was this vulnerability accepted?’.

“We utilize the vulnerability management features of AristotleInsight to set goals and track patch management progress,” explains Spafford. “We are able to report out to other departments on the metrics of vulnerability management to show how the department has improved processes.”

“We are easily able to focus our efforts on the workstations that have the highest levels of risk, or where vulnerabilities are the most widespread so we can have the biggest impact.”

Exploitable vulnerabilities and privileged user accounts are two of the most common targets for attackers of healthcare organizations. Spafford is confident in Black River Memorial Hospital’s ability to monitor both areas.

“By using information on privileged users, we have been able to tighten our security controls and improve administrative processes. Tracking active directory changes and reviewing system activity shows the clear separation of duties that are required during risk reviews.”

What differentiates AristotleInsight from other monitoring solutions is the forensic level detail of the collected data. The advanced machine learning platform UDAPE® tracks any changes made and provides the diagnostics needed to track security events.

“The drill-down capabilities have given me forensics tools to determine how a particular machine became infected. I was able to use that information to put other security defenses and alerts in place and to educate users on risks based on threats that targeted our organization,” explains Spafford.

“We are able to create the timeline of events on command and control, malicious software, and indicators of attack. These tools help identify, protect, detect, respond, and recover to show our cybersecurity maturity improvements to The Joint Commission, Baldrige Excellence, and the NIST Cybersecurity Framework.”

“IT Departments need tools like this to automate processes, set alerts, and provide an ‘at a glance’ view of the details all the way through trends.”

AristotleInsight® for the Healthcare Industry

The needs of organizations in the healthcare industry are constantly changing. It is important for a security solutions to be able to adapt along with these changes.

“One of my favorite things about AristotleInsight is how it has evolved through compliance changes in regulatory requirements and best practices and how it responds to the ever-changing threat landscape,” explains Spafford.

“Over time, my favorite features have changed because it continues to get better and better as information security becomes more complex. I appreciate the scope of the product and services that offer so many tools for tracking, reporting & alerting, and improving processes within one, affordable solution.”

Black River Memorial Hospital, and Spafford trust the Integrated Visibility platform, AristotleInsight from Sergeant Laboratories, with their cybersecurity monitoring and reporting.

“AristotleInsight has been a significant tool in helping me accomplish data mapping all the information into, within, and out of our organization. Tracking the flow of data in a healthcare organization is a challenging project, but I feel like we now have proof of control over the systems,” says Spafford.

“I don’t feel like I could work in information security without this product.”

About the Author

Josh Paape is an Online Marketing Specialist at Sergeant Laboratories, a leader in security and compliance solutions that allow businesses, governments, and healthcare institutions to comply with regulations and stay a step ahead of criminals. As a graduate of the University of Wisconsin - La Crosse, Josh has experience marketing products from a variety of industries. As a contributor to CDM, he hopes to spark new thought and discussion topics in the information security community.

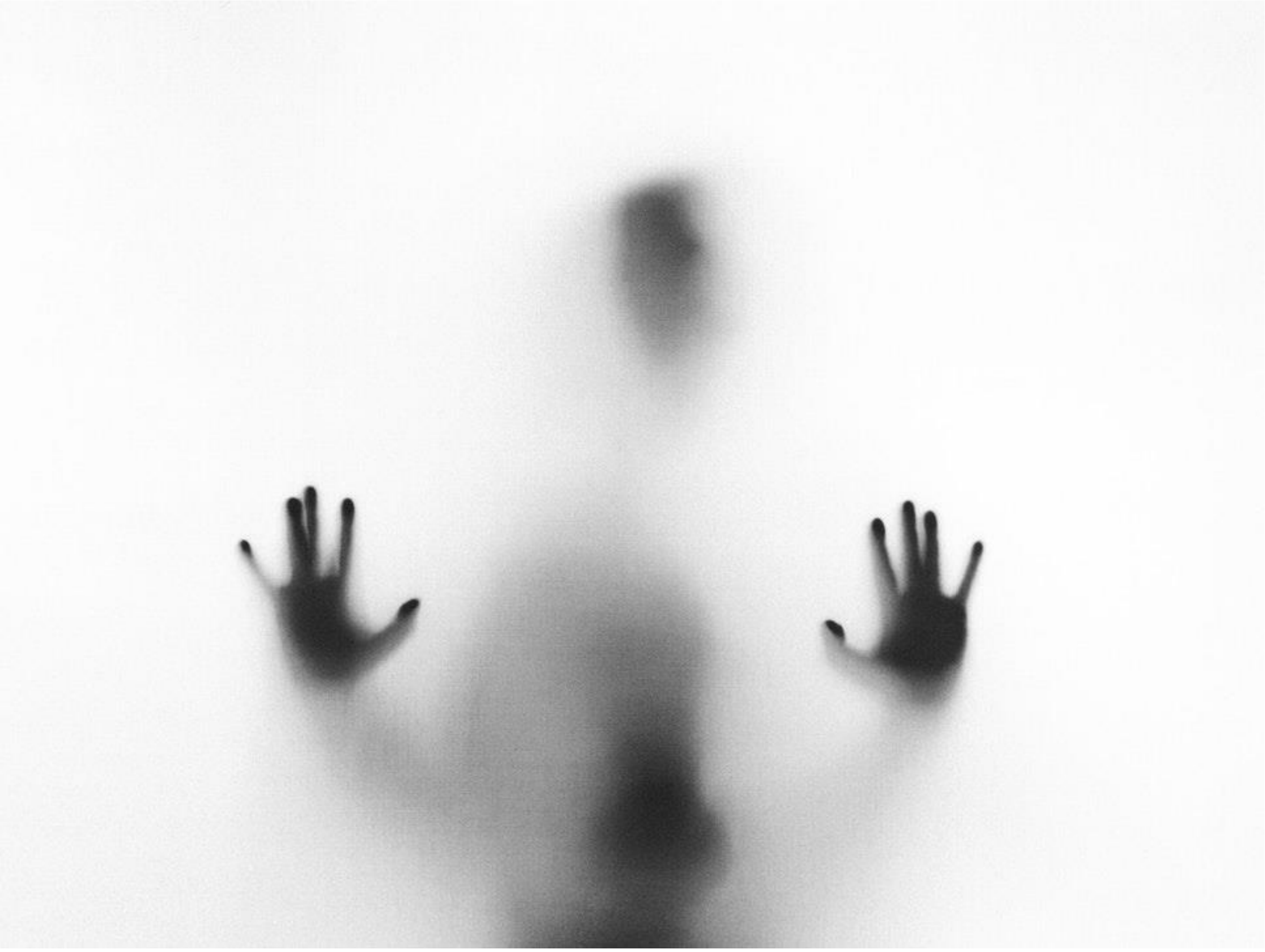
Connect with Sergeant Laboratories: https://www.sgtlabs.com
Sergeant Laboratories Blog: https://www.aristotleinsight.com
LinkedIn: https://www.linkedin.com/company/sergeant-laboratories-inc
Twitter: @Sergeant_Labs

The Four Most Serious Threats Facing Online Businesses In 2018

by Matt Davis, Future Hosting

Online crime will cost businesses $2 trillion in 2019. SME's can't afford to ignore the risk posed by DDoS attacks, ransomware, phishing, and cryptojacking.

Businesses can't afford to ignore online crime. The average cost of SME security breaches has risen by 62 percent over the last five years. In 2019, online crime will cost businesses an estimated $2 trillion..The cost of combating online crime is far less than the potential cost of a successful attack. It is inexpensive and straightforward to mitigate the risk of the most common types of attack, but first you have to know where your business is most likely to be hit.



DDoS Attacks

Distributed Denial of Service attacks have been overshadowed in the media by the up-and-coming attacks we'll look at in a moment, but over the last year they have become larger, longer, and more sophisticated.Newly discovered vectors for launching amplified replication attacks have increased the amount of data attackers can send to victims. The use of open memcached instances is particularly worrying: a recent attack against GitHub using this vector broke the previous record, peaking at over 1.35TB per second. That record was broken soon after by an attack that measured 1.7TB per second. Businesses without a DDoS mitigation solution in place cannot hope to combat attacks of even a fraction of this volume.

Phishing attacks

Phishing attacks continue to be a major source of data leaks and security breaches. Phishing attacks use email to trick victims into installing malicious software, disclosing sensitive information such as login credentials, and even transferring money directly to the attacker by masquerading as a company executive. While automated spam detection solutions can limit the impact of phishing attacks, the only real defense is training. Employees must be trained to identify phishing attacks and to understand the risk inherent in

Ransomware

Last year, tens of thousands of businesses and millions of individuals lost data or money because of ransomware. WannaCry, NotPetya, and Locky became household names. We have seen fewer high-profile attacks this year, but thousands of businesses have been the target of ransomware in 2018.Businesses should use a two-pronged strategy to reduce the risk of ransomware. First, they must stop ransomware entering their network by following security best practices and ensuring that all software is regularly updated. Second, comprehensive, automatic backups to a remote location remove the ability of attackers to extort victims in exchange for their data.

Cryptojacking

Cryptojacking uses malware to mine cryptocurrencies like Monero. When a malware infected web page is loaded by a browser, it uses the device's resources to mine cryptocurrency coins.The growing prevalence of cryptojacking is one of the reasons that ransomware attacks declined slightly over the last year. It generates more money with less effort. In 2017, cryptojacking attacks increased by 8,500 percent. Most cryptojacking attackers use vulnerabilities in internet-facing software to compromise out-of-date or misconfigured web servers, eCommerce applications, and content management systems. Phishing attacks are another common vector. The best defense is to update software to remove vulnerabilities and to ensure that all software is configured by someone who knows what they are doing. The best way for SMEs and startups to defend their businesses against online crime is to understand the risks and take basic security precautions.

About the Author

Matthew works as a writer for Future Hosting, a leading provider of VPS hosting. He focuses on data news,cybersecurity, and web development topics. You can usually find his hiding behind a computer screen, searching for the next breaking news in the tech industry. For more great articles, check out FH's blog and give them a follow at @fhsales

Inadequate Cybersecurity Hurts Where it Counts the Most

by Adrejia L. A. Boutté Swafford, Partner/Attorney at Christovich & Kearney, LLP

According to the Merriam-Webster.com Dictionary the term, “cybersecurity,” first used in the year 1998, are the “measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack.” What happens when you failed to properly protect? You get hacked, phished, breached, or the victim of countless other types of cybercrimes. Cybercrimes cost money, reputation, or even one’s livelihood. Protect yourself *before* **and** *after* the crime. Get cyber risk insurance.

There should be a legal mandate requiring cyber risk insurance in the United States. Rational for this requirement should in part be influenced by the fact that, the increasing number of cyber liability policies are partially motived by the ever-developing mandatory notifications of data breach laws and the high costs of said notifications to consumers. Moreover, the ever-developing world of technology, and increasing use of the Internet of Things (IoT) devices, simply create a mountain of vulnerabilities which extend far beyond the commercial walls of a business. The threat has evolved past the Fortune 500 company’s poor firewalls and has easily entered the homes and smart devices of every person living “on the grid.”

Cyber risk means something slightly different to an individual than to an entity. Nevertheless, people are at the heart of both. “Cyber risk includes any risk associated with online activity, such as storing personal information online or completing online transactions. This includes damage to you or your business’ reputation, loss, or disruption to your life or your business operations.” How we define our degree of cyber risk, prior to an actual cyberattack event, is often directly correlated to what we believe we can afford to lose. Instead, the risk should be directly correlated to our value; what we have to lose.

Annually, an estimated $8.5 billion are incurred for cyber-related losses. The value of data and information put at risk for an individual and/or an entity, will greatly increase as the number of violations and breaches continue to escalate. The cost of this risk is not only quantitative--as in it will cost an exact amount of money to recover from the breach but, it can also mean exposure to fines, criminal charges, and/or the value in a name.

Insurance is generally procured to transfer risk from one to another. We also obtain insurance for a financial reimbursement after a loss. Cyber risk insurance can offer more than financial recoupment for actual loss. Many cyber risk policies bring breach coaches, attorneys, reimbursements after paying ransom fees, and access to other experts and risk management plans. Cyber risk coverage can come in the form of a stand-alone policy or an add-on or an endorsement to an existing policy. It is not typically covered under traditional homeowner's policies or commercial general liability policies.

Cyber risk insurance policy is just as practical as buying health insurance or automobile insurance. Although we have, as U. S. citizens, governmental and regulatory bodies in place to help prevent and protect us from a cybercrime or cyber incident; it is not enough. The alternatives, to cyber risk insurance, simply help us mitigate our exposure. They do not and cannot prevent the inevitable so don't forget to:

1) Assess your risk,
2) Beef up your cybersecurity,
3) Consult with a cyber risk specialist,
4) Be clear about your risk to your when you meet with your insurance broker/agent, and
5) Get a tailored cyber risk insurance policy.

Adrejia L. A. Boutté Swafford is an insurance defense attorney at Christovich & Kearney, LLP in New Orleans, Louisiana. She has practiced commercial defense litigation for over 12 years, focused on: insurance coverage disputes, homeowners' insurance policies, automobile insurance policies, toxic torts, premises liability claims, assisted living facility issues, construction law claims, and workers' compensation; among other areas.

Adrejia also offers services on compliance related matters, including but not limited to, corporate consultation (regarding organizational/business ethics, state, federal, and industry standards) and litigation work based on general compliance issues and cyber risk insurance policy issues.Adrejia can be reached online at: alboutte@christovich.com http://linkedin.com/in/Adrejia-bswaffordcyberriskno1 , and at www.christovich.co

How SOAR Can Help You Get Amazing Results from Your Security Analysts

by Stan Engelbrecht, Director of Cybersecurity Practice, D3 Security

Security orchestration, automation, and response (SOAR) platforms are becoming increasingly prevalent security operations tools, emerging out of the categories of incident response, security automation, and threat intelligence platforms in the last few years. Some SOAR platforms are narrowly focused on automating simple tasks, but leaders in the sector are expanding SOAR across the SOC with numerous modules and the ability to orchestrate across the entire security stack.

The best SOAR solutions are valuable for everyone on a security team, from people on the front lines to managers and executives tracking reports and metrics from a birds-eye view, or even compliance and legal personnel working outside the SOC. Because SOAR can act as a central hub within the SOC, it helps coordinate efforts through automating escalations and task assignments, eliminating data siloes, and enforcing adherence to policies in workflows. These unique capabilities have allowed SOAR to become the heart of the SOC for many organizations.

