
7th Annual Edition for RSA Conference 2019
CYBER DEFENSE
MEDIA GROUP
2019
PREDICTIONS
INFOSEC
AWARDS
CYBER DEFENSE MAGAZINE
2019
I.A.M. Saving The Cloud?
A.I. & M. L. Working? Deception-Based Technology Delivering?
Much More Inside!

WELCOME ABOARD

We're honored to bring you our 7th Annual edition of Cyber Defense Magazine (CDM), exclusively in print at the RSA Conference (RSAC) 2019. It's thrilling to our team to know we're 3 years away from coming to RSAC for a decade. And what a decade it has been, both for the evolution of cyber security as well as the dynamic nature of exploitation. There have been major changes in cybercrime, cyber espionage and even cyber terrorism that many futurists would not have been able to predict. With the advent of cryptocurrency like Bitcoins, we've seen criminals shift to developing criminal botnet code to do cryptocurrency mining at the expense of our CPUs and electric bills. We've seen ransomware turn into ransom worms — literally becoming intranet distributed denial of service technologies, working from the inside-out instead of traditional DDoS attacks. WannaCry is a perfect example.

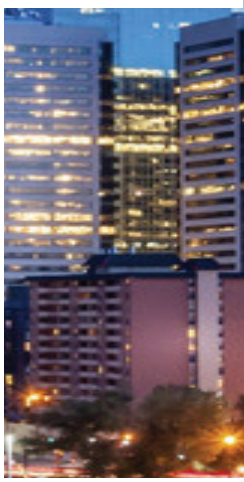
Enter the world of cyber defenses — automation of penetration testing, artificial intelligence and machine learning touted as the be-all end-all of fixing the problems and stopping the breaches, yet in parallel, we've seen so many breaches that the total record count for PII breaches has reached the Billions, in fact, more than the entire population of the globe.

Considering all these evolutionary changes and improvements to attacks and defenses, there has been a revolution in cloud computing, digital transformation and the Internet of Things (IoT). With that said, there are so many new types of devices running TCP/IP and having an IP address that it has become like a free candy store for sweet tooth cyber criminals and nation states looking for new espionage exploit vectors. It is time we see a revolution in breach prevention. Will this manifest on the trade show floor, here at the RSA Conference in 2019? Will leading vendors share with us some dramatic new findings and insights into how they are going to help us retool our cyber defenses?

Read on, walk the trade show floor, spend time to see and hear amazing speakers and panelists here at RSA Conference 2019 and find out. If you are reading the online version of this special edition of CDM, we suggest you enjoy some of our new platforms where we will continue to have great content and updates coming out of RSAC 2019.

Visit www.cyberdefenseawards.com to find the latest award-winning innovators. Visit www.cyberdefensetv.com for the latest interviews with some of these market innovators and leaders. Visit www.cyberdefenseradio.com to stream or save a podcast for later listening. Keep on enjoying our free online daily updated content and publications at www.cyberdefensemagazine.com and expect great things from us as we expand our media platforms, based upon your feedback! For example, if you are hiring in the field of cyber security or you are looking to fill one of the 100,000+ openings in our marketplace, please go to www.cyberdefenseprofessionals.com, our latest platform to help match make the job seekers and those hiring, specifically in the information security field, all at no cost in 2019. To our faithful readers, we thank you. Enjoy!





Pierluigi Paganini, Editor-in-Chief
Cyber Defense Magazine
www.cyberdefensemagazine.com

Gary S. Miliefsky, CEO
Cyber Defense Media Group
www.cyberdefensemediagroup.com

CONTENTS

4	Welcome Letter RSAC 2019
5	Top Cyber Security Predictions for 2019
9	Inspiring Greater Accountability ...
13	Taking the Fight to the Cybercriminals
17	Threat Intelligence: Data Driven Security
20	Winning the Battle for the Inbox
26	Zero Trust? Not if You're Surfing the Web...
31	CSIOS Corporation: Scaling New Heights...
34	Fraud Protection and AI in the Financial Markets
38	Thanks to Human Expertise, Companies...
42	Why Major Data Breaches Will Continue in 2019
46	The Impact of the Marriott Breach...
50	For Better Protection, Stop Buying Security...
54	Deception-based Technology Market Overview
59	Five Things You Need to Know...
61	Unlocking Your Users' Digital Identities...
67	What do Organizations Need to Build...
70	02. Ericsson, and Equifax: How Certificate...
73	'To Be or Not To Be': Here's How SMBs...
77	Frontline Defense Against CyberWar
81	Attacked on All Sides
84	High-Level Strategies for Third-Party Risk Mitigation
87	What to Look for When Selecting an MSSP
90	Quis custodiet ipsos custodes?
94	Aligning Cybersecurity Effectiveness...
98	Defense by Offense
101	Third Party — Minimizing Organizational Exposure by...
104	Filling the Public Relations Void...
107	Welcome to the InfoSec Awards for 2019

CYBER DEFENSE MAGAZINE
is a Cyber Defense Media Group (CDMG) publication distributed electronically via opt-in GDPR compliant e-Mail, HTML, PDF, mobile and online flipbook forwards. All electronic editions are available for free, always. No strings attached. Annual print editions of CDM are distributed exclusively at the RSA Conference each year for our USA editions and at IP EXPO EUROPE in the UK for our Global editions. Key contacts:

PUBLISHER
Gary S. Miliefsky
garym@cyberdefensemagazine.com

PRESIDENT
Stevin V. Miliefsky
stevinv@cyberdefensemagazine.com

VICE PRESIDENT OF BIZ DEV & STRATEGY
Tom Hunter
tom@cyberdefensemediagroup.com

EDITOR-IN-CHIEF
Pierluigi Paganini
Pierluigi.paganini@cyberdefensemagazine.com

MARKETING, ADVERTISING & INQUIRIES
marketing@cyberdefensemagazine.com

Interested in writing for us:
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: +1-833-844-9468
International: +1-603-280-4451
New York (USA/HQ): +1-646-586-9545
London (UK/EU): +44-203-695-2952
Hong Kong (Asia): +852-580-89020
Skype: cyber.defense
E-mail: marketing@cyberdefensemagazine.com
Web: www.cyberdefensemagazine.com
TV: www.cyberdefense.tv

Welcome Letter RSAC 2019

RSA Conference 2019 is here. Welcome to our 28th annual event! Running from March 4–8, 2019, RSAC anticipates hosting around 45,000 security professionals, media, analysts and vendors in San Francisco — it's where the world talks security.

Each year following the Conference, we gather information and feedback from a cross section of attendees, sponsors and exhibitors to help us figure out how we can improve the Conference experience for all involved. We're thrilled with where we landed and are delighted to provide another content-rich experience with a variety of new programs. For example, we'll have two keynote stages: West Stage keynotes will continue to feature sponsor keynotes, panels and esteemed guest speakers, and South Stage keynotes will utilize the newly opened Moscone Center South to bring highly coveted sessions from industry experts to a broader audience.

You'll also see track sessions throughout the week discussing geopolitics, frameworks, supply chain and third-party risk, privacy, DevSecOps, artificial intelligence and much more. Early in the week, expanded Innovation Programming will include more events and opportunities for entrepreneurs to push our industry forward with new solutions, from mobile security to biometrics. In addition, we've added the RSAC CISO Boot Camp for senior-level security executives to join forces in one room and focus on solving the industry's biggest issues, from cyberespionage to the skills gap. To say I'm eager to see the ideas that will unfold would be an understatement!