Of all the roles that SOAR supports, security analysts see the most direct benefits, because SOAR automates and simplifies repetitive manual tasks like event escalation, intelligence gathering, contextualization, scripting, collaboration, and reporting. To illustrate how significant this impact can be, let’s take a look at how a SOAR platform can make an analyst smarter, faster, wiser, and even happier.

Smarter

A large part of the role of an analyst in an enterprise SOC is evaluating what alerts pose real threats and how best to handle them. An analyst with a few years of experience may have built up their ability to effectively Assess alerts, but with a SOAR platform in place, their decisions can be augmented with contextual Information aggregated via integrations with the security systems and threat intelligence sources on which they rely.

Analysts can also use tools like link analysis and incident timelines, which ease investigations by visualizing patterns and relationships. Even bi-directional SIEM integrations help analysts "be smarter", because the SOAR tool can dynamically grab additional relevant data—from a prior event, for example—and present it to the analyst as part of the incident record's contextual element. No matter how skilled your analysts are, having the full story of each alert drastically reduces human error while boosting alert management and decision-making capabilities.

Faster

The need for speed is real—especially given the volume of alerts and increasing complexity of targeted cyberattacks. Fortunately, with a SOAR platform, when an analyst opens up an incident record, the grunt work has already been done. With an incident already confirmed, contextualized, and prioritized, an analyst simply needs to oversee the response—and approve, when necessary—any security actions, such as blocking a website, closing a port, or disabling a compromised account. Compared to a manual response to a typical phishing incident, which might take an hour, a SOAR-powered response should only take 45 to 90 seconds.

Wiser

Security teams accumulate tribal knowledge over time about the history and patterns of incidents, plus the intricacies of their IT and security infrastructure. Senior analysts can build up this wisdom over time, but without a way of documenting the lessons they have learned, their wisdom is lost when they leave the organization—or simply go on vacation. With the right SOAR platform, senior colleagues can codify their knowledge into playbooks, guided workflows, and reports, and share their experience with the team, including in the critical onboarding phase for new analysts. Junior analysts can also access historical data from every previous incident to see how comparable cases have been handled in the past. This empowers the entire team with the wisdom of their most experienced analysts—past or present.

Happier

It may seem trivial, but the happiness of analysts can have a significant impact on the functioning of a SOC. Without the right systems in place, analysts often get frustrated with the relentless pace of menial, repetitive tasks. With the growing cybersecurity skills gap, high turnover can be crippling for a security team, because it is hard to hire and retain talented employees.

Put simply, SOAR platforms reduce burnout. With automation and orchestration, analysts spend less time on tedious tasks like copying and pasting hashes, looking up reputation data in third-party apps, and chasing after false positives. This lets them focus on meaningful tasks that require skill and protect the company from genuine threats. With SOAR, analysts get more done, feel less overwhelmed, and have much higher job satisfaction.

About the Author

Stan Engelbrecht is the Director of Cybersecurity Practice at D3 Security and an accredited CISSP. Stan is involved throughout the product delivery and customer success lifecycle, and takes particular interest in working with customers to configure solutions.

You can find Stan speaking about cybersecurity issues at conferences, in the media, and as the chapter president for a security special interest group. You can find more writing from Stan on the D3 website http://www.d3security.com/

5 Common Incident Response Problems that Automation and Orchestration Can Help Solve

by Stan Engelbrecht, Director of Cybersecurity Practice, D3 Security

Most companies that are struggling with their incident response program fall into two categories:

1. They don’t realize what their problems are, because they’ve always done things a certain way
2. They know exactly what their problems are, but don’t have the resources to fix them

Whichever category your company is in, you probably have many of the same problems as other organizations. There are a handful of universal issues with which almost every incident response program struggles. Incident response platforms (IRPs) have always offered some assistance with these issues, but recent advances in automation and orchestration technology have vastly expanded the impact an IRP can have.

In this article, we’ll look at five of the most common incident response problems and how an IRP that leverages automation and orchestration can help solve them.

Problem #1: Lack of Personnel

It's no secret that most SOCs are understaffed and overworked, so perhaps the most obvious problem for many security analysts is that they are too busy to give major incidents the time they deserve. Unfortunately, this problem reinforces itself: if a company is unable to hire enough analysts, their analysts become stressed and dissatisfied. Those employees are more likely to quit, which makes the hiring problem even worse.

An IRP with automation features can solve the two problems going on here: the quantity and quality of analysts' workloads. With automated investigations and actions, analysts don't have to spend their time on repetitive low-risk tasks. Automated risk scoring to identify false positives also reduces the number of alerts analysts need to respond to, and automated reporting and notifications mean analysts can collaborate without getting bogged down in time-consuming administrative tasks.

Being able to focus primarily on challenging security incidents keeps analysts happy, and should result in lower turnover across your security team.

Problem #2: Lack of Context

Ironically, the problem that security analysts face isn't a lack of information; it's that there's too much information with no way to make sense of it. In most SOCs, an overwhelming amount of security data comes in from numerous systems, but stays in those separate repositories. When an analyst is evaluating a new incident, they must gather the information they need manually, going from system to system.

With automation in place, each incident can be enriched with both external (e.g. threat intelligence) and internal information (e.g. SIEM data, link analysis, previous incident records). This instantly reveals the context of the incident, not only saving analysts from having to waste time gathering data, but also isolating the important information to inform their decisions.

Problem #3: Lack of Scalability

Your existing incident response processes might work fine—but only at a certain scale. Manually managing tasks, communications, and investigations is feasible for minor incidents, but when a major incident hits, you'll be in trouble. Incidents that involve compliance reporting, complex forensics, and thousands of workstations will quickly reveal the shortcomings of an ad hoc incident response program.

A centralized platform with automation and orchestration features is the best way to scale your response capability and prepare for major events. Automation allows you to conduct investigations and conduct actions at a large scale, instead of, for example, manually pulling data from every affected system and blocking individual IPs. Orchestration features leverage centrally logged data to communicate tasks across teams and execute workflows throughout the company, facilitating fast and consistent response at scale.

Problem #4: Lack of Collaboration

In most organizations, teams work in siloes. These divisions are reinforced by the tools teams use, because without common software solutions, it is especially hard to communicate securely, share data, and work together on tasks. Many companies are forced to rely on emails, spreadsheets, and other makeshift methods for communication and collaboration.

For collaboration to be efficient, secure, and properly documented, there needs to be one centralized system that supports users beyond the security team. An IRP with security orchestration features can perfectly meet this need. Automated notifications, reporting, and task assignments make collaboration part of the everyday workflow. Task management dashboards and case management folders enable users to track and share work across teams. As an added benefit, a strong IRP will have configurable access controls, so data confidentiality can be preserved when sharing incident records between teams.

Problem #5: Lack of Prioritization

Reducing incident volume isn't the only way to alleviate the strain on your analysts. You can also do it by effectively prioritizing the incidents they deal with. Many companies don't have a way to determine how potentially serious an alert is until after it's been investigated. This leaves most analysts spending the majority of their time chasing after alerts that turn out to pose no real threat.

Organizations with solid incident record data have an incredible resource to tap into, yet many don't even realize it. By tagging every resolved incident as either a false positive or a true positive, you can build a dataset that your IRP can mine to learn what factors most highly indicate false positives. Then automation and orchestration can be used to automatically resolve events that are very likely to be false positives, or sort them to a lower priority position in analysts' queues.

About the Author

Stan Engelbrecht is the Director of Cybersecurity Practice at D3 Security and an accredited CISSP. Stan is involved throughout the product delivery and customer success lifecycle, and takes particular interest in working with customers to configure solutions.You can find Stan speaking about cybersecurity issues at conferences, in the media, and as the chapter president for a security special interest group. You can find more writing from Stan on the D3 website
http://www.d3security.com/

4 Concrete Ways Threat Intelligence Can Make Organizations Safer

by Jonathan Zhang, Founder and CEO, Threat Intelligence Platform

The practice of threat intelligence (TI) is gaining momentum, helping organizations of all sizes to better understand and fix their weak links before cybercriminals have enough time to exploit them instead. This is made possible through the collection and integration of evidence-based data — actual facts about organizations' online assets including websites, domain names, hosting infrastructure, and servers.

This information comes in handy in today's cybersecurity landscape where hackers and scammers always seek the easiest approach to access sensitive data and deceive employees and customers into committing mistakes. In this article, we talk about the specific ways TI enables security professionals to step up their game, mitigate risks, and respond faster in the event of a data breach.

Thinking like a Cybercriminal

What's going on in the mind of cybercrime perpetrators? What type of threat — malware, phishing, spoofing, ransomware or else — is going to bring them the highest financial yield? As part of their sophisticated plans for attack, cybercriminals spend a lot of time analyzing their targets and then decide what is most logical for them to maximize returns.

TI allows security teams to follow a similar process but focusing on what reinforcements their organization requires as a priority in order to minimize the likelihood of successful data breaches. In that sense, TI is about proactively thinking a step ahead and spotting misconfigurations that may result in harmful yet avoidable damages.

Smart Resource Allocation

TI is not a silver bullet, however. Once their most salient vulnerabilities have been identified, companies must take actions. An advantage of incorporating TI insights in the cybersecurity roadmap is that those enable security professionals to take into consideration their particular gaps and allocate their security budget accordingly — rather than blindly following all security best practices out there without bearing context in mind.

For example, let's say that your company's biggest security problems are poor encryption and malware. Hackers repetitively manage to gain access to your website and upload files capable of running malicious code. And when visitors download and open these documents, they inadvertently release spyware that silently collects their sensitive personal data — names, addresses, credit card numbers, and passwords — as they make purchases online or sign in to various applications.

In this scenario, a threat intelligence platform could recommend how to improve encryption — e.g., reconfiguring SSL certificates and enforcing HTTPs — and conduct a domain malware check, retrieving details about emerging threats from various cybersecurity databases and providing guidance on how to deal with them.

Third-Party Monitoring

When cybercriminals find it too hard to reach a company directly, they may turn to partners and suppliers with more lenient security practices. So when CSOs implement TI, they should not only consider how their own infrastructure may be conducive to data breaches but also pay attention to third parties with whom confidential or strategic information is frequently shared.

In fact, chances are that your marketing department is using various cloud services on a daily basis — such as email marketing platforms and social media tools — to streamline their operations. But to function and segment subscribers adequately, these applications need customer data including their email address, identifier, past purchases, and location.

From a cybersecurity standpoint, transmitting personally identifiable details to third parties is a risk, and TI assists in assessing the reliability and safety of external vendors' systems before selecting them and throughout the execution of contracts.

Tackling Data Breaches

Data breaches are still going to happen, no matter how much effort organizations put into avoiding them. What makes the difference between a small and significant cybersecurity incident, however, is often the speed of response. Conducting a TI analysis can help limit damages and recovery time by providing a list of security weaknesses that may have been exploited by hackers and scammers.

Security professionals and investigators can use that information to narrow down the possibilities of what went wrong and take appropriate actions faster — e.g., contacting relevant authorities, temporarily freezing affected systems, and alerting customers.

Through the use of evidence-based data, threat intelligence has become a valuable instrument to learn more about system vulnerabilities, allocate resources intelligently, monitor third parties, and deal with data breaches.

About the Author

Jonathan Zhang is the founder and CEO of Threat Intelligence Platform (TIP). He has vast experience in building tools, solutions, and systems for CIOs, security professionals, and third-party vendors and enjoys giving practical tips for better threat detection and prevention. Jonathan can be reached online at jonathan@threatintelligenceplatform.com and at our company website https://threatintelligenceplatform.com/.

From Theory To Practice: 5 Applications Of Threat Intelligence

by Jonathan Zhang, Founder and CEO, Threat Intelligence Platform

Threat intelligence (TI) has caught the eye of CSOs and cybersecurity teams seeking to fight cybercrime strategically while allocating IT security budgets more efficiently. In fact, 60% of organizations already implemented TI initiatives, and 78% of practitioners feel that their security capabilities and responsiveness to threats have increased as a result.

While these numbers show that the popularity of TI is on the rise, some security professionals do not yet see the full value of TI and what it can do for their organizations in concrete terms. This post aims at bridging that knowledge gap, looking at five practical applications and how TI connects to common cybersecurity efforts you might be currently undertaking.

1. Malware Detection

From ransomware to spyware to viruses, it's hard to keep track of the countless forms of malware emerging every day around the world. As part of their evidence-based data collection process, TI applications typically conduct thorough domain malware checks and retrieve actionable information from major anti-malware databases — e.g., detailing the nature of such attacks and their evolution and sharing best practices around how to detect and tackle them.
Security analysts who can get access to this centralized information avoid a lot of redundant and repetitive work. Instead of researching about each malware that may affect them, TI makes it possible to proceed directly with the analysis of IT systems and, if necessary, the removal of known malicious software with tried-and-tested techniques.

2. Phishing Prevention

Gone are the days when all phishing threats could be spotted with the naked eye. Today's social engineering attacks such as spearphishing and website forgery are highly sophisticated and convincing. TI can support security professionals and other employees with the detection of advanced scams by collecting data from reliable public sources — like whois data — and identifying signs of fraud that include:

- Newly registered domain names similar to those of well-known brands and companies
- Contact details that differ across touchpoints and are inconsistent with verifiable records
- Strange domain activity, e.g., domain owners and hosting providers changed multiple times within a short period

3. Vulnerability Investigation

The likelihood of successful cyber attacks remains high no matter how much organizations invest in protecting their infrastructure and data. Understanding the cause of a breach, however, can be challenging, especially when working with multiple internal systems and third-party applications.

In that context, TI can be used as an investigative instrument, checking for the most salient vulnerabilities, and providing an overview of potential weak links — e.g., misconfigurations, poor encryption, and malicious files that may have caused the loss of sensitive data.

4. Cyber Defense Optimization

Even when no data breach has occurred, various organizational changes require security professionals to reconsider whether their company's cyber defenses are still optimized — e.g., mergers, acquisitions, spin-offs, joint ventures and partnerships, outsourcing of business processes, and software and hardware upgrades.

IT operations may evolve drastically in such instances, potentially leading to new gaps exploitable by hackers and scammers. TI can help to spot emerging weaknesses resulting from business decisions and establish a cybersecurity roadmap to tackle these by investing in new tools and software or reconfiguring and harmonizing systems.