Our theme for this year's Conference aims to answer the candid question: How can we make cybersecurity better?. We know that, in order to fortify our industry against tomorrow's cybercrime, we need to create better products, harness the power of innovation and produce better results. But we believe a better, brighter future is only possible through dedication and collaboration.

Our mission at RSA Conference is centered around the collective desire to do more. We believe it's about unifying everyone — from engineers to CEOs — to work toward building a more secure world so that others can get on with the business of making it a better one. That's the goal of being better: staying ahead of tomorrow's threats, putting in the extra hours and making security an "everybody issue." So, yes, we must create better technology and more efficient solutions, but we also must realize the importance of the way we source those ideas and how we communicate the priority of what we do to our colleagues and customers. I believe that will help us all to make better a reality.

We are so pleased you could make it to this year's Conference and help our industry become the best it can be. Welcome to RSA Conference 2019!

Linda Gray Martin

Director & Chief of Operations, RSA Conferences



Top Cyber Security Predictions for 2019

What will happen in the threat landscape during the next 12 months? Let's try to imagine which will be the threats and the threat actors that will influence the cyber arena next year.

2019 — Predictions

P1 - Cyber-crime-as-service — stronger than ever

In 2019, the crime-as-a-service model will continue to a key factor for the growth of the cybercrime ecosystem. The model will allow a growing number of cybercriminals and wannabe crooks to easily access to malicious services and products, including malware, exploits, DDoS-for-hire services, RDP accesses, and botnets.

Novice criminals could approach cybercrime even without specific skills, while skilled hackers could prefer crime-as-a-service to speed-up their operations and make it hard the attribution of attacks to specific threat actors.

Among the numerous services offered in the cybercrime underground, Malware-as-a-service platforms focused on cryptocurrency mining, RaaS services and DDoS-for-hire platforms will monopolize the threat landscape in the next months.

P2 — The number of IoT attacks will increase

The number of cyber-attacks carry out through huge botnets of compromised IoT devices will increase. Threat actors will leverage known vulnerabilities to compromise smart objects such as routers and connected cameras. Security experts will discover a growing number of thingbots composed tens of thousands of infected IoT devices that were used to carry out malicious activities, such as DDoS attacks or spam campaigns.



P3 – Nation-state hacking, it's an emergency

The number of operations attributed to nation-state attackers will increase in the next months. The lack of a global framework of norms of state behaviour in the cyber space and the absence of severe sanctions for rogue states will encourage state-sponsored hacking. Government will continue to carry out cyber espionage and sabotage campaigns, Russia, China and North Korea will be most aggressive countries in the cyber arena. While China will be more focused on cyber espionage, North Korea will focus its operations on stealing funds due to the sanctions against its Government. The most dreaded state will be Russia, its state-sponsored hackers will be more focused on cyber espionage and on online misinformation.
In this scenario, other APT groups, such as Iran-linked cyber espionage crews, will be very active in 2019.

P4 — Supply Chain attacks on the rise

Threat actors, especially state-sponsored attackers, will focus their efforts in compromising the supply chain of popular software to hit a wide audience. Threat actors implant malware into legitimate applications replacing their software update with tainted versions. In this way, every user receiving the update will automatically have their system compromised.
In the last months security experts discovered several attacks against supply chain of popular applications. In August, experts from Trend Micro uncovered the Operation Red Signature, attackers compromised update server of a remote support solutions provider in South Korea and delivered a remote access Trojan (RAT) used to steal sensitive information from the victims.
In July Microsoft revealed that hackers attempted to compromise the supply chain of an unnamed maker of PDF software.
Experts fear that a growing number of threat actors will target the supply chain in the next months due to the efficiency of this attack scheme. The attacks will be more sophisticated and could be hard to detect.



P5 — ICS/SCADA attacks a global concerns

We will observe a growing number of cyber attacks aimed at ICS/SCADA systems most of which are still not designed to be resilient to cyber assaults.
The majority of the attacks will be not targeted in nature, but we will observe also sophisticated nation-state actors that will develop new cyber weapons to hit industrial control systems and SCADA devices.
Both targeted attacks and collateral infections could have destructive effects on the systems in critical infrastructure- Energy and manufacturing industries will be the most exposed sectors to these threats.

P6 — Facing the cyberbullying

Cyberbullying is a social emergency in almost any country, the number of victims will continue to increase and the official figures provided by the authorities are just the tip of the iceberg. Governments will continue promoting awareness campaigns aimed at preventing these crimes, youngsters are particularly exposed and damages caused by cyberbullying could be dramatic for the victims.



P7 —AI-based attacks, a nightmare for security experts

The adoption of AI systems in cyber security is not a novelty. Some threat intelligence systems already employ AI to detect threats and neutralize them.

Basically AI-powered defense systems today are used to automate manual tasks and enhance human activities, but many experts argue that currently many entities are already working to use it for offensive purposes. AI-based systems could be used to automate some phases of the attacks like reconnaissance or exploitation of vulnerabilities.

Intelligent systems could be used to search for unfixed vulnerabilities in a target system and exploit them to carry out the attacks. AI systems could be also used to carry out sophisticated social engineering attacks or to use false flags to deceive the defenders and make hard the attribution. The involvement of AI-based systems in misinformation campaign conducted by rogue states is a nightmare for security experts and intelligence analysts.

The risk that AI-bases systems could be used to launch surgical attacks is concrete and most of defense systems could be not prepared to detect and repel these kind of attacks.

P8 – Cloud storages, the gold mines for attackers

A growing number of companies already rely on cloud storages, it's normal that threat actors are devising new technique to find unsecured systems and attack them.

Cloud infrastructures are a potential targets of security breaches, attackers will use several techniques to steal data and to monetize their efforts. Cloud-based ransomware could target infrastructure of businesses and cause heavy losses.



Inspiring Greater Accountability with Improved Security KPIs

By Lewie Dunsworth, EVP Technical Operations, Herjavec Group

Getting a good night's sleep has become increasingly difficult for CISO's. In a recent Cybersecurity CEO piece Herjavec Group Founder & CEO, Robert Herjavec, referenced how CISOs toss and turn, kept awake by thoughts of:

- Accountability to leadership — being held accountable to delivering on expectations as the board approves investments to improve security
- Capability of team — questioning do I have the right skills and right people to do the right things?
- Compliance & Privacy Regulation — how do GDPR, and other industry or regional regulations impact my security program?

The good news is that the CEO and board are more engaged in cybersecurity conversations than ever before. C-Level members are no longer passing off responsibility. CISOs aren't educating in the board room as they used to — and trust me, I've been in their shoes. The board is asking the right questions and holding their teams accountable. I would confidently say the C-suite is maturing when it comes to security knowledge.

Keep in mind, each player around that table may have slightly different priorities:

- CEO — Concerned with the reputation of the company in the event of a breach. How could credibility, customer retention and overall stock price/business value be impacted?
- CFO — How will we fund ongoing security initiatives? Are we maximizing the value of our investments today? What risk remains and what risk are we sharing with 3rd parties, including contractors, suppliers and customers?
- COO — Will any business operation be impacted by the security program or new technology roll out? Is the roadmap on schedule? What is our incident response plan to regain business operation in the event of a breach?