5. Security Awareness

Not all cyber attacks can be prevented through technology, however. It's not rare for threats to go undetected by antivirus, firewalls, and other applications — meaning that regular employees often end up as the last line of defense against hackers and scammers.

For that reason, it's essential to keep staff informed about the dangers that may come their way. TI insights can assist with the coordination of security awareness initiatives bearing in mind existing IT vulnerabilities and, therefore, where cybercriminals are the most likely to strike.

More and more organizations are allocating resources to the practice of threat intelligence, practically relying on it to detect and tackle malware and phishing, investigate their infrastructure's weak spots, and empower targeted security awareness.

About the Author

Jonathan Zhang is the founder and CEO of Threat Intelligence Platform (TIP). He has vast experience in building tools, solutions, and systems for CIOs, security professionals, and third-party vendors and enjoys giving practical tips for better threat detection and prevention. Jonathan can be reached online at jonathan@threatintelligenceplatform.com and at our company website https://threatintelligenceplatform.com/.

Cyber Forensics: An Academic Partnership with Pittsburgh Technical College

by Professor Phil Grabowski

One of the most important aspects to get a Cyber Security or Security Forensics job is to show evidence of work experience, internships, certifications, participating in Cyber Security Challenges, and degrees. Philip Grabowski Professor at Pittsburgh Technical College for the School of Information Systems and Technology does exactly that with hands on experience in the classroom. Using a wide variety of forensics tools in the classroom for Digital Forensics, Ethical Hacking and Cyber Security.

Grabowski not only teaches the theory of forensics or Cyber Security he uses hackathon's and cyber security challenges that are provided free of charge to his students from Symantec Coyote Diamond, IBM's Master the Mainframe contest, Syracuse SEED Labs, and the Digital Forensic Research Workshop (DFRWS). More importantly Grabowski insist in academic partnerships with industry technologies and companies.

Studies from Ponemon from the 2017 Cost of a Data Breach Study show us that the amount of days to detect a breach is over 200 days. It is imperative that students get acclimated to software in the classroom before they leave school, because the average time an IT person gets to look at software on any given IT day is about a half an hour maximum. That is why companies like AlienVault, Paessler PRTG, Correlog, Belkasoft, and Commodo provide an Academic Partnershp and free software to PTC's Information Technology students.

Students can obtain an associate's degree in Information Systems in a concentration of Network Administration, Security, and Programming. They can continue their education at PTC with a bachelor's of science with a concentration of Information Technology, Information Systems Security, and Information Systems Development.

PTC is also partnered with IBM Academic Initiative, Cisco, and Red Hat Academy. Using the tools in the classroom is imperative. We have three different Security Incident and Environment Management Software (SIEM's) that can be used in the lab environment such as Alien Vault, IBM Qradar, and Correlog. Seeing all three products at any given time has advantages. Students get firsthand experience installing the product, patching the product, maintaining the product, and monitoring the resources of the product. Before they leave school they have real hand on experience of industry product that are used in the field. This generate sales in the future because students have heard of the product and use the product. They also become important voices to C-level management about products.

Several students that have graduated from the associates program have come back and stated that the knowledge they gained from using software in the classroom helps them with their day-to-day operations. Companies that hire from PTC IT graduates are currently using AlienVault and PRTG.

The Ponemon study showed that a majority of breached organization were notified by someone other than their own staff. Grabowski concludes that is a problem because IT people do not know the software used in the industry. They don't have time to analyze the software and they don't have time in their day to day operations to learn how to use the product. If it is in the classroom first we can literally send out hundreds of students a year with product knowledge. To be able to be a professional tester you must use the same techniques that a criminal hacker does to search for vulnerabilities.

At any given moment a student can spin up a virtual workstation on VMware Virtual Center Stack using hybrid Nimble Technology and create an entire infrastructure. Any distribution of Linux can be used as well as any Microsoft Operating System. Linux distribution for security include Kali 2018, Deft, Paladin, and Security Onion. Grabowski also uses Syracuse's University's Security Education (SEED) labs provided by Dr. Kevin Wu, which are based off Ubuntu. The SEED labs provide an abundance of training for information security education.

IBM Qradar a SIEM runs on Redhat, AlienVault runs on Debian. Correlog runs on anything and can be easily installed onto a Windows operating system. PRTG is also a self-install onto a Windows operating system. We are marketed these tools thoroughly in the cyber security realm. However, who has time to understand what is going on with the product. When we monitor things in something as common as Wireshark sniffer, we could literally learn something new every day. When using something like Wireshark we can see everything happening we just need to learn how to filter it properly to find what we are looking for. Did a rogue device get an IP address from a Man in the Middle (MITM) attack? Did a Bluetooth device connect to the network or device? Was a door opened that was connect to a Google Hub? Did the Nest Smoke detector generate an encrypted alarm?

More importantly as we start to understand these breaches, how did we detect them? How did we reconstruct the events? Using tools such as Belkasoft Evidence Center, Encase, FTK, Autopsy, or OSForensics in conjunction with Linux Distros of Kali for Pen testing.

Even more beneficial is determine an actual false positive in a SIEM. Recently we were trying to detect torrent traffic on our network and we having problems popping the alarm. Then a week later the alarm popped up in the executive summary dashboard as torrent traffic. The port was reporting 17500, which isn't common for torrent traffic. Torrent traffic is on ports 6881-6889. Was the port obfuscated? Pinging the IP address of the VM we retrieved a host name which corresponded to a student ID. Upon questioning the student to determine if they were running torrent traffic they denied their involvement. Believable because the student was a trustworthy student. Research concluded that he opened Drop Box on the computer, which indeed uses port 17500.

Students also participate in live hackathons or in Master the Mainframe contest. Symantec held a hack that included Ransomware. Students had to determine a bitcoin address, look in Wireshark to find the URL, gain admin rights of the website, and then convert the encrypted file using key with Python. Technologies included Wireshark, bitcoin, Ransomware, PHP, Python, Linux. In that particular hackathon there is a tremendous gain of reconstructing events, which become a valuable asset to our skill sets that reinforce the theory in the classroom. We learn something new every day from the products we get to use every day.

About the Author

Phil Grabowski is an IT Network and Security Forensics Instructor at Pittsburgh Technical College located in Oakdale Pennsylvania. He has an AS degree in Specialized Technology Electronics from Penn Technical Institute, BS degree and Information Systems with a concentration in Security from University of Phoenix, MS in Management with a concentration in Security from Colorado Technical University, and a MS in Information Systems and Communications from Robert Morris University. With over 20 years' experience as a hardware technician in the field he now teaches over 20 courses at PTC as a full time faculty member. He is also an IBM z Champion for his work with Mainframe Technology.
http://www.ptcollege.edu
Grabowski.philip@ptcollege.edu
Twitter: procoachphil

Why Smartphone Security Should Grow Beyond Biometrics

After passwords and traditional biometrics, behavioral biometrics is transforming the security of smartphones

by Alex Miller

An average user either uses a PIN, pattern or a password to secure his phone. When it comes to passwords, we are advised to create strong ones that are hard to crack, but the problem is, they are easy to forget. In a study conducted UnifyID, 75% of the respondents said it was difficult for them to track their passwords and 83 percent claimed they never want to use a password on their phone again.

That's just the customer's side of the story; wait till you hear the vendor's side. The IT staff complains that resolving the password issue is a significant drain. As per the Forrester Report, users contact help desks 28 times a year for password issues. What about the two-factor authentications? Don't they provide an added layer of security? Yes, they do make it difficult for attackers to impersonate a user, but it's a cumbersome process which most users don't want to get into.

Thanks to encryption and biometric, a user no longer has to enter a password to access his phone or type multiple special characters the next time he wants to use his smartphone for purchasing something. Mobile manufacturers have started embedding biometrics such as fingerprint or face, voice or iris sensors to provide a higher security assurance to users. People like choosing convenience over security and biometrics relieved them of the responsibility of creating and remembering a strong password.

The thing is, the biometric system has a few complications too. Firstly, it requires deliberate user behavior. Scanning your face or finger every time you want to access your smartphones adds a friction to the user experience. If you think biometrics is hard to compromise, then you are wrong. It's not as secure as people think it is. Researches came up with synthetic fingerprints for unlocking 65 percent of the smartphones. Even an algorithm can mimic your voice with a few audio snippets and fool your biometrics just like that.

Biometrics and Passwords are vulnerable

Passwords have always been a weak link. Yes, they are hard to keep track of but people still use them because they are easier to change if compromised. But when it comes to biometrics, in case it's stolen, you cannot change your face or your fingerprints, right? Ever since biometrics technology was introduced, cybercriminals have done their research to come up with tactics and backdoors in the system to steal the fingerprints of users. One example of that is the breach at the Federal Office of Personnel Management in 2015 that leaked fingerprints of 5.6 million people.

Security experts are worried that if more and more smartphone users start adopting fingerprints for authentication, this could lead to a series of identity thefts. You already know that it's possible to steal fingerprints but do you know that facial recognition can be tricked too by using a photo on a Windows or Samsung smartphone?

In conclusion, anyone can break into your phone even if it is password protected or requires biometrics authentication. Who knows what a criminal can do with your personal data from there. An unlocked device is just like a treasure chest for an unauthorized user. They can access your online banking accounts, emails, calendar, photos, or even install a tracking app such as Xnspy to monitor your location, and online behavior. Hackers even have a way of tapping into the Bluetooth or Wi-Fi connection of your phone, sniff your network traffic and steal all locally stored passwords and the passwords that you type when you check into your bank account. Crazy, right?

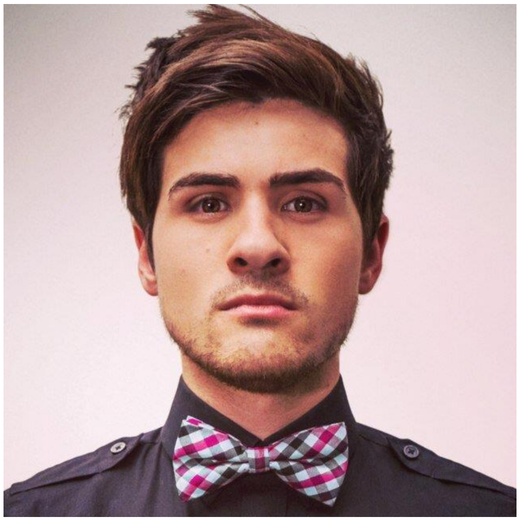
So what's the future of mobile security then?

If passwords and biometrics fail to provide smartphone security, how is a user supposed to protect his device? This question needs attention. Fortunately, companies such as BehavioSec, UnifyID, and SecureAuth have started employing different aspects of behavioral biometrics to provide better security to smartphone users.

Behavioral biometrics measure the patterns of user activities. The user is authenticated by what he does rather than what he is. The machine learning algorithm gathers the smartphone sensor data and determines the user by his personal traits such as walking gait, the way he sits, or the Wi-Fi access points his device typically connects to. These algorithms also take into account the changes in the user behavior. Let's say a user sprains his ankle and that changes his gait and because of that the machine learning systems loses confidence in authenticating him. In that case, it will then present an alternative method of authentication to the user like a PIN or a password. This is something only an authorized individual would know.

Lots of industries (finance, travel, hospitality, e-commerce, and healthcare) have already started employing behavioral biometrics measures. Although it's not a foolproof method, since our behavior uniquely identifies from the rest, it is a more secure system for authentication than what's available so far.

About the Author



Hi, I am Alex Miller a front-end developer for a VoIP company in Tennessee. As a part of my routine, I review the latestgadgets and applications.

Currently, I am covering the best apps available in all the major categories. I love watching football and Netflixing when I have some extra time. First Name can be reached online at (milleralex572@gmail.com) and at https://en.gravatar.com/milleralex1

Rampart de Troika: A Three-Step Process to Overcome Cybersecurity’s Top Threat

by Daniel Jetton, Vice President of Cyber Services, OBXtek

The weakest link in most network security is human; however, recent research has determined an effective, three-part process to mitigate the human factor vulnerability.

The Human Factor

Many cybersecurity experts consider the greatest threat to network security to be the manipulation of people to circumvent protocols. People are the wildcard because firewalls, intrusion detection, doors and passwords are predictable. People less so. The manipulation of people to penetrate a network is defined as social engineering. Hackers prefer this psychological, non-technical attack method because using human interaction to subvert security protocol is easier than penetrating a network using direct means.

Mitigating Social Engineering

Despite the prevalence of social engineering, research shows that mitigation can effectively be broken down into a three-step process. The research demonstrates the relationship between cybersecurity training and reduced social engineering incidents. The study concludes that three steps must be taken to counter social engineering and mitigate the threat:

1. **Awareness/knowledge** introduces the user to threats and the need to be vigilant.
2. **Training** prepares users to address and act on threats to minimize loss by exploitation.
3. **Reinforcement** ensures users remain vigilant in their activities to combat social engineering.

The process has been named the Rampart de Troika (fortification of three).

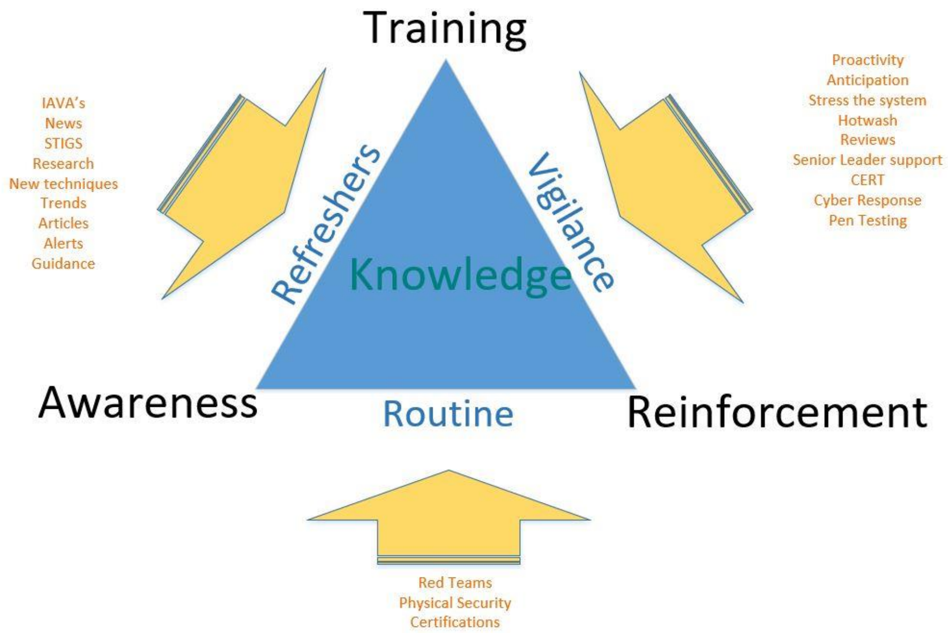


FIGURE 1. JETTON'S RAMPART DE TROIKA.