At the end of the day the C-Suite shares mutual concerns about security risk and liability in the event of a breach. How you communicate this and keep them informed is pivotal.

As security becomes a more digestible topic of conversation at the quarterly board meeting it's imperative CISOs have the proper metrics to measure their progress and the inherent risks that remain. Herjavec Group recommends aligning early with your executive leadership team on a Security Roadmap — then developing key performance indicators (KPIs) that you can report on so status updates and progress measurements are concise, clear and continue to be digestible.



I've summarized a sample roadmap below and recommend a template with 5 Key Performance Indicators to keep your security program on track:

1. Mean Time To Detect and Contain — Measures the effectiveness of your controls, monitoring and response time. We recommend you compare to industry average, and compliance requirements to reduce liability concerns.

2. Vulnerabilities Per Host — Demonstrates the importance of an effective security hygiene program. Provides the opportunity to highlight your effectiveness in patch management.

3. Control Efficacy — Review and critique of security stack to measure effectiveness of security controls. Highlight current coverage as well as scheduled investments/areas of improvement. Demonstrates your ability to protect the business and highlights any gaps/risks that remain.

4. Audit and Compliance — Provide progress update on audit findings and inform on new compliance measures the board needs to be mindful of.

5. Key Dates/Achievements — Highlight upcoming program milestones, share key dates that were hit/missed etc...

Sample Security Roadmap

Herjavec Group often customizes a security roadmap with our customers to ensure we are on the same trajectory regarding their security controls, planning and investments. It is imperative we communicate openly about investment, risk and timelines to set our partner CISOs up for success as they present Security Key Performance Indicators to their respective boards. We typically review these programs quarterly with the KPIs highlighted above in mind.

Year 1: Build Your Security Foundation

- Have you undergone an assessment for your current security program?
- When was the last penetration test performed?
- Have you conducted a full review of your technology stack?
- Do you have a Managed Security Services Provider partnership in place? If so, what is the status of your onboarding and support?
- Have you developed an Incident Response plan? Has it been communicated internally and was it amended for any findings from the pen test performance?

Year 2: Have Proactive Measures in Place

- Have you conducted table-top and red-teaming exercises to test the efficacy of your security program improvements over the last year?
- Have you engaged an Incident Response team on retainer in the event of a cyber-attack?
- Have you evaluated how Threat Management could bolster your SOC Operation & Threat Detection abilities?
- What Security Workflows do you have covered through play book orchestration? Have you evaluated a Managed Detection & Response service to advance your use of workflow automation?

Year 3: Implement Workflow Orchestration

- Have you kept up with your security testing? We recommend alternating penetration tests and red team exercises each year, unless you have a compliance requirement for pen tests on an annual basis.
- Have you implemented a security awareness program across your employees? When was your last social engineering exercise to determine the likelihood of your organization falling victim to insider threats?
- Have you renewed your incident response retainer?
- Have you augmented the tools logging to your SIEM within your Managed Security Services Provider partnership?
- Do you have dedicated Threat Hunting Support?
- Have you advanced your use of MDR services?

After a three-year cycle, it's common to refresh the complete program, review the foundation and step back to consider how the business has changed.

– Perhaps M&A activity altered your security priorities?
– Maybe you inherited a mandate to bring security services in house in year two?
– Could be that the introduction of a new compliance measure through your plans off track?

Take time to reflect on the Security Roadmap set out in year 1 and evaluate what is still critical to your success going forward. How has the program performed relative to the KPIs aligned to?

As Bruce Schneier, an American cryptographer and author, famously stated, "Security is a journey, not a destination." While the only thing constant in our industry is change, with a strong security roadmap and digestible metrics, you will be well on your way to inspiring the confidence of your executive board and ensuring their commitment and accountability to your organization's security program.

ASK YOURSELF:
1. How would you summarize your security program metrics to your executive team?
2. Do you have an aligned to security roadmap and key performance indicators you share on a regular basis?
3. Do you have open conversations with your security partners about how they augment and support your overall security roadmap?



About Lewie Dunsworth

Lewie Dunsworth is CISO & Executive Vice President of Technical Operations at Herjavec Group, bringing more than 17 years of information security experience to the role. Prior to Herjavec Group, Lewie held executive roles as the CISO at H&R Block and the SVP of Advisory Services & Managed Services at Optiv. His business-forward approach helps companies create a balanced strategy and effective security program, to adequately protect their most critical assets. He earned his Bachelor of Science degree in Network and Communications Management from DeVry University and a Master of Business Administration, Executive from the University of Missouri in Kansas City. He is also a Certified Information Systems Security Professional (CISSP).

Does Your Organization Need MFT Software?

Determine if a secure file transfer solution is right for you.



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

GO ANYWHERE®
Managed File Transfer

Visit us at RSA Conference
South Hall Booth 150

But is this solution right for you?

You might benefit from MFT if:

1. You need to audit your file transfer activity.
2. You need to comply with data security laws and regulations.
3. You use traditional methods (e.g. FTP or legacy scripts) to send data.
4. You need to automate secure file transfers that are business critical.

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

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

Taking the fight to the cybercriminals

Why organisations urgently need to outsource threat intelligence gathering

As cybercrime itself matures into an industry with its own software-as-a-service and highly organised underground professional networks, the task of adequately securing their systems against attack is already well beyond the resources of most enterprises.

The major problem faced by CISOs today is how to identify which of the millions of cyber threats now attacking organisations across the world is directed at them. The dilemma is growing daily as more data is stored on more servers, as more businesses move their information onto the cloud and as the Internet of Things starts to connect almost every device on earth. Robotics, AI, 3D-printing, not to mention biosciences, will all be increasingly data-driven and will therefore form additional targets.

According to industry estimates, the global cost of cybercrime is set to grow from $500 billion in 2014 to over a $1 trillion before the next decade. But even this may turn out to be a gross underestimate as the world becomes increasing data-driven and connected. The massive technological changes taking place over the next five years, sometimes known as the Fourth Industrial Revolution, will not only mean more connected devices but also more reason to break into them. It is already hard to think of any aspects of our lives that are not data-driven — in five years' time, it will be impossible to name one.



But a fully-connected world is a Utopia for every type of hacker, cyber-criminal, spy, terrorist and 'rogue' nation state on earth. And there will be even greater reason to break into data networks in the future when the stakes will no longer merely be confidential customer information or new product designs but whole financial systems, national power grids, airlines, drones, driverless electric cars, smart factories and smart cities, not to mention armies, navies, air forces and their entire supply chains. All will be considered fair game for hackers and cybercriminals.

Given that the stakes are becoming so high and our lives and businesses are so interconnected, cybersecurity is too vital a component of national prosperity, national security and, eventually, national survival, to be left to individual organisations. Many CISOs still rely on patches for well-known viruses while taking precautions against well-publicised threats such as Wannacry. Enterprises attempting to pursue this traditional type of security strategy into the next decade will risk not only severe financial losses and compromised customer confidence but are also potentially liable for swingeing fines of up to €20 million or four per cent of turnover, whichever is greater, under the GDPR for failing to take precautions that were available in the marketplace.

The only really effective way to safeguard data is for organisations to extend their security perimeters well beyond traditional boundaries in order to encompass areas such as the Dark Web, where organised groups of highly professional cybercriminals orchestrate increasingly sophisticated cyber-attacks. Over the last few years, the Dark Web (DW) has also become a training ground for relatively unskilled and inexperienced cyber criminals. Some DW vendors now offer not only off-the-shelf malware-as-a-service but also have 24-hour help lines to offer assistance with complex cyber-attacks.

Over the last 18 months, a string of major organisations have exposed their ignorance and vulnerability by only realising that they had suffered a major hack far too late and only once someone informed them that their customers' confidential data was being sold openly on the Dark Web. Major airlines, banks and retailers have also been unaware that cybercriminal gangs operating on the DW are selling kits that allow even relatively unskilled criminals to clone corporate websites in order to elicit credit card details and other personal data from the brand's existing customers. Customers who have been defrauded in this way are likely to avoid the brand in future, even though the company was unaware its website had been cloned. Domain-jacking software being sold on the DW also now enables even inexperienced hackers to break into corporate IT systems.

Had those organisations which have been named and shamed for poor cyber security practices over the last year and a half been able to gather crucial forward intelligence of the cyber-attacks threatening them as they were being orchestrated across the Dark Web and social networks, they would have been forewarned and forearmed in time. They could easily have avoided the damage that the successful breaches have done to their reputation and customer and investor confidence in addition to the significant financial losses incurred.

But to accomplish this would require organisations to commit thousands of man hours on the part of expert researchers to patrol the DW forums and monitor the organisation's brand across all platforms including social media. The cost would be prohibitive and the results would be likely to be patchy as few organisations can fully grasp the sheer scale and number of the cyber threats now looming in 2019 and beyond. And even if they were in possession of such a vast amount of data, it would be virtually impossible for them to sift through millions of incoming threats to single out those aimed directly at their own organisation.

Resecurity's own meta database of upcoming cyber threats is currently growing at an accelerating rate and Resecurity's CONTEXT™ now offers organisations of all sizes access to a comprehensive platform with a growing meta database of over 300 million DW records, 8 billion compromised credentials, 9 million threat actors and over 30 million indicators of compromise (IOCs).

In order to assist organisations of all kinds in identifying those cyber-attacks that are heading straight for them and to enable them to spend their cybersecurity budget in the most effective manner, Resecurity has developed machine-learning technology capable of cross-referencing vast volumes of data. It is extremely important for all organisations to have a proactive and reliable solution for timely risk mitigation. Resecurity Risk™ is a cloud-delivered solution that protects against both external and internal threats, safeguarding the company brand, employees, network devices (IoTs), critical business applications, processes and services, cloud environment and the company's entire supply chain.

As more companies shift data storage to the cloud, new vulnerabilities also begin to emerge. Companies therefore also need around-the-clock security monitoring of cloud workloads in AWS Amazon in order to prevent data breaches at an early stage. Effective and early identification of insider threats also requires expert and up-to-the-minute knowledge of the latest cyber scams. This is also crucial when determining whether the inside threat is the result of a dishonest or disgruntled employee or whether a member of staff's terminal has been hacked externally.

Effective intelligence gathering and the contextualisation of such vast volumes of data is now beyond the simple remit of most internal IT departments. This disparity is set to grow as the fourth industrial revolution gathers pace this year and then starts to create a truly data-driven world in the early 2020's.

CISO's can no longer be expected to gather their own cyber intelligence or gauge its importance relative to their own organisations. Just as enterprises universally outsource the manufacture of their hardware and the running of their external communications networks and power supplies, they will increasingly need to use third parties to supply sufficient contextualised threat intelligence to provide 24/7 360-degree protection against all incoming and insider threats in 2019 and beyond.

Tony Glover is the senior consultant at TGPR. He heads a London-based international public relations consultancy based in London representing cybersecurity companies across several continents. Until becoming a PR consultant three years ago, he was an award-winning journalist specializing in IT and international crime and has been writing about IT security issues since the dawn of the internet. His articles have been published in Time Magazine, the Financial Times, Institutional Investor and many other newspapers and magazines. He has also made numerous TV and radio appearances on networks including the BBC and NBC. His current mission is to help the cybersecurity industry communicate effectively with those organizations that are most in need of its services.Tony can be reached online at tonyglover@tgpr.co.uk.



GTB Technologies
Data Protection that Works

Newport Beach, CA USA
info@gttb.com / www.gttb.com
+01 800.626.0557



RSA Conference 2019
San Francisco
March 4–8
Moscone Center

Protecting Sensitive Data

Booth 264, South Expo

Discover, Monitor & Control

IP & COMPLIANCE DATA

Can your organization meet the compliance and regulation requirements of California Consumer Privacy, GDPR, NY DFS, HITECH, the everchanging State and Federal Regulations including those policies and procedures to address privacy rule controls, security rule controls and breach notification controls?

Many years of experience

As the creator of DLP for Intellectual Property and pioneer of DLP for Compliance, GTB solutions are proven, patented and powerful.

Powerful knowledge

GTB's team of cybersecurity experts have years of experience educating on security threats & best practices.

Trust of clients

Used by the Who's Who of Global Enterprises, Governments & Organizations

Technology Leadership

Our technology is simple and easy to deploy yet it is the most powerful within the Data Protection space.

Why GTB Technologies

Today DLP solutions must have ways of identifying threats and protecting against attacks. Proprietary algorithms such as GTB's artificial intelligent programs can identify even partial data matches so managers remain alert to any attempts at data exfiltration from a malicious insider or malware.

GTB's Data Loss Protection tools offer streamlined solutions for companies that seek the most robust in data security while not hindering workflow. GTB ensures data remains under the highest standards of protection, while avoiding blanket security protocols that create obstacles for employees and impede collaboration.

For over 13 years, GTB Technologies, the creator of DLP for IP, has provided data protection solutions that accurately prevent sensitive data loss / data ex-filtration from within the network, at the endpoint, in the cloud or anywhere else; either agent or agent-less, in files or data streams.



Threat Intelligence: Data Driven Security

by Liejun Wang, director of 360 threat intelligence center, 360ESG

Gartner's definition on threat intelligence is as follows:
"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."
This is an ideal definition, which proposes clear requirements for the amount of information to be included in intelligence. The complete intelligence style, as the basis of providing decisions for high end users, can be considered as narrowly defined threat intelligence.
In fact, such accurate and comprehensive intelligence services mentioned above are not available to most organizations and agencies. Even if such services are obtainable, they may not be so actionable. Just imagine, even though a security vendor is able to provide the background of a foreign APT group, including source countries and even the personnel information (These are all necessary to high end threat intelligence), to a large enterprise is faced with, what else could the company do? Generally, the organizations and agencies cannot serve as law enforcement agencies to take measures to mitigate threats arising from the intelligence.
For general companies or organizations, relatively low-end indicator of compromise (IOC) is more realistic. It consists of data that can be applied to boundary security devices and host security protection software. The typical intrusion indicator includes file HASH, IP, domain name, program operating path, registry key, etc. The continuous accumulation and iteration of the producible threat intelligence cannot be accomplished in a single day.

As threat intelligence has very high demands for timeliness and industry, experts ever conducted researches specifically for open source threat intelligence and found that 75% malicious IP intelligence lasts for no more than 5 days. The threat intelligence against financial industry might not apply to telecom industry.