Awareness

Awareness is the first step in confronting social engineering threats. Here, a user is introduced to the tactics of the social engineer, such as vishing (telephone), phishing (email), and smishing (text) exploits. Within this step users must learn the value of information as well as sources of exploitation used by social engineers.

Training

Training is the next step. Once awareness is created, users learn what to do and what not to do. Users learn to not only protect their valuable company information but to also actively defend against engaged social engineers.

Training Musts:

- Whether conducted in a classroom or online, training must be as hands-on and realistic as possible.
- Training must be consistent, which means everyone at the company must have the same information and guidance.
- Regardless of whether training is internally or externally sourced, it must reinforce what the company values and deems important while teaching users how they can avoid and/or mitigate social engineering techniques.
- The training should cover, at a minimum, disclosure of personal information, policy review, effective destruction of old data, credentials, challenging individuals, physical security and techniques/motivations of the social engineer.

The standard should be no less than quarterly training, so that skills and vigilance do not diminish over time.

Reinforcement

Reinforcement is the last step in the Rampart de Troika. Because unused skills lose their effectiveness, a company must not only actively test its staff with social engineering cold calls, phishing emails and chance meetings, but also notify employees that it will test them to ensure retention.

As in most cases, an important part of reinforcement is emphasizing the positive through incentives. Those who follow the proper protocol in response to any security incident should be rewarded with recognition. A mention in the company newsletter, an email, gift card or any other form of acknowledgement is satisfactory in letting the user know they are doing the right thing. It is imperative that organization leaders recognize staff if they do the right thing, catch a mistake or foil a social engineering attempt. The ultimate result is that the staff member is recognized, other staff recognize what positive behavior is and follow the example and potential insider threats take note and reconsider any negative actions.

About the Author

Daniel “Dan” Jetton is the Vice President of Cyber Services for OBXtek. He is responsible for leading and defining cyber strategy while ensuring security, defense and risk mitigation for his clients.

OBXtek’s accomplished teams have an established reputation for consistently and efficiently achieving goals for its portfolio of federal government customers. Dan Jetton, MBA, MS, MA is a CISSP, CAP and PMP with 20 plus years of military service.

He can be reached online at https://www.linkedin.com/in/danieljetton/ and at the OBXtek website http://www.obxtek.com/.
You can follow him on

Twitter @CyberPhalanx for cybersecurity news.

Malware Basics

And a brief on new Self-updating, Anti-viral Malicious Software
by Joe Guerra, Cybersecurity Instructor, Hallmark University

Malware, which is concise for “malicious software”, is software designed to be utilized or foster the disruption of computer operations, procure sensitive data, or acquire access to confidential information systems. It shows up in the form of source code, short active scripts and tied to other software. Malware is the main nomenclature used to reference the categorical forms of software that are annoying, hostile and intrusive.

In the early days of technology, malware was designed for the sole purpose of experiments or personal pranks. However, today, malware is primarily utilized to steal confidential, sensitive, financial, personal or business data for the gain of criminals-alike. They are sometimes implemented to gather secure information from government or corporate sites to infiltrate and disrupt their overall operation. Nonetheless, malware is often applied in the utilization against the public to garner personal data such as credit card or bank account numbers, social security information, and other related personal identifiable information (PII).

Plainly speaking, malware operates through a threat vector to send a malicious payload that executes an adverse function once it is conjured. Malware comes in a variety of flavors from viruses, Trojan horses, worms, spyware, adware, and the profitable ransomware.

The way a successful malware attack works on computer systems, usually consists of two components. One is the malware created by the attackers to penetrate the computers with the intent to corrupt or damage. The other element is the tandem component in hacking called social engineering, which basically is tricking the user. But let’s focus on the malware component since the programming aspect of creating these code creatures are advancing exponentially.

One in particular is called “Baba Yaga.” It is a new advanced malware that Wordfence security discovered early this year. The name they gave it stems from Slavic folklore for a mythical creature and they believe it was brought into existence by Russian hackers. The key features that make this malware very unique and astonishing are the fact that it is self-updating and has antiviral capabilities. It primarily infects Wordpress, Drupal, Joomla and other generic PHP sites. It is crucial to elucidate the fact that this corrupting software is capable of installing and upgrading Wordpress. That particular part of the code in the malware is in place to ensure that the website is functional. The part that is mind-blowing is its antiviral process. BabaYaga has the capability to check your system for existing files and if malware is detected, it replaces them with clean versions. It does this so that the existing malware will not reveal its presence in the system.

With the advent of this new type of malware that implements an antiviral component, the future of malware analysis is looking more dynamic by the second. Overall, this has thrown down the gauntlet for malware architects to compete amongst each other in designing better-sophisticated code with not just the proliferation aspect, but also the new anti-viral feature.

In Conclusion, the author of the Wordfence security, Brad Haas, put it best by writing “BabaYaga is an emerging threat that is more sophisticated than most malware. It deeply infects a site, spreads to other sites, ensures that the infected site is in good working order and will even remove other malware. It even has the ability to update or reinstall WordPress.”

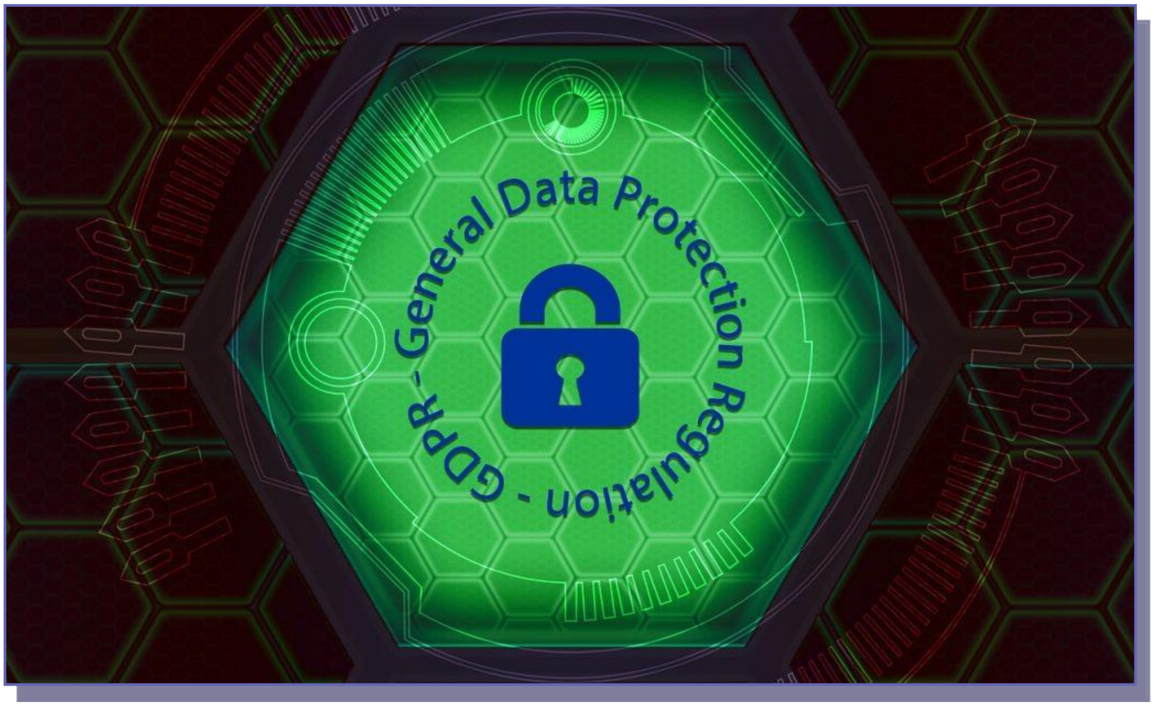
So as mentioned above, this will eventually require the development of new techniques to detect or defend against advanced malware incidents. It is a continual digital arms race as the advancement technology implementations of attackers proceed to evolve in order to stay ahead of cybersecurity analysts.

About the Author

Joe Guerra, Cybersecurity Instructor, Hallmark University Joe Guerra is a cybersecurity/computer programming instructor at Hallmark University. He has 12 years of teaching/training experience in software and information technology development. Joe has been involved in teaching information systems security and secure software development towards industry certifications. Initially, Joe was a software developer working in Java, PHP, and Python projects. Now, he is focused on training the new generation of cyber first responders at Hallmark University. Joe can be reached online at (Jguerra2@hallmarkuniversity.edu) and at our company website http://www.hallmarkuniversity.edu/

Five GDPR Mistakes that Will Put Your Company in Hot Water

by Steve Dickson, CEO, Netwrix



Only 29 percent of small businesses and 41 percent of midsize businesses in Europe have taken steps to prepare for the GDPR, according to IDC, and there's no reason to think that organizations elsewhere in the world are any more ready for the May 2018 deadline.

But panicking can do more harm than good — you're likely to make costly missteps. If your organization isn't prepared, you definitely need to get moving. But be sure to avoid these five common mistakes that can harm your company:

Mistake 1: Rushing the process.

With the GDPR deadline looming and compliance challenges in the headlines every day, it's easy to run mad and make bad decisions. The most absurd example might be British airline Flybe: In their eagerness to prepare for the GDPR, they crafted an email advising users to update their personal information and marketing preferences, and sent it their entire customer base — including people who had unsubscribed from the company's emails. That rash action violated an existing law, the Privacy and Electronic Communication Regulations (PECR), and got the company slapped with a £70,000 fine.

If you're unsure about how to meet the requirements of the GDPR, don't do anything in haste. Seek council from legal advisors and other experienced consultants before taking action. And keep in mind all the compliance standards you are subject to, so you don't violate one as you try to comply with another.

Mistake 2: Taking a fragmented approach to security

GDPR compliance requires a comprehensive approach to security that involves not just technology, but also governance, processes and people. However, a recent Forrester report found that many organizations are focusing too heavily on IT measures and taking a piecemeal approach instead of thinking holistically.

This strategy isn't an effective way to protect your organization from security incidents and audit penalties. I urge you to see the new GDPR legislation as an opportunity to get back to the basics that will improve cybersecurity across your IT infrastructure. In particular, make sure you know where your sensitive data resides, who has access to it, and which services and software are the most critical for your business.

Mistake 3: Being reactive rather than proactive

The GDPR requires a proactive approach from your IT department, which is notoriously hard to put into practice. During a recent presentation for IT security professionals, I did an informal survey about how proactive they consider themselves to be. It turned out that 80% of them are reactive to new compliance requirements and lack a long-term strategic approach.

If your IT department is overwhelmed by routine troubleshooting, it won't be able to prevent data breaches, respond promptly to requests to be forgotten, or comply with other GDPR requirements. Try to figure out the root of the problem: Is your department understaffed or lacking the expertise you need? Are your security systems insufficient or poorly managed? Are employees unaware of proper security protocols? Then take action based on your findings, so you can free up your team to be more proactive.

Mistake 4: Putting responsibility on IT only

Compliance failures are not always the fault of IT. The Netwrix IT Risk Report found that 65% of organizations have experienced security incidents, and most were due to human errors and malware. You don't want to get fined because someone copied a file with customer's ID to his laptop or clicked on a malicious link that delivered ransomware, so make sure all employees who deal with sensitive data (such as your marketing, sales, accounting and legal teams) are trained on your cybersecurity policies and procedures. Make sure your educational efforts go beyond boring lectures about security — include relevant case studies and edutainment programs. More broadly, work to establish a new business culture that puts security and personal data privacy at its center.

Mistake 5: Being too radical

Richard Stallman, president of the Free Software Foundation, has suggested that, instead of protecting and regulating personal data, we should ban its collection. I personally know of companies that have deleted all customer data that could be considered sensitive to try to eliminate the risk of GDPR fines.

These responses aren't just radical; they're also ineffective. Getting rid of your customer database won't erase your obligation to report to auditors; it will just hurt your ability to be competitive. Auditors will be looking for a credible plan to ensure compliance, so make sure you can demonstrate them you are on the right path to better control your security. As for your customers, respecting their privacy and preferences will increase their loyalty; ditching the information you have about them makes it impossible for you to do that, and customers will look for someone else who can.

For too long, businesses have been collecting personal data from customers to meet their own revenue goals. Now it's time to recognize their rights and make the tenets of the GDPR into your core values. The scope of this change might seem daunting, especially with the deadline for compliance fast approaching, but your customers will reward you with stronger loyalty. Plus, if you address GDPR compliance as a strategic business challenge, you'll be in good shape when the next piece of compliance legislation comes around; you'll have a simple reporting issue, not a fundamental engineering task, on your hands.

About the Author

Steve Dickson was named Netwrix CEO in April, 2018 after joining the Netwrix board of directors in August 2017. Dickson was previously with Dell, Inc., where he served as Vice President and General Manager of the Windows Platform Management business, as well as VP of Marketing for the Systems Infrastructure Management Group. Prior to Dell's acquisition of Quest Software, Steve held leadership positions including SVP of the Windows Management business unit and the Identity and Access Management business unit. Other positions he held at Quest include SVP Products and Marketing, VP of Worldwide Sales for Microsoft Management Solutions, and VP of Sales for the Western Region. Before joining Quest Software in 1998, he worked for Air Liquide as a general manager. Steve holds a bachelor's degree in applied mathematics from Weber State University and a master's degree in business administration from Pepperdine University in Southern California.Steve can be reached online at Steve.Dickson@netwrix.com and at www.netwrix.com

How Do We Get Privacy?

Revisiting the Basics and Importance of Cryptography

By Joe Guerra, Cybersecurity Instructor, Hallmark University

Since the onset of technology in society, it has broken the levees of data and has eroded our personal privacy. In this digital age, the procurement and access to our personal data may be utilized and manipulated in a quiet manner to control our behavior. With this in mind, let us peruse through the concepts of Privacy, Encryption and Cryptography.