It is for these reasons that threat intelligence has high requirements on suppliers' customization capability. In many cases, security vendors' integrated threat intelligence services will not achieve expected results, but produce a lot of noises and increase the burden on security personnel.

360 ESG, itself, is endowed with PE sample collection capacity at tens of billions level. The capability of full-dose data collection and rapid data processing makes 360 more efficient in producing threat intelligence. On the one hand, the timeliness of threat intelligence is guaranteed to the greatest extent; on the other hand, the customization capability of threat intelligence products in many subdivided fields is also supported by sufficient data.

Then how can 360 ESG own such big data for security? To be more specific, it aims to provide useful and all-dimensional IP reputation for information and realize the ability to discover, evaluate and track a variety of epidemic and advanced targeted attacks by producing attack discovery logs of vast terminal samples, active defense data, file credit information and a variety of security products (such as website security, firewall, situational awareness, advanced threat discovery, etc.), and integrating the identification and portraits of associated threat sources based on huge security terminal software installation foundation in China. Meanwhile, as the basic data of machine-readable intelligence in batch production, it can realize local and popular attack IOC coverage. Besides, relying on vast threat intelligence source data like historical Passive DNS and Whois data, 360 ESG is endowed with efficient capability to discover threat, associate and attack sources.

Based on threat intelligence, 360 ESG also owns the first-class ability to discover and track APT groups. According to the statistics, 38 APT groups are monitored by 360 in total, which is the supplier who published the most APT reports in China. APT groups firstly discovered and named by 360 include OceanLotus, APT-C-12, APT-C-01, etc.

In the year of 2018, 360 threat intelligence center published more than 20 technical reports on APT activity, which involve six independent APT groups, including two firstly revealed groups in 2018, and discovered two in the wild Oday vulnerability attack cases, thus taking the leading position together with internationally recognized suppliers.

Such kind of experience accumulation and strength demonstration is attributed to 360 ESG threat intelligence research and analysis team, which is formed by nearly 100 experts. Specialized talents are available for all links of threat analysis, including public intelligence collection, data processing, malicious code analysis, network traffic analysis and clue mining expansion, thus providing powerful basic data and threat assessment support for improving the ability in developing security services and products of threat intelligence.

Till now, 360 ESG has already published many threat intelligence products like Alpha threat analysis platform, threat intelligence platform – TIP, threat intelligence platform for regulatory industry – threat radar, advanced threat intelligence analysis services and Cloud SaaS API, and has been able to provide customized industrial solutions for different customers, thus playing a leading role in the industry in terms of the delivery success rate.

In addition, core security products and services like 360 intelligent firewall, EDR, NGSOC, situational awareness, Cloud security and virtual security are integrated into the threat intelligence ability. The machine-readable intelligence can be rapidly sent to security devices, formulating a linkage defense system driven by threat intelligence. 360 ESG will make persistent efforts to demonstrate more excellent threat intelligence ability in the future.

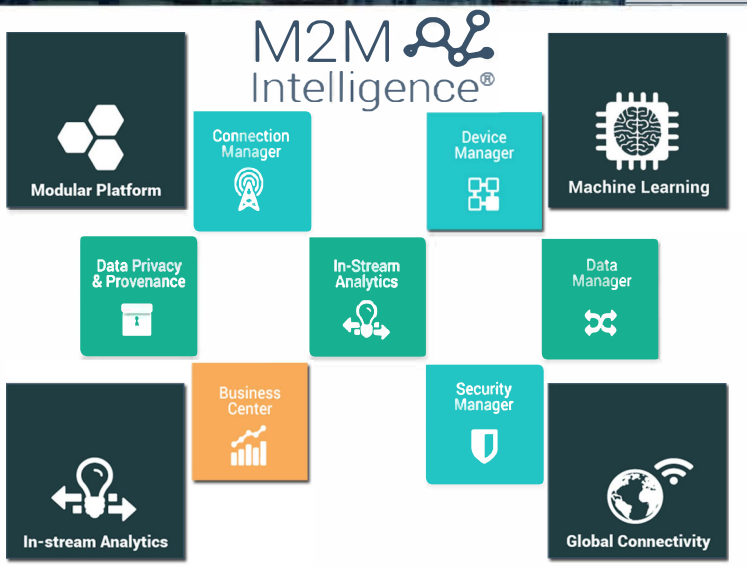
Liejun Wang is the Director of 360 threat intelligence center, with a focus on malware analysis and APT tracking.



M2Mi
Machine-to-Machine Intelligence Corporation

IoT SECURITY PROFESSIONAL SUITE™
FOR CYBERSECURITY COMPLIANCE

The proliferation of connected devices is generating new economic opportunities in industries all over the world. During this tremendous growth M2Mi is ensuring that organizations remain secure as regulatory compliance increases.The IoT Security Professional Suite™ is M2Mi's award winning solution composed of cutting edge cryptographic ciphers and primitives as well as M2M Intelligence®.





OVERVIEW

The IoT Security Professional Suite™ solves the pressing problem of preserving compliance as cybersecurity threats and regulations are on the rise. The rapid growth of IoT has resulted in tightened cybersecurity regulations and the large increase of attack vectors. As a consequence, obligations to meet industry compliance and regulations is becoming ever more challenging to achieve.

The IoT Security Professional Suite is designed for industrial applications and therefore specific industry compliance. This allows organizations to quickly generate and deploy IoT device code that comply with their industry's regulations. The IoT Security Professional Management Portal™ allows device owners to monitor their fleet's health using intuitive dashboards, alerts, group commands, and insight analytics.

CONTACT

contact@m2mi.com
+1 (415) 613 0684
www.m2mi.com

FEATURES

Through M2Mi's award winning IoT application, the solution provides an intelligence layer capable of addressing complex IoT challenges such as data normalization and transform, machine learning and analytics, device and communication management as well as resource metering using microservices.

The IoT Security Professional Suite™ was built on the recommendation of the DHS CyberSecurity S&T. It supports legacy and forefront cryptographic technologies.

The solution supports multiple protocols such as MQTT, CoAP, SCADA, or communication technologies such as Wi-Fi or ZigBee.

Security models with tamperproof services suitable for preserving the integrity of revenue.

The IoT Security Professional Suite™ cryptography is certified for National Security Systems, Smart Aviation Architecture and supports industry 4.0, IIC.

Copyright © 2019. Machine-to-Machine Intelligence [M2Mi] Corporation. All rights reserved.



Winning the Battle for the Inbox

by John Randall, VP Product Management, EdgeWave

Winning the battle for the inbox

For virtually everyone, email is the primary way of connecting and doing business. However, as we all know, the inbox isn't as safe as it once was. All sorts of bad actors are increasingly competing to penetrate into users' inboxes and exfiltrate confidential information, or launch nefarious links or code that enable them to open backdoors into critical systems and data.

As email threats become more and more targeted and sophisticated, the challenge to protect inboxes has taken on a whole new level of complexity. Even as recently as a few years ago, all an organization had to do was deploy an email gateway to filter out spam, malware and other inbox invaders. Done.

Unfortunately, the game has changed. Today's advanced, socially engineered email threats blow right past traditional gateways and attack users in a variety of ways with spear phishing, Business Email Compromise (BEC), ransomware and more. An email security gateway is no match for these attacks. Consequently, users are being conned, spoofed and deceived more than ever, and it's costing businesses billions of dollars a year in damages.

The reality of today's email threat landscape.

Recently, we conducted a survey of over 300 IT security professionals, from CISOs to infosec administrators. While we asked a number of questions, several key points stood out. More than 80 percent of participants said they were "confident" or "very confident" that traditional email gateways will protect their organizations from targeted email attacks. Yet a substantial percentage — 42 percent — also reported that their organization fell victim to a recent phishing attack. That's quite a disconnect.

In another contradictory finding, the survey revealed that the majority of IT professionals aren't confident in employees' ability to spot or flag malicious emails, even though over 70 percent of responders reported that their organizations had conducted security awareness training during the previous 12 months.

The survey results are a wake-up call, revealing a significant disconnect between IT professionals' confidence in their existing email security strategy and the realities of the threat landscape. These survey findings also serve as a call to action, underscoring the need for IT professionals to honestly assess their current email security measures and take steps to achieve a modern email security posture.

Is Security Awareness Education the answer?
Several years ago, security awareness education became the defacto "next step" in tightening inbox security. Since users are on their own with email, training helps users spot or flag suspicious emails so they can send them to their IT department to investigate. Education is always a good thing, and many companies have seen some benefit from the investment. However, education alone is not enough. In fact, the 2018 Verizon Data Breach Investigations Report states that despite significant investments in Security Awareness Training, users only reported 17% of phishing campaigns. Which isn't surprising when you consider our always-connected, always-emailing workforce. Employees today are far more distracted than ever, and that presents even more risk as users email from mobile devices at all times day and night. Clearly, with over 90% of data breaches starting from an email attack vector, organizations today need to drastically change how they think about email security.



Next-generation email security is needed.
For the past two years, EdgeWave has been committed to helping better protect users and data with advanced email security solutions beyond the traditional gateway. We launched our Email Security Platform in 2018 with a mission—Delivering the World's Safest Inboxes™. At its heart are three essential elements:

1. Predelivery Protection with a modern gateway solution: The best defense is a good offense, and predelivery measures can stop attacks before they start. The right predelivery protection via an email security gateway is still effective at stopping broad-based malicious campaigns (though limited in prevented highly targeted phishing emails, which is why a multi-layered email security posture is required). A modern email gateway should stop threats from reaching the inbox without tying up IT resources. Look for a comprehensive email security gateway that addresses the most advanced threats while keeping false positive rates low.

An ideal predelivery solution is also capable of stopping zero-minute attacks and other emerging threats without hampering the flow of legitimate email. Look for a sophisticated solution that integrates machine learning and multi-engine scanners with human analysis.

2. Postdelivery Detection: The most sophisticated anti-phishing strategy includes postdelivery detection that automates threat resolution right inside the user's inbox. With this approach, if an attack gets through the predelivery defenses and the employee submits the suspicious email for review, the postdelivery detection technology routes the email through machine learning filters and subjects it to expert human analysis automatically — without IT or user intervention.

A truly groundbreaking innovation, postdelivery detection can dramatically reduce vulnerability to data breaches. It's only possible with a threat mitigation solution that features a human layer of analysts to review and categorize email-borne attacks 24/7 to augment the work of advanced threat filtering engines.

3. Incident Response with Global Remediation: An advanced postdelivery detection solution can automatically quarantine, analyze and remove malicious emails from an employee's inbox. But a broader incident response capability is needed to reduce dwell time for email attacks and phishing threats since attacks often target multiple users. A 2018 Ponemon Institute study found that the current dwell time has actually increased to 197 days from 191 last year. The mean time to contain the threat is longer as well, rising to 69 days from 66. It takes organizations nearly nine months to mitigate risk and get back to business as usual. As timeframes extend, the damage and costs associated with breaches increase.

An advanced incident response capability reduces the odds that a malicious email will be clicked on or receive a response from an employee. Look for an incident response solution that automatically removes multiple instances of a targeted attack across an organization.

> ***"As attacks become more sophisticated, even email security gateways with advanced features find it impossible to detect threats 100 percent of the time. That's why a predelivery, postdelivery and incident response approach is a must."***
>
> ***IDC Technology Spotlight***

The time is now.
The traditional gateway is no longer enough. And Security Awareness Training relies too heavily on making each user an expert at recognizing advanced phishing techniques. Lastly, based on our research there appears to be an overconfidence on the part of IT professionals that they are sufficiently protected standing pat, which is clearly not the case. Protecting the inbox takes a defense-in-depth approach, and that starts by adding postdelivery detection and incident response capabilities on top of your email gateway. This approach will help you get the heightened risk of phishing attacks under control once and for all.

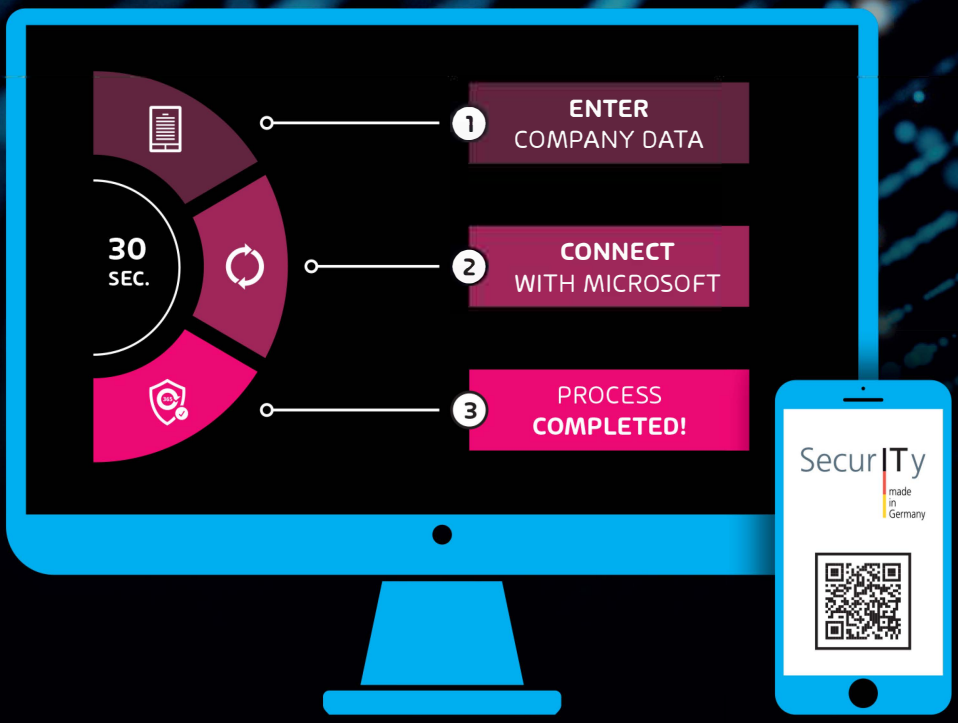
Mr. Randall brings over 25 years of cybersecurity and technology experience. As the Vice President of Product Management, Mr. Randall is responsible for developing both product innovations and solutions strategies to help EdgeWave customers protect their organizations from the latest security threats.
Mr. Randall brings deep technical and market expertise driven by his diverse background. His past experience includes roles as Director of IT providing internal security services as well as overseeing key relationships with multiple security vendors. Prior to joining EdgeWave, Mr. Randall has also held several leadership positions, most recently with Trustwave and Websense, across both Product Management and Product Marketing.