In the field, one of the most intriguing and disheartening things about cryptography is how minute amount of cryptography we actually mess with. So, let us quickly review what privacy technically is and what today’s technology has done to increase the vulnerabilities it has bestowed on it.

Privacy, what is it all about in Technology?

Privacy is a condition of being liberated from the public eye to the extent that you choose it to be. Today, information is gathered and organized on almost every action and transactions that you initiate, perform, or involved in. From web searching, buying, doing those online surveys, communicating through social media platforms, etc. All these actions leave a digital exhaust that you left behind. Data bots and analysts then aggregate this. This supposedly private data has associated risks. The risks are either inconveniences, grouping or being profiled. Your data is used for marketing or sold to identity impersonators, which is a theft or inconvenience. Your data is then associated with groups of similar background, interests and tendencies. Alternatively, your data is deeply analyzed through statistical algorithms and informationally profiled and grouped. A more in-depth way of profiling you.

However, there are measures of protection that may be administered to alleviate the risks associated with private information. Organizations should follow the law and establish policies to take responsibility. People and companies should follow best practices. Then we have the implementation of cryptography through the process of encryption.

What exactly is Encryption and Cryptography?

Encryption is the scrambling of information so that it cannot be read and only people with a certain key can access it. Encrypted data is what has been translated from plaintext to cipher text. In getting it to work backwards, we decrypt the message by changing the scrambled message back to the original text.The terms encryption and decryption are what sum up the process of the broader term called Cryptography. The primary purpose of Cryptography is to secure digital information confidentially, as it is stored on systems at rest and as well as transported through the web or other interconnected networks. In our day and age, Cryptography is the most effective and favored information security approach administered by managements. Cryptography can accommodate and administer to several necessities when it comes to information systems security. Through confidentiality, it ensures those who have been authorized by having been given the key can only see encrypted data. Integrity is ensured, as the data cannot be modified with the exception of the authorized accounts who have access to the key. Through availability, only privileged users are given the decrypting key to get the data. Lastly, the concept of nonrepudiation is also a trait it can push through as it prevents individuals from denying they were involved.

While Cryptography may seem like a treacherous, daunting and complicated task, it is an essential in computer security. However, it is a form of art with dashes of arithmetic. Let me see if I can break it down for you to comfortably digest. Now, Encryption at its core is a conglomerate of logic called a formula with a key to encode the data. It is an algorithm that utilizes mathematical formulas. The way it works is an encrypted key is composed of a huge number that is then applied to encrypt and decrypt the data. How long the key is dictates how secure the information will be. So, concisely, the more elongated the key is the better the data will end up secure. The majority of encryption algorithms used have a length between 40-128 bit or more. This is great since most internet browsers do support this key length range.

Symmetric or Asymmetric?

There exist two main categories in data encryption symmetric encryption and asymmetric encryption also referred to as public key encryption.

Symmetric encryption, also referred to as single-key encryption, is the process of using only one key to decrypt and encrypt your information. Both parties, the sender and receiver use the same exact key. The most comprehensively used standard for this encryption process is Data Encryption Standard (DES). This method is broken up into 64-bit blocks and then transferred. It is then manipulated in the process of 16 encryption steps implementing a 56-bit key. It then becomes scrambled by a substitution algorithm and finally transposed for one last time. That was then, but this is now and DES has been replaced with Advanced Encryption Standard (AES), which was officially chose by the U.S. government as the replacement and has become the most popular symmetric key algorithm. Nonetheless, there is a major dilemma with symmetric key process. How do you transfer the key? The correct answer is, hopefully guessed it, public key encryption. That major issue of distributing the keys in symmetric encryption is why public key encryption is preferred. Since, the mere loss or leak of the symmetric key will lead to a significant problem of giving someone else the opportunity to decrypt secure messages.

Public key encryption, which is technically asymmetric key encryption, is the opposite of the single key method. You have two keys, one public used to encrypt and the other one is private and is used to decrypt. So only, the individual holding the private key is able to decrypt the messages. Mathematically, asymmetric relies on large prime numbers and number theory. This is the most widely known and used public key infrastructure.

The Key Roles in Asymmetric key cryptography

Public key encryption enables you to transfer and convey through any open channel with a great degree of assurance and allows you to trust the process in various ways:

- Authentication- Messages sent to you will be from the appropriate source
- Integrity- Messages will arrive unmodified
- Privacy- Messages will only be able to be read by the intended target.

Given this, we know that the scheme of cryptography is a necessity for computer systems to implement the security and privacy that users' desire. The power of this process rests in the size and means applied for the protection of the cryptographic keys.

In conclusion, Cryptography provides a range of security defenses. It can support the protection of Confidentiality, Integrity, Authentication, and Non-repudiation. It is the practice of transforming plain text data to an obfuscated text that cannot be revealed by unauthorized entities. It hides data, which is why it is called Cryptography, a word that from its Greek roots means "hidden writing."

About the Author

Joe Guerra, Cybersecurity Instructor, Hallmark University Joe Guerra is a cybersecurity/computer programming instructor at Hallmark University. He has 12 years of teaching/training experience in software and information technology development. Joe has been involved in teaching information systems security and secure software development towards industry certifications. Initially, Joe was a software developer working in Java, PHP, and Python projects. Now, he is focused on training the new generation of cyber first responders at Hallmark University. Joe can be reached online at (Jguerra2@hallmarkuniversity.edu) and at our company website http://www.hallmarkuniversity.edu/

Role of Identity and Access Management (IAM) in Cyber Security

by Bhavdip Rathod, IAM Solution Architect, Sailpoint Technologies, Inc

In today's digitally enabled world, Identity and Access Management (IAM) plays a critical role in any enterprise security plan, as it is inseparably linked to the security and productivity of companies. As more and more business store their sensitive data electronically, ensuring that data remains secure is critical. The rapid transformation to the digital world has cut across all organizations and industries and has required changes to how companies manage their workforce and ultimately how they deliver access to their critical applications and data. The workforce has also developed gradually, especially from a simple to a more complex type of labor force for organizations. In addition to providing access to employees, organizations now also need to include contractors, vendors and partners, each with their own set of access requirements and restrictions. Furthermore, data and applications spread across cloud, on-premises and hybrid infrastructures are being accessed by a variety of devices including tablets, smartphones and laptops. Identity and Access Management is a Cyber/Information security discipline that ensures right people have appropriate access to the organization's critical systems and resources at the right time. IAM assimilate three major pillars:

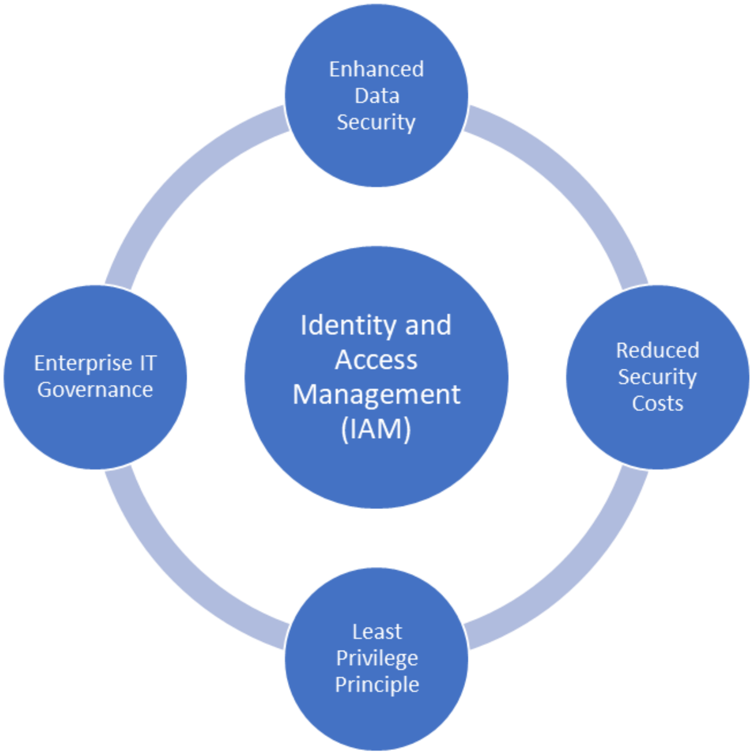
- Identification
- Authentication
- Authorization

When a user tries to access any system or resource, he or she first enters the username as very first step of identity verification into the system. System then goes and verifies user's identity via authentication process. Authentication can be done via basic knowledge-based mechanism such as, passwords or more advanced techniques can be used, such as multi-factor authentication (MFA) or biometrics. Once, system successfully completes authentication process, then IAM system will initiate authorization process to ensure that logged in user is only allowed to perform the tasks which he or she is entitled to do as part of their job function based on the pre-defined security policies in the IAM system (e.g. Developer should not be allowed to have admin rights on production system). The fact that a user proves his or her identity is not enough to gain access.

Effective IAM infrastructure and solutions help enterprises establish secure, productive and efficient access to technology resources across these diverse systems, while delivering several important key benefits:

Enhanced Data Security: Consolidating authentication and authorization capabilities on a single centralized platform provides business and IT professionals with a streamlined and consistent method of managing user access during identity lifecycle within organization. For example, when users leave a company, centralized IAM solution gives IT administrators the ability to revoke their access with the confidence that the revocation will take place immediately across all the business-critical systems and resources which are integrated with centralized IAM solution within the company. This will ensure no lingering access stays with the terminated users and hence significantly improves the overall Information Security posture of the company.

Reduced Security Costs: Having a centralized IAM platform in an organization to manage all users and their access allows IT to perform their work more efficiently. In today's world, each employee has access to thousands of systems and resources as part of their job. Imagine, if an IT administrator has to grant access to each of these systems manually when employee joins the company and then again revokes these system accesses manually from each system when user leaves the organization, it will be a nightmare for IT staff and also a huge monetary overhead for the company to maintain these on-boarding and off-boarding processes. Efficient centralized IAM solution can address this challenge diligently which results in huge savings of time and money for the company. A comprehensive IAM solution can reduce overall IT costs by automating identity processes that consume IT resources, such as onboarding, password resets and access requests, eliminating the need for help desk tickets or calls



Least Privilege Principle: Least privilege is an important practice of computer and information security for limiting access privileges for users to the bare minimum rights they need to perform their job duties. With 77% of data breaches involving an insider, it is necessary to ensure access to all your corporate resources are secured and granted using least privilege principle. In a company, it is common for employees to move across different roles in the organization. If the granted privileges are not revoked as the employee change the role, those privileges can accumulate, and this situation poses great risk for many reasons. It makes that user an easier target for cyber hackers as his/her excessive rights can be an easier gateway for criminals to access the broader part of the company's critical systems and resources. Or this can eventually turn into the insider threat where person gets the ability to commit data theft. Sometimes companies forget to remove these excessive privileges from user's profile when he/she leaves the company resulting in security risk where user can still access the company's systems freely even after the termination. A well-designed centralized IAM solution can help organizations eliminate insider threat challenge by utilizing Least Privilege Principle to a great extent.

Enterprise IT Governance: Taking compliance regulations around the world such as the HIPPA, SOX, upcoming EU GDPR (General Data Protection Regulation) into account, a lack of effective identity and access management poses high risks to compliance. On March 1, 2017, the state of New York's Department of Financial Services (NYDFS) new cybersecurity regulations went into effect. The regulations prescribe many requirements for the security operations of financial services companies that operate in New York, including the need to monitor the activities of authorized users and maintain audit logs, something identity and access management systems typically do. Modern IAM solutions and products provide the ability to enforce user access policies, such as separation-of-duty (SoD), and establish consistent governance controls, eliminating access violations or over-entitled users through automated governance controls. This will ensure companies stay compliant with business and government compliance and regulation standards. Not adhering to these standards could cause companies millions of dollars in penalties.

World has witnessed an alarming trend in security data breaches (e.g. Yahoo, Equifax, Linkedin, Target, etc.) every year which are both larger in scope and increasingly devastating. Businesses must be able to guard themselves from these cyber threats within the company and from the unknown exposure points of internet. Identity and access management provides a critical security layer against these unknown security vulnerabilities to protect companies from cyber security data breaches. A robust IAM infrastructure can ensure consistent and standard access rules and policies across an organization by providing an important additional layer of protection.

All of these reasons prove relevance of Identity and Access Management (IAM) for business success and productivity and why should embrace for comprehensive IAM processes and infrastructure.

About the Author

Bhavdip Rathod is an Identity and Access Management Solution Architect at Sailpoint Technologies, Inc. Bhavdip is an experienced cyber security technologist and architect through combined experience in Identity and Access Management. He is primarily responsible for providing innovative solutions to the companies in the field for their most complex challenges in the IAM and Cyber Security areas to strengthen their security infrastructure and prevent potential cyber and data breaches.

He has strong understanding and in-depth experience of Identity and Access Management (IAM) Frameworks and industry best practices. Bhavdip has served as an SME and Expert Advisor on the largest and most complex IAM Implementations for various retail, financial, healthcare and manufacturing organizations in last 10 years.

Bhavdip serves an IAM Expert Advisor and speaker at various IAM user groups and conference events.Bhavdip holds a Master of Science degree with Commendation from University of Hertfordshire in UK."

Spear-phishing Is The Next Threat After A Data Breach

Employees' awareness must be a mandatory routine.

by Pedro Tavares, CSIRT.UBI and seguranca-informatica.pt Founder

During the last years, we have observed a tremendous number of data breaches that have made headlines. Opening the online newspaper and reading news about a data breach has almost become a habit as they occur anywhere and at any time. In fact, the Internet has become a giant channel for data transactions, and all of this because anything is now online — our life, our digital identity, basically our digital footprint.

Today, digital information is seen as the “new petroleum” and organizations must apply the best security practices to keep save data from cyber attacks and possible data leaks.

2018 Data Breaches

If we look at the recent past, we easily realize that data breaches are indeed one of the biggest problems in this information era. Besides, they can usually trigger other threats such as attacks based on social engineering.

Just looking at the current year, we can easily list devastating situations. Maintaining an updated list of data breaches is a very hard task as the number of threats are growing exponentially. For this reason, organizations have to improve their security strategies by training their employees in order to provide an improved reaction when events of this nature occur.