HORNETSECURITY

365 TOTAL PROTECTION

"SECURE YOUR **OFFICE 365 EMAILS** IN UNDER 3 MINUTES!"



365 TOTAL PROTECTION BUSINESS

- Email Live Tracking
- Infomail Handling
- Content Control
- Compliance Filter
- Threat Defense
- Outlook Black & Whitelisting
- Userbased Individual Signatures
- 1-Click Intelligent Ads
- Company Disclaimer
- Global S/MIME & PGP Encryption
- Secure Cipher Policy Control
- Secure Websafe
- Email Archiving
- 10-Year Email Retention
- eDiscovery
- Forensic Analyses

365 TOTAL PROTECTION ENTERPRISE

- ATP-Sandboxing
- URL Malware Control
- Global Security Dashboard
- Malware Ex-Post Alert
- Contingency Covering

Please visit us at **Booth #567-2** during the RSA Conference to learn more!

www.hornetsecurity.com/365

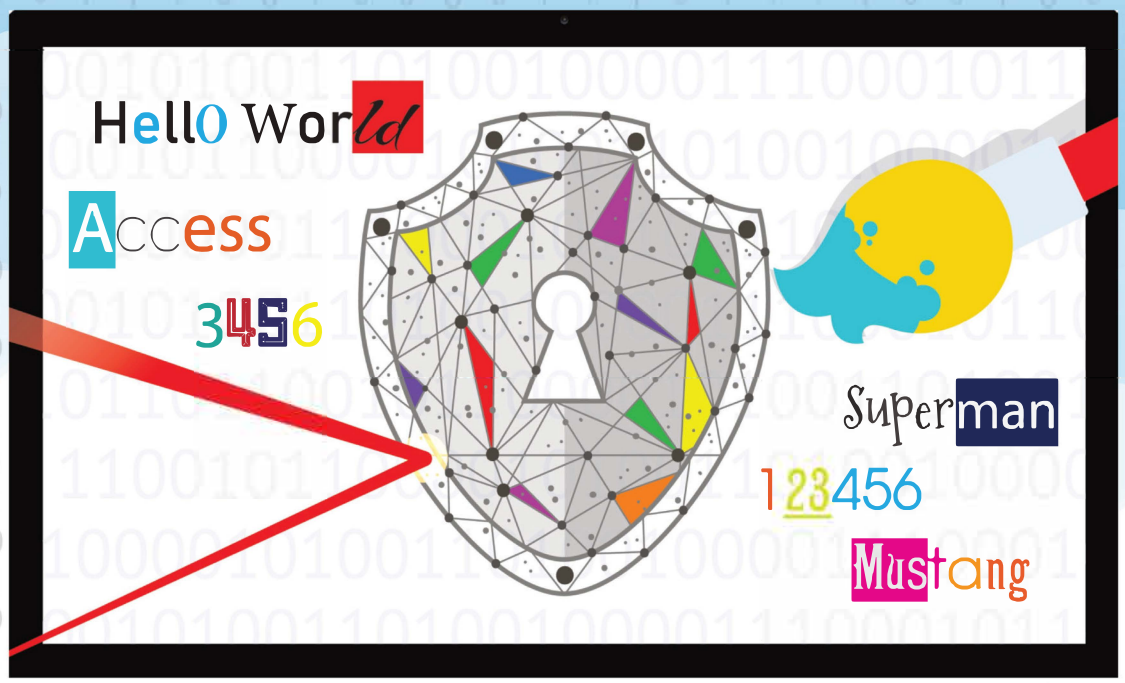


Rainbow Password, GEOACL LLC

Authentication, Verification & E-Signature

Future Password • Rainbow Password

Incredibly Strong Fights Password Attacks



Creativity for Credential strength, Patented Rainbow Password allows Font Color, Shading & Formatting options like Font Name, Size, Font Styles like bold, italic, underline & many more.

RAINBOW PASSWORD • RAINBOW PICTURE PASSWORD
RAINBOW PATTERN PASSWORD • RAINBOW VERIFICATION
RAINBOW E-SIGNATURE

For privileged, non privileged & all users using Mobile, Web or Desktop in Cloud, Sas, Banking, Payments, Pharma, Insurance, Healthcare, Realty and Government.

Subscribe Plans or License Technology

info@rainbowpassword.com
www.rainbowpassword.com



Zero Trust? Not if You're Surfing the Web...

Reshaping the Security Landscape
by Daniel Miller, Senior Director Product Marketing, Ericom Software

Though it may come off as a bit dramatic, the idea of not placing your faith in anyone or anything has become the new paradigm in security. In the past, we'd look at internal traffic as trusted and external traffic as untrusted. With the proliferation of insider threats and highly sophisticated malware, this notion is not only long outdated, but downright dangerous.

Zero Trust

The Zero Trust concept transforms the way modern security strategy is planned and executed. No security barrier, whether it's a physical appliance, a software product, or a cloud service, is regarded as safe enough on its own. No enterprise can be viewed as fortress, protected by its own perimeter defenses. No traffic is automatically "okay." Point-blank, organizations must stop trusting anything or anyone, inside or outside their network.

In the years since the Zero Trust concept was formulated, an explosion of new micro-segmentation solutions have been introduced to bring it from theory to practice. The thought behind micro-segmenting applications and environments is that to enforce security policies, organizations must be able to control what communication should — or should not — be allowed between various points on the network. To accomplish this goal, activities are broken down to the smallest processes and each one of those processes can be individually secured. Under the Zero Trust paradigm, machines, networks, and IP addresses are all segmented and access to each component, and between components, is restricted according to rigorously applied security policies and authentication.

Micro-segmentation is quite demanding. Within a true micro-segmented network, an IT team must manage large amounts of data processes across people, networks, devices, and workloads. One small misconfiguration can set organizations back a day's worth of productivity. Moreover, nuanced access and authentication processes can create a poor user experience and can further hinder productivity.
More significantly, while micro-segmentation and related solutions go a long way toward securing networks and data from everyone and everything, gaps still remain in truly locking down all traffic both within the network and from the outside.