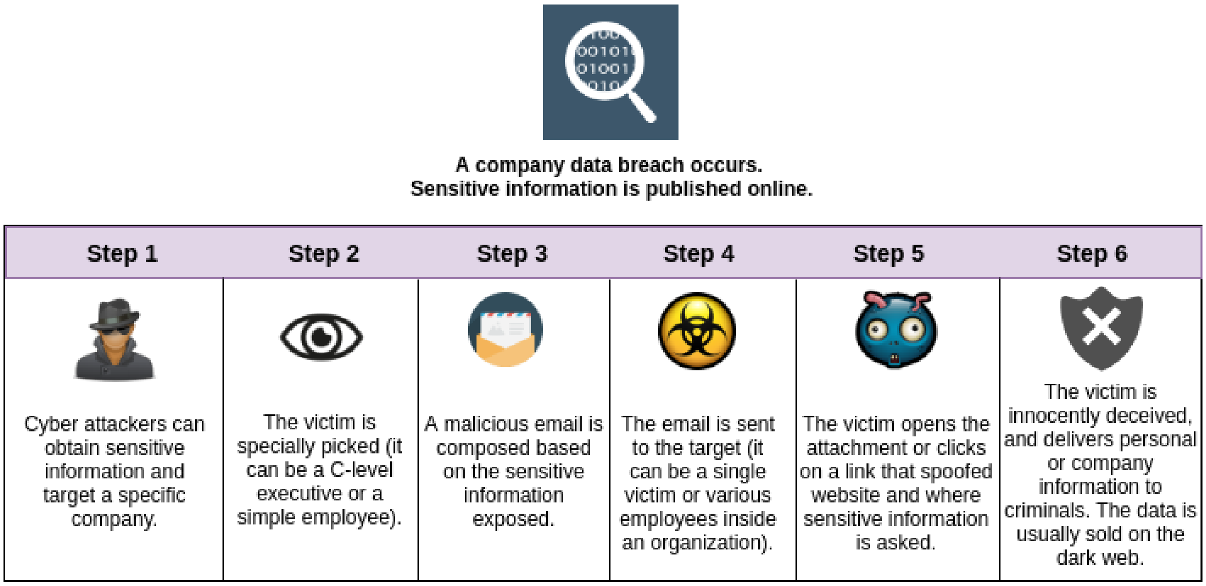
Data breaches must be detected early on inside the organization. This is mandatory since a leak typically represents a valuable point of attack from the cyber attacker perspective.

How cyber attackers can use data breaches to their own profit

After a data breach, an immense quantity of data is leaked and exposed online (often personal and professional information). Due to this, spear-phishing attacks are highly targeted and customized and are far more likely to succeed than traditional phishing attacks. This way, crooks can use all the exposed information to produce huge phishing campaigns strictly targeting an organization.

In general, spear-phishing represents a targeted email scam for the sole purpose of gaining unauthorized access to sensitive data. Unlike phishing scams, which perform wide and scattered attacks, spear-phishing focuses only on a specific group (a restrict target). Crooks typically use data exposed by a data breach to obtain more information about the victim and organization. In order to increase the success rate these kind of attacks, the messages often contain urgent explanations on why they need sensitive information. At this time, victims are coaxed to open a malicious attachment or click on a link that takes them to a spoofed website where they are asked to provide sensitive information, such as passwords, account numbers, credit card numbers, access codes and personal information numbers (PINs).

Figure 1 below presents how that type of attacks can be performed by crooks



A company data breach occurs.
Sensitive information is published online.

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Cyber attackers can obtain sensitive information and target a specific company.	The victim is specially picked (it can be a C-level executive or a simple employee).	A malicious email is composed based on the sensitive information exposed.	The email is sent to the target (it can be a single victim or various employees inside an organization).	The victim opens the attachment or clicks on a link that spoofed website and where sensitive information is asked.	The victim is innocently deceived, and delivers personal or company information to criminals. The data is usually sold on the dark web.

Figure 1: General workflow of a spear-phishing attack.

How to avoid spear-phishing attacks

If you think you were infected through a spear-phishing attack, the rule of thumb is very simple: do not panic over it! Only opening an email that can be represented by a scam campaign will not affected your computer.

There are some measures that you need know to avoid spear-phishing attacks and also to detect them saving thus all organization against this plague.

- □ If you think that you have indeed been a victim of a phishing attack, then immediately disconnect the computer from the network.
- □ Do not make it easy, talk to your colleagues about it. Flag the email as phishing and communicate the potential phishing scam to your organization's IT team. They will address you towards the next steps.
- □ Be proactive! You can perform a phishing/malware scan in your computer (especially when you open an attachment).

- □ Change your passwords. This must be adopted as a monthly task. Use and encourage your colleagues to follow a cyber-hygiene routine in order to protect their personal information away from crooks.
- □ Try to understand what the source of the malicious email is. Check whether your information was exposed by a data breach online and communicate that.
- □ And finally, use logic. Every time that you open an email from a “friend” asking for personal information (including passwords, or other sensitive data), you should carefully check if the email address is legitimate. Use an old strategy: personally talk to your friend.

Conclusion

Traditional security often fails to prevent spear-phishing attacks, as they are expertly customized. The error of an employee can have serious consequences for organizations and sensitive information can be exposed when the appropriate measures are not adopted at the right moment.

Fraudulent campaigns are performed by crooks typically when a data breach occurs. Organizations need to be prepared to fight this threat face to face, eyes to eyes. That is why data breaches must be always detected as early as possible in order to inform and aware organization's employees against potential spear-phishing attacks in the wild.

About the Author

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

Segurança Informática

blog:	www.seguranca-informatica.pt
LinkedIn:	https://www.linkedin.com/in/sirpedrotavares
Contact me:	ptavares@seguranca-informatica.pt

Where do I “Sign”?

A short Review on Digital Signatures

by Joe Guerra, Cybersecurity Instructor, Hallmark University

The fundamentals of data security is defined as applying techniques, procedures and other means to protect the confidentiality, availability and integrity of information. Most of the time the focused scenario is keeping the attackers at a distance, and adding barriers around the information. These barriers vary from physical property fences to technology firewalls to do the job.

Whereas these defenses are essential, what about applying an additional factor that would make the information fruitless to the attacker? What if the data was gibberish in such a way that only the authorized entities can view it while the infiltrators could not? This is the kind of security that cryptography offers: it hides the information in a manner that would leave no opportunity for the threat to read it.

Cryptography offers a range and level of security. It provides the basic protections of confidentiality, integrity, authentication and non-repudiation. The latter two are in a relational category that has been an issue since the dawn of humanity. Some kind of authentication procedure has been in place in civilization since the advent of writing. Although, markings, hand written signatures or seals were sufficient in those ages, in the now, a more relevant process is necessary for an accelerated global interconnected society. As online transactions exponentially rise daily, there is an escalated demand to ensure authenticity, integrity, and non-repudiation of the entities involved, the asset and information exchanged between the parties, and a comprehensive secure provisioned agreement process.

So, how do we provide for this need of authentication, integrity and non-repudiation in today’s digital civilization. The answer lies in a cryptographic component called Digital Signatures. First of all, digital signatures should not be confused with digitized signatures which is essentially an electronic variation of your actual physical signature. Relatively, digital signatures do adhere to the identity of a party to specific information or piece of data. This cryptographic feature is not for the confidentiality aspect of security. Although, it does establish the integrity of the message and authenticate the sender of the data. Digital signatures come from the public key cryptography concept, which is also referred to as asymmetric cryptography. This cryptography provides better authenticity than its counter-part symmetric cryptography.

What makes symmetric encryption inferior in the authenticity and integrity spectrum? If an individual sends information to a co-worker, the message is encrypted with his secret key and the co-worker, in order to view the message must have the same key for decryption. Now, if the same user wants to send another encrypted message to another individual, another key must be implemented. So, if you factor in copious amounts of colleagues into the equation, the problem lies in keeping track of the keys applied to who. An additional issue is how does the receiver get the copy of the key. E-mailing is not a secure option. In other words, symmetric cryptography does not provide authentication or even non-repudiation

Symmetric cryptography works with the use of the same key to encrypt and decrypt content. This is only powerful against attacks if you securely store away the key.

Asymmetric cryptography implements two keys as opposed to one. The keys are mathematically conjoined and are titled the public and private key. You make public key transparently known and the private key secure. Here is how asymmetric cryptography operates.

Suppose Joe wants to relay a message to Jane. Jane has her private key, and keeps it safe, and her public key, which is known to everyone. Joe utilizes Jane’s public key for encrypting a message, Joe then transmits the message, Jane now can only decrypt it with her secure private key. Because she does have sole access to her private key, she goes about to decrypt and view the message. Now, if Jane wanted to respond to Joe, she will need to encrypt her message with Joe’s public key which is also known to everyone and send it. Joe will then have to use his private key to read the response. Appropriately, you can understand the value of asymmetric encryption in using it for digital signing.

Suppose Joe wants to relay a message to Jane. Jane has her private key, and keeps it safe, and her public key, which is known to everyone. Joe utilizes Jane’s public key for encrypting a message, Joe then transmits the message, Jane now can only decrypt it with her secure private key. Because she does have sole access to her private key, she goes about to decrypt and view the message. Now, if Jane wanted to respond to Joe, she will need to encrypt her message with Joe’s public key which is also known to everyone and send it. Joe will then have to use his private key to read the response. Appropriately, you can understand the value of asymmetric encryption in using it for digital signing.

Digital signatures are implemented as an industry standard within the whole framework called Public Key Infrastructure (PKI). PKI lays out the factors and limitations for public and private keys correlated with a digital signature. As stated in the scenario above, the private key is the responsibility of the sender, and does not in any way share it. The public keys may be free to share and used by anyone, especially to validate the signature of the sender.

Overall, digital signatures have two respective intentions: ensure that the original information was not modified and verify the message does come from the sender. For this to be a success, a two-step cryptographic process takes place. First, the message is hashed, thus creating a digest that is tied to the message. So, if the message is modified, the digest changes and leaves full indication of tampering, which will violate the integrity principle. Then second, is being able to decrypt the digital signature’s hash encryption with the sender’s public key, thus validating the authenticity of the sender. The person says who he says he is.

In conclusion, while Digital Signatures are quite an effective and efficient practice in eliminating impersonation and data manipulation, they are only as good as long as the organization or individual keeps the private key secure. For as soon as the private key becomes public the digital signature tied to that private key can be maliciously used. With this in mind and with the tremendous amount of trust we have in place for digital signatures and the delicate tasks that we attach to them, the more vulnerable they are becoming and the more damaging they can become.

About the Author

Joe Guerra, Cybersecurity Instructor, Hallmark University Joe Guerra is a cybersecurity/computer programming instructor at Hallmark University. He has 12 years of teaching/training experience in software and information technology development. Joe has been involved in teaching information systems security and secure software development towards industry certifications. Initially, Joe was a software developer working in Java, PHP, and Python projects. Now, he is focused on training the new generation of cyber first responders at Hallmark University. Joe can be reached online at (Jguerra2@hallmarkuniversity.edu) and at our company website http://www.hallmarkuniversity.edu/

EVENTS

UBC

RansomProtect Summit

Combating Malware and Advanced Persistent Threats

Singapore
8th – 9th November

Dubai
14th – 15th November

Registrations are now open

This Summit is at the forefront of the discussion to prevent Ransomware attacks and prevent organizations from the nightmare that follows. 2017 was the year Ransomware threats became bigger than ever. It has easily become one of the worst nightmares for a CISO and InfoSec professionals across the world.

Join us as we bring together leading experts, industry champions and Technology leaders at this 2 day Summit to share best practices, strategies, frameworks and technology to combat malware and advanced persistent threats against your organization.

Limited seats. Register today.

WWW.RANSOMPROTECTSUMMIT.COM

events@ubcompliance.com

3rd Asia Cyber Risk Summit

Theme: "To Be Cyber Resilient in a World of Evolving Cyber Threats"

17-18 September 2018, Mandarin Orchard Hotel, Singapore

**REGISTER NOW!
EARLY BIRD ENDS
17 AUGUST 2018**

SPEAKERS

Daniel Hofmann
Senior Advisor,
Financial Stability and Insurance Economics,
The Geneva Association

Joel Pridmore
Head of Financial Lines & Business Development, Asia,
Munich Re Syndicate

Faisal Yahya
Head of IT,
PT IBS Insurance Broking Service, Indonesia

Nicolas Michellod
Senior Analyst,
Celent Switzerland

Zao Wu
Analyst,
Celent Hong Kong

Abdallah Zabian
General Manager for Security,
Asia, DXC Technology

Ian Pollard
Managing Director,
Delta Insurance New Zealand

Tan Shong Ye
Digital Trust Leader,
PwC Singapore

Vineet Jaiswal
Head of Bancassurance,
National Bank of Oman

Sasikumar Adidamu
Chief Technical Officer,
Bajaj Allianz General Insurance Company

Jim Fitzsimmons
Director of Cyber,
Control Risks Group

Pankaj Khushani
Head of Analytics & Platform,
Partnerships, SEA, Google

Thomas Herde
Managing Director, Head Casualty Specialty Practice,
Asia Pacific, Guy Carpenter

Rob Phillips
Director, Digital Forensics, Cyber and e-Discovery Computer Forensics & Electronic Discovery, RP Digital Security

Mark Camillo
Head of Cyber,
EMEA,
AIG

Andrew Cook
Senior Associate,
Kennedys Legal Solutions

Ronak Shah
Regional Head of Financial and Professional Lines,
QBE Asia Pacific Operations (APO)

Wolfram Hedrich
Executive Director,
MMC's Asia Pacific Risk Center

REGISTER ONLINE: www.asiainsurancereview.com/AIRcyber

FOR SPEAKING/SPONSORSHIP/PARTNERSHIP OPPORTUNITIES: ✉ may@asiainsurancereview.com | ☎ +65 6372 3185

@AIReDaily #AIRcyber /company/asia-insurance-review /AsiaInsuranceReview

Organised by
ASIA INSURANCE REVIEW

Supported by
AiSP Association of Information Security Professionals
asia cloud computing association
CELENT
Life Insurance Association Singapore LIFE IS WORTH PROTECTING. INVEST IN IT.
RIMS the risk management society
IIS INTERNATIONAL INSURANCE SOCIETY

Media Partners
CDM CYBER DEFENSE MAGAZINE
GII Global Information
MIDDLE EAST INSURANCE REVIEW

GLOBALPLATFORM®

THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

6th ANNUAL SEMINAR

Security in Our Connected World

19 September 2018

+ TECHNICAL WORKSHOP

GlobalPlatform Technologies

20 September 2018

Sheraton Grand Beijing Dongcheng Hotel | Beijing, China

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES
20 YEARS

For more information & to register:
https://globalplatform.org/seminar/annual-seminar/

The seminar will focus heavily on the Internet of Things (IoT), as well as examine security technologies including the Trusted Execution Environment (TEE) and Secure Element (SE). It will also delve into these technologies' business and technical use cases, to explore the need for security in our connected world.

Topics covered at the event will include IoT (consumer, industrial and enterprise), identification and authentication, payment and value-added services, premium content protection, device trust and certification.

Speaker agenda includes individuals from Alibaba, Baidu, Brightsight, CAICT, China Unicom, Gemalto, Huawei, Infineon, Oracle, STMicroelectronics, Tencent and Trustonic.

The technical workshop – for system architects, engineers, application developers and technical product/project managers – will provide insights into key GlobalPlatform technologies and an opportunity to interact with

Last year's event, hosted in Beijing, China, was our largest seminar to date, with over 200 delegates, from 85 companies representing 13 different countries.

GAME ON

The Midwest's most impactful week of IT Security!

THE SUMMIT

OCTOBER 22-26

CLEVELAND, OH

energytech
lighting the way to a brighter future

INFORMATION SECURITY SUMMIT
Building Community Through Education

GREGORY RICHARDSON
CTO Ambassador
"Security in a world of adversarial machines"

Ohio Turnpike
RANDY COLE
"Leading From the Edge"

Author
RICHARD GUIDA
"What is Security and Privacy in today's Business Environment"

Amazon #1 Author
RENEE SMALL
"Closing the Security Talent Gap"

Swim CTO
SIMON CROSBY PhD
"Toward Computing Infrastructure You Can Trust"

STEPHEN L. GRIMES
FACCE FHIMSS FAIMBE
""How the Lack of Medical Device Security Will Harm Patients".

Plus scheduled insights from David Kennedy - Founder/CEO, TrustedSec, Deral Heiland - IoT Research Lead, Rapid7, Laurence Pitt - Director, Security Strategy, Juniper Networks, John O'Leary - President of O'Leary Management Education, John DiMaria - Product Champion for Information Security/Business Continuity, BSI Group, John O'Mara - Media Crisis Communications

Earn CPEs

Presented by

Check Point SOFTWARE TECHNOLOGIES LTD

Hurricane Labs

MCPc

ASMGi

www.informationsecuritysummit.org/events/summit-2018/

Large Group? Contact us at **cso@informationsecuritysummit.org**

Each Admission Pass Includes Complimentary Parking, Continental Breakfast, Access to All Sessions, Wi-Fi, Midday Refreshments and Xceptional Networking Happy Hour

SICW
Singapore International
Cyber Week

Cyber Security Agency of Singapore
proudly presents

SINGAPORE INTERNATIONAL CYBER WEEK

FORGING A TRUSTED AND OPEN CYBERSPACE

Singapore International Cyber Week 2018 is the region's most established cybersecurity event – the ideal platform to discuss, network, strategise and form partnerships, with an emphasis on international and regional cooperation, cyber ecosystem development, and ever-evolving innovation in strengthening cybersecurity as a foundation for the digital economy.

GovernmentWare (GovWare) is the cornerstone conference for SICW, featuring the latest trends in technology, organisational implementation and user perspectives, with a speaker faculty of over 100 government officials, thought leaders, visionaries, technology experts and industry professionals, and over 100 exhibitors and sponsors.

DATE

18 - 20 Sept 2018

VENUE

Suntec Singapore
Convention and
Exhibition Centre

WWW.SICW.SG

ORGANIZED BY
CSA SINGAPORE

EVENT PARTNER
image engine

www.cybersecuritysummit.co.uk

CYBER SECURITY SUMMIT&EXPO

15 NOVEMBER 2018 // BUSINESS DESIGN CENTRE, LONDON

CO-LOCATED WITH:

DATA PROTECTION SUMMIT 2018

By exhibiting at the Cyber Security Summit & Expo you are associating yourself with the UK's largest one day event dedicated to cross-sector learning for cyber preparedness across government, the public sector, critical national infrastructure and industry. The show is an unmissable opportunity to showcase your solution and provides an excellent platform to position your organisation in front of your customers.

6 stages
of content

2,000
attendees

New
expo features

Supporters & Contributors

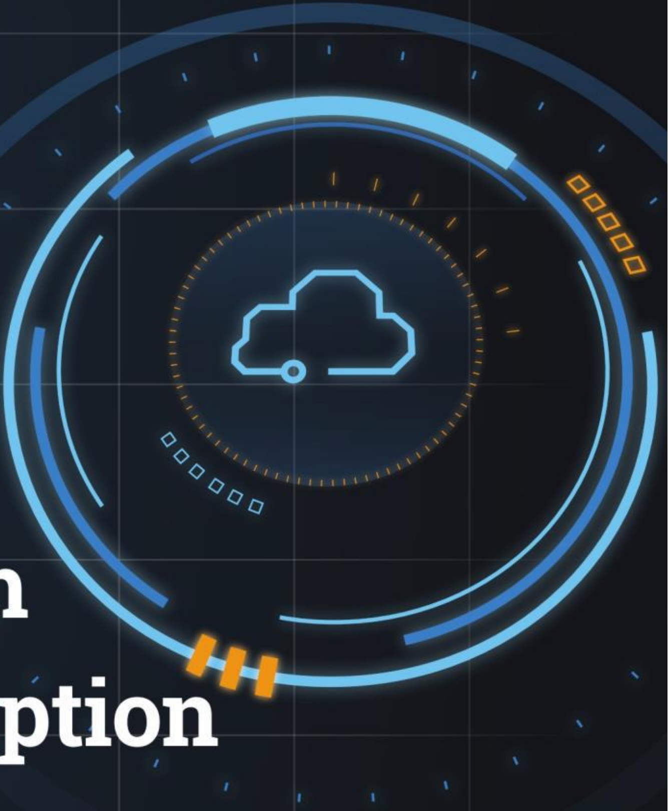
CREST. glg global legal group iisp irms techUK

Enquiries:
Jamie Hushon-Brown,
Senior Sales & Key Accounts

Tel: 0161 200 8697
E: Jamie.Hushon-Brown@govnet.co.uk

MIS|TI™ AND CSA PRESENT

CLOUD SECURITY ALLIANCE CONGRESS 2018



Navigating Through This World of Disruption

Technology and the regulatory landscape are changing rapidly. How can you as a security professional prepare yourself for tomorrow's problems? How do you evolve?

The Cloud Security Alliance and MIS Training Institute have partnered to host the **2018 Cloud Security Alliance Congress** on **December 10-12** at the **Omni Orlando Resort** in **ChampionsGate, Florida**. This year's event welcomes world leading security experts and cloud providers to discuss global governance, the latest trends in technology, the threat landscape, security innovations, best practices and global governance in order to help organizations address the new frontiers in cloud security.

As a valued Cyber Defense Magazine subscriber, you **SAVE 10%** when you use discount code **CSA18-CDM** at checkout!

CSACONGRESS.MISTI.COM

December 10-12, 2018 | Omni Orlando Resort at ChampionsGate | ChampionsGate, FL

MIS|TI™
TRAINING INSTITUTE

CSA cloud security alliance℠

International Conference on

INFORMATION SYSTEMS SECURITY AND BLOCKCHAIN

November 05-06, 2018 | Las Vegas, USA

Theme: Identifying and Combating Cyber Attacks

Sessions:

- Security and Privacy in Cloud
- AI based security
- Blockchain
- Cryptographic Security
- Syntactic attacks and firewalls
- IoT security
- Network Security & Management
- Hacking
- Vulnerabilities
- Mobile Systems Security

Email: cybersecurity@annualmeetings.net | **Web:** http://www.meetingsint.com/conferences/cybersecurity

DIGITAL
TRANSFORMATION SUMMIT

the 2nd Annual Edition

17-18 September 2018
Abu Dhabi, UAE

Leveraging Emerging Technologies And Building New Delivery Models To Unleashing Digital Potential In Business Operations And Service Delivery

Hear From C-Level Decision Makers From 7 Industries Including:

Major Mohammad Obaid Al Obaidly, Deputy Director Digital Transformation & Systems Development, **Abu Dhabi Police GHQ**

Umar Saleem, Chief Transformation Officer, **Al Jaber Group**

Graham Colclough, Partner, **UrbanDNA UK**

Anshul Srivastav, Chief Information Officer & Digital Officer, **Union Insurance**

Delel Chaabouni, CIO - Middle East & Africa, **PepsiCo**

Sherif Gomaa, Chief Executive Officer, **Obeikan Printing & Packaging – Obeikan Investment Group**

SPECIAL OFFER FOR CDM CYBER DEFENSE MAGAZINE THE PREMIER SOURCE FOR IT SECURITY INFORMATION READERS

QUOTE DTSM18 AND GET 10% DISCOUNT!

www.digitaltransformationuae.com

Advanced Conferences and Meetings FZ-LLC | T: +971 4 563 1555 I F: +971 4 422 7548 I E: opportunities@acm-events.com

Hardware Security Conference & Training 2018

Training 11-12 September
Conference 13-14 September

NH Hotel Den Haag, the Netherlands

Hands-on Security Trainings by renowned hardware experts:

- Low-Level Hardware Reversing by Javier-Vazquez Vidal & Ferdinand
- IC Reversing 101 by Olivier Thomas
- Practical Car Hacking by Guillaume Heilles & Emma Benoit
- Side-Channel Attacks 101 by Lejla Batina & Kostas Papagiannopoulos
- ICS Security by Marko Schuba & Nico Jansen

Early Bird Prices till 30th June!

ABU DHABI

GLOBAL ROAD & TRAFFIC SAFETY

Under the patronage of:

دائـرة الـتـخـطيط العـمراني والبلديات
DEPARTMENT OF URBAN PLANNING AND MUNICIPALITIES
بـلديــة مـديـنـة أبـوظـبـي
ABU DHABI CITY MUNICIPALITY

24 - 25 SEPTEMBER 2018 | Abu Dhabi, UAE

CREATING AWARENESS AND DELIVERING INNOVATION IN ROAD AND TRAFFIC SAFETY

AN EXCELLENT AGENDA PUT TOGETHER WITH A STELLAR LINE-UP OF SPEAKERS

Eng. Saleh Aljabri, Head of Traffic Services Section, **Abu Dhabi City Municipality**

Eng. Mohammed Faisal Al Hashmi, Senior Engineer - Traffic Safety, **Abu Dhabi City Municipality**

Stephen Lambert, Road Engineer, **Abu Dhabi Municipality**

Susanna Zammataro, Executive Director, **International Road Federation – Geneva**

Thomas Edelmann, Founder & Managing Director, **Road Safety UAE**

Eng. David Dunn, Lighting Expert, **Abu Dhabi Municipality**

Dr. Britta Lang, Technical Director – Education and Evaluation, **4E Road Safety and Transport Consultants**

David George, Road Safety Specialist, **Al Ain City Municipality**

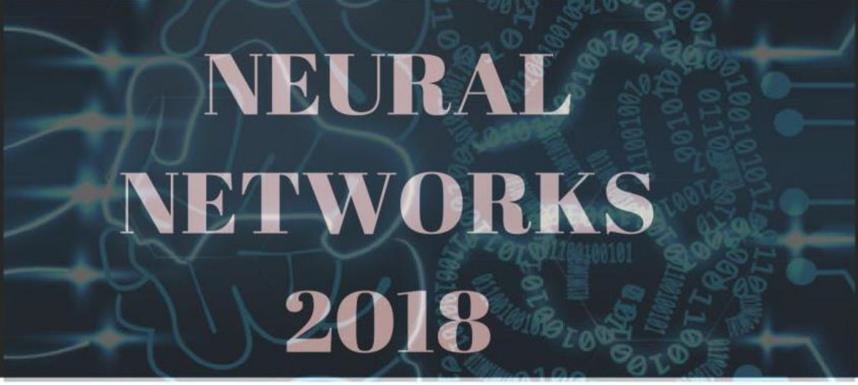
Special offer to CDM CYBER DEFENSE MAGAZINE THE PREMIER SOURCE FOR IT SECURITY INFORMATION readers

QUOTE GRTSM18 AND GET A 10% DISCOUNT

SUPPORTING ORGANISATION	RoadSafetyUAE.com
NETWORKING PARTNERS	Camera Lowering Systems NorthStar Lighting SSAB HARDOX® WEAR PLATE
MEDIA PARTNERS	Railway Gazette International الرؤية arab wheels VL Voices of Leaders UAEBusiness.com

www.roadtrafficsafetyabudhabi.com

Advanced Conferences and Meetings FZ-LLC | T: +971 4 563 15 55 | F: +971 4 422 75 48 | E: opportunities@acm-events.com



NEURAL NETWORKS 2018

☎

+44-2088190774
neuralnetworks@enggconferences.com
artificialintelligencemeet@gmail.com

"Harnessing the power of Artificial Intelligence"

Major Sessions:

- **ARTIFICIAL INTELLIGENCE**
- **BIG DATA**
- **BIOINFORMATICS**
- **AUTONOMOUS ROBOTS**
- **SUPPORT VECTOR MACHINES**
- **COGNITIVE COMPUTING**
- **DEEP LEARNING**
- **ARTIFICIAL NEURAL NETWORKS**
- **CLOUD COMPUTING**
- **NATURAL LANGUAGE PROCESSING**