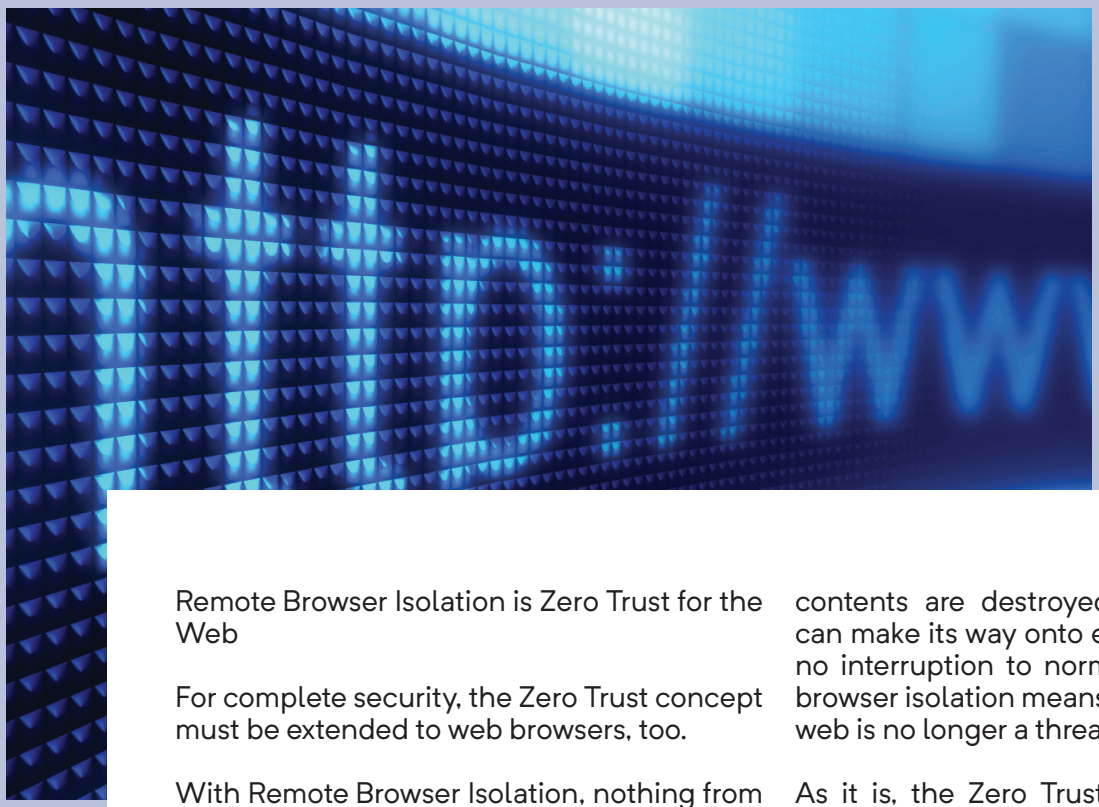


What About Web Browsing?

One of the main areas of risk not covered by micro-segmentation is web browsing. While essential in today's business environment, browsing remains a wide-open loophole through which malware can penetrate organizations. You can micro-segment to your heart's content, but it can't prevent browser-based malware, like many ransomware variants, cross-site scripting attacks and drive-by downloads from gaining a foothold in your network. Once malware bypasses that interface, it can make its way on to your endpoints and then onto your network.

Zero Trust advocates often cite whitelisting trusted sites as the solution, while denying access to all others. But time after time, it has been demonstrated that limiting access to all but known-to-be-needed sites kills productivity. This limited access creates hurdles for IT staff and end-users alike; users are forced to request and wait for access and IT staff must divert their attention from more strategic priorities to manage and grant access to such requests.

Moreover, even if organizations could whitelist every site their employees need, they would still be vulnerable to malware that infiltrates via legitimate sites. There is no way to know with certainty what's taking place behind the scenes on any given website, even one that has been whitelisted. There is always the chance that the site may have been infected with malware via "malvertising" campaigns — so although it's technically "trusted," it may still deliver malware to visitors. Even methods like URL filtering, anti-phishing lists, web gateways, and other types of filtering and screening solutions cannot hermetically block threats that originate from the web. Thus, the current Zero Trust model leaves room for browser-borne malware to infiltrate networks.



Remote Browser Isolation is Zero Trust for the Web

For complete security, the Zero Trust concept must be extended to web browsers, too.

With Remote Browser Isolation, nothing from the web is trusted. Every website, each piece of content, and all downloads are treated with the same extreme suspicion. There is no need for whitelisting or access requests and users can interact as normal with whatever sites they need.

All browsing takes place away from vulnerable assets, in a virtual disposable container which is located in a DMZ or in the cloud. Users get real-time access to websites and applications, free of any browser-based threats. When that tab is closed, the container and all its contents are destroyed. Nothing untrusted can make its way onto endpoints and there is no interruption to normal workflow. Remote browser isolation means that the whole of the web is no longer a threat to your organization.

As it is, the Zero Trust concept still leaves organizations at risk to browser-borne malware. While trusting "no one and nothing" is smart way forward in today's ever-changing and highly complex threat landscape, if this is to be the new paradigm there is little point in only adopting it part way. Remote browser isolation is the answer to taking Zero Trust to the next level in order to create a truly secure organization.

Daniel Miller is the Senior Director of Product Marketing at Ericom Software. He has more than 15 years of industry experience in corporate and product marketing, business development, and product management, supporting an array of technology services, hardware and software solutions—with a strong focus on cybersecurity in recent years. He frequently shares his insights on cybersecurity at industry conferences and podcasts, and regularly contributes articles to enterprise security publications. Daniel holds graduate degrees in Behavioral Sciences and Business Administration. Daniel can be reached online at daniel.miller@ericom. com and at company website https://www.ericom.com



CSIOS

2019
CAPABILITY STATEMENT



WHO WE ARE

CSIOS is a Maryland based Corporation certified as a **Veteran–Owned** and **Small Disadvantaged Business.**

WHAT WE DO

CSIOS provisions full spectrum **Cyberspace Operations** (*Defensive*, *Offensive*, and *Information Network Operations*) and **Cybersecurity** services to U.S. Federal customers worldwide.

WHY CSIOS CORPORATION

- The **ONLY** cyber firm with Cyberspace Operations and Cybersecurity services certified under **quadruple** ISO standards.
- Winner of Maryland's **2018 Cybersecurity Defender of the Year Award**.
- Winner of **2018 American Business Awards Information Technology Team of the Year Gold Stevie Award** (awarded to CSIOS Cyberspace Operations Team).
- Recognized by The Silicon Review Magazine as **One of 50 Most Valuable Brands of 2018**.

GENERAL INFORMATION

- **EIN No.:** 47–4147943
- **DUNS No.:** 079858391
- **CAGE Code:** 7GU86
- **NAICS Codes:** 541330, 541511, 541512, 541519, 541611, 541690
- **SIC Codes:** 7379, 7371, 8711, 8742, 8748

PREFERRED CONTRACT VEHICLE

GSA IT Schedule 70 Contract Number: GS35F657GA

- **SIN 132 51** *Information Technology Professional Services*
- **SIN 132 45A** *Penetration Testing*
- **SIN 132 45B** *Incident Response*
- **SIN 132 45C** *Cyber Hunt*
- **SIN 132 45D** *Risk and Vulnerability Assessments*

ISO CERTIFICATIONS

- **ISO 9001:2015** *Quality Management System* (No. C310-QMS135-12-17)
- **ISO/IEC 20000-1: 2011** *Information Technology Service Management System* (No. C313-SMS5-12-17)
- **ISO 22301: 2012** *Business Continuity Management System* (No. C312-BCMS6-12-17)
- **ISO/IEC 27001: 2013** *Information Security Management System* (No. C311-ISMS82-12-17)

SAMPLE CUSTOMER BASE

- **U.S. 24 Air Force** (*DOD Cybersecurity Service Provider*)
- **Office of the Secretary of Defense** (*Director, Operational Test and Evaluation*)
- **U.S. Army Research Laboratory** (*DOD Cybersecurity Service Provider*)

CONTACT

Mr. Cesar Pie, President and CEO
Cesar.Pie@csioscorp.com
(301) 752-2729

Dr. Edmund Mitchell
Chief Business Development Officer
Edmund.Mitchell