6th Global Summit on Artificial Intelligence and Neural Networks

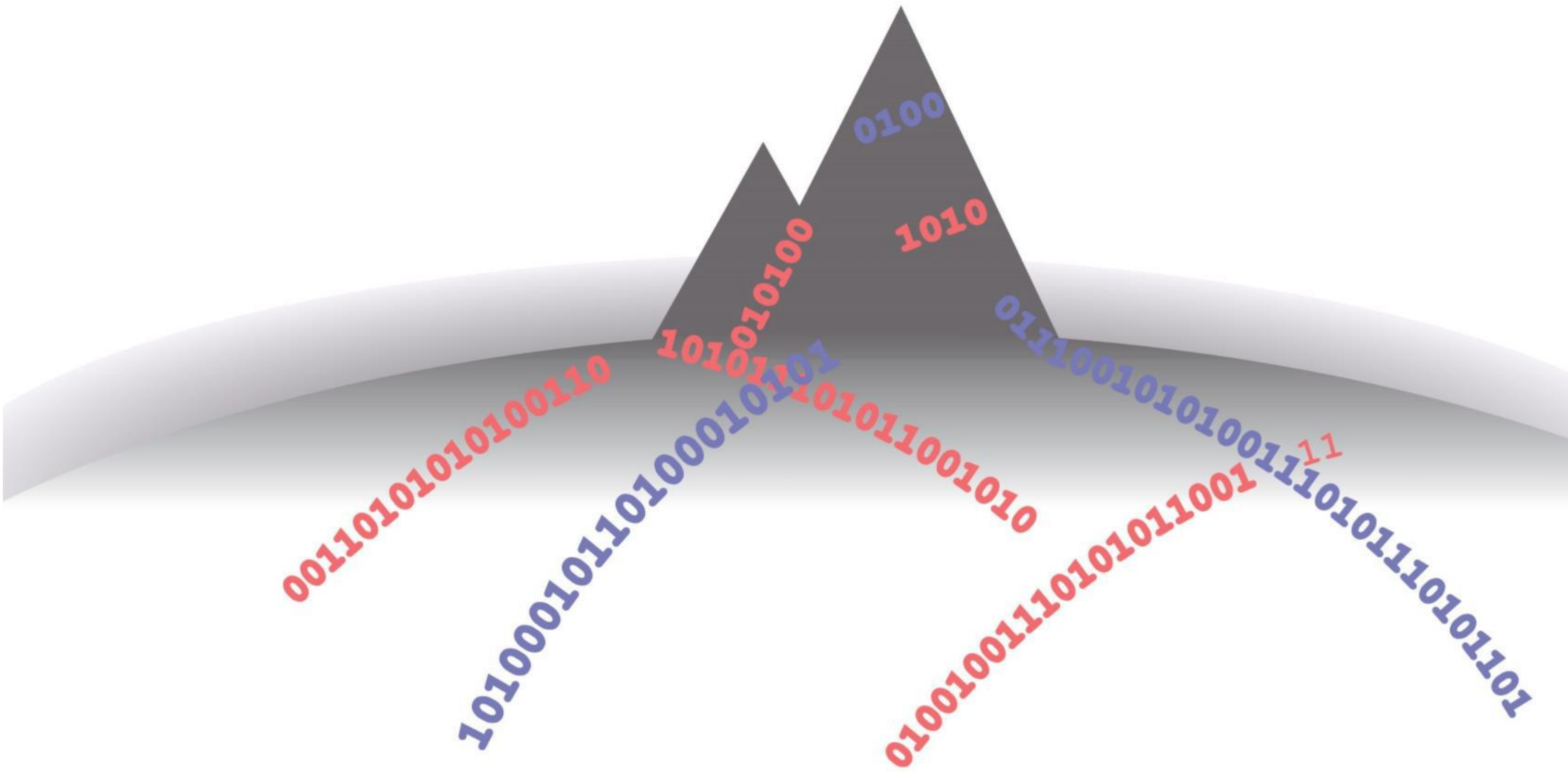
Venue: Helsinki, Finland

October 15-16, 2018

https://www.linkedin.com/in/sheo-shankar-singh/

@networks_neural

https://neuralnetworks.conferenceseries.com



The Midwest’s most impactful week for IT Security Information Collaboration is coming to Cleveland, Ohio October 22-26th

Now accepting Call for Papers through July 15th

www.informationsecuritysummit.org/summit-2018/

INFORMATION SECURITY SUMMIT℠
Building Community Through Education

Don't Forget To Register For

FutureTech EXPO Presents

The Bitcoin, Ethereum & Blockchain Superconference II

September 14-16, 2018

Held at the Kay Bailey Hutchison Dallas Convention Center.

TOP CONFERENCE SPEAKERS

Randi Zuckerberg
Founder & CEO - Zuckerberg Media
Created Facebook Live

Tim Draper
Billionaire Venture Capitalist DFJ Ventures; Draper University

Mark Yusko
Founder, Morgan Creek Capital Mgmt ($4.5 Billion under mgmt)

David Hirsch
Enforcement Attorney at U.S. Securities and Exchange Commission

Nick Spanos
Founder and CEO of Blockchain Technologies Corp.

Arman Rousta
Founder & CEO of KidCoin

Dustin Byington
President of Wanchain

Gary Leland
Speaker, Blogger, Podcaster, Videographer, Social Media Marketer , Publisher at CryptoCousins

Get 10% OFF - Use Code: CDM10
Get a Companion Ticket For $97 With Every Ticket Purchase

1,000+ Attendees Expected

www.thefuturetechexpo.com/register

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

“Amazing Keynote”

“Best Speaker on the Hacking Stage”

“Most Entertaining and Engaging”

Past and Upcoming Engagements: RSAC, NAB, CloudSEC, IPEXPO Europe October 2018 and many more... …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

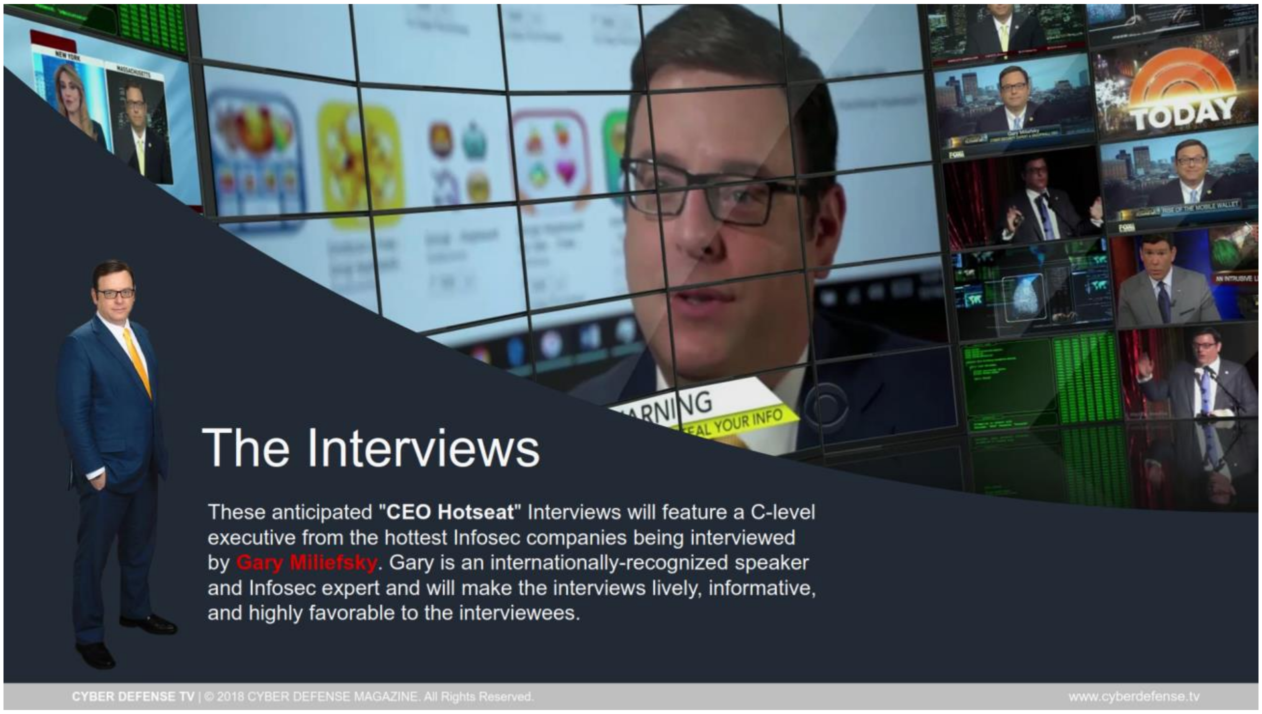
INFOSEC KNOWLEDGE IS POWER

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.



The Interviews

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

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved.

www.cyberdefense.tv

FREE MONTHLY CYBER DEFENSE EMAGAZINE VIA EMAIL

ENJOY OUR MONTHLY ELECTRONIC EDITIONS OF OUR MAGAZINES FOR FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry.

Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

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

CDM
CYBER DEFENSE MAGAZINE
eMAGAZINE
IN THIS EDITION:
NEVER STOPS GIVING
InfoSec Thoughts for 2018
Network Traffic Insecurities
Endpoint Security Best Practices
Vulnerability Equities Process
5 YEARS
DECEMBER 2017
MORE INSIDE!
SUBSCRIBE TODAY! NO STRINGS...
IT'S FREE

MARKETING AND PARTNERSHIP OPPORTUNITIES

BANNERS, E-MAILS, INFOSEC AWARDS, DOWNLOADS, PRINT EDITIONS AND MUCH MORE…

ANNUAL EDITION - RSAConference 2018
CDM
CYBER DEFENSE MAGAZINE
2018
PREDIC
CDM
CYBER DEFENSE MAGAZINE
Download
MediaKIT
Special Annual Edition
RSA Conference 2018
Email: marketing@cyberdefensemagazine.com
Call us Toll Free (USA): 1-833-844-9468
International: +1-603-280-4451 M-F 8am to 6pm EST
CDM | © 2018 CYBER DEFENSE MAGAZINE, All Rights Reserved.
www.cyberdefensemagazine.com

Copyright (C) 2018, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) PO Box 8224, Nashua, NH 03060-8224. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. marketing@cyberdefensemagazine.com Cyber Defense Published by Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC. Cyber Defense Magazine, CDM, Cyber Defense eMagazine, Cyber Defense Test Labs and CDTL are Registered Trademarks of STEVEN G. SAMUELS LLC. All rights reserved worldwide. Copyright © 2018, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them.

JOB OPPORTUNITIES

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

Cyber Defense Magazine

PO Box 8224, Nashua, NH 03060-8224.
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
mailto:marketing@cyberdefensemagazine.com
http://www.cyberdefensemagazine.com
Our New Office Addresses coming soon: **NEW YORK** (US HQ), **LONDON**, **HONG KONG**
Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 9/12/2018

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

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

THIS IS 100% POSSIBLE WITH

GOANYWHERE®
Managed File Transfer

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

Dropbox

Google Drive

VOTIRO SECURED.

salesforce

SharePoint

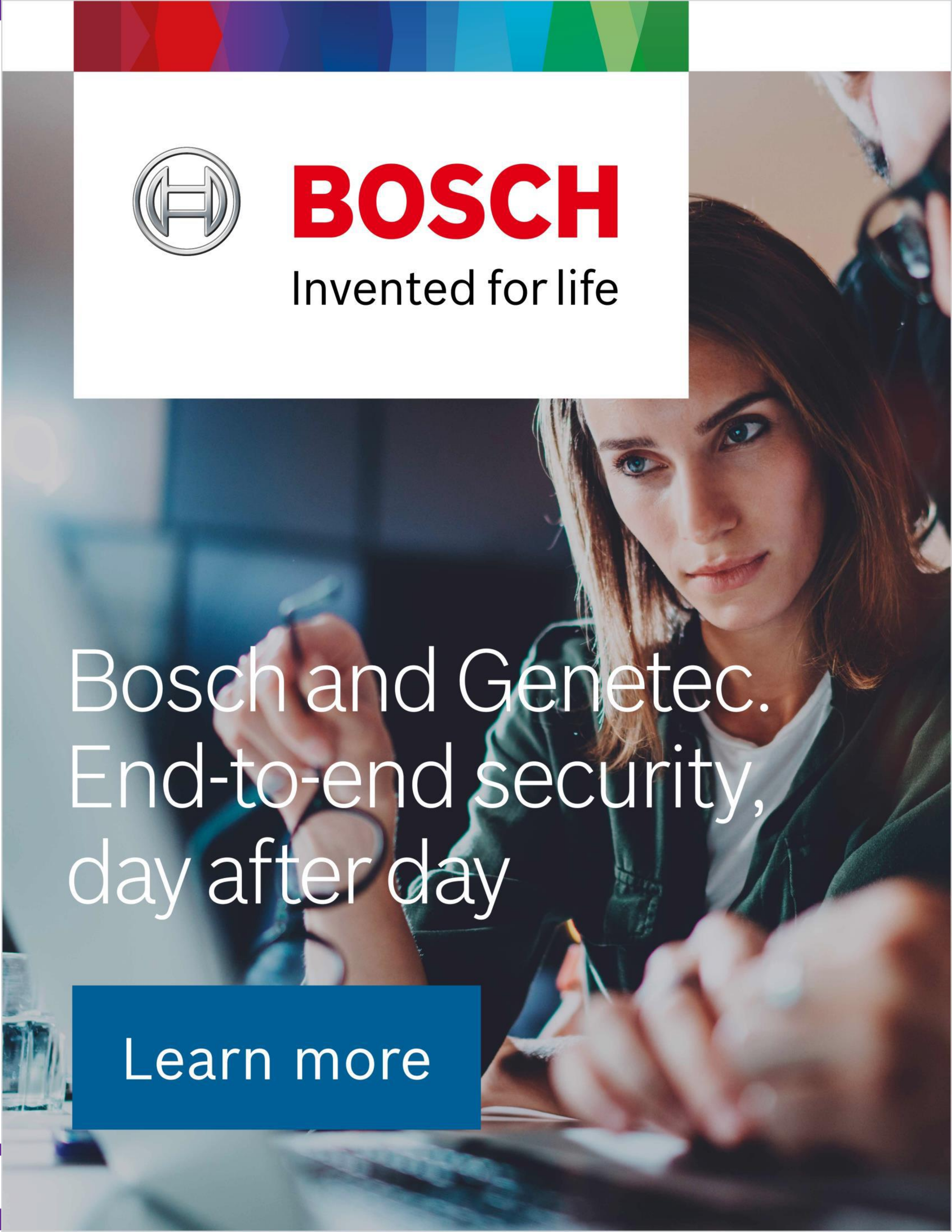
Jenkins

Microsoft Dynamics 365

zendesk

Simplify Your Processes and More with Secure Cloud Integrations

Request a Demo: www.goanywhere.com/demo


BOSCH
Invented for life
Bosch and Genetec.
End-to-end security,
day after day
Learn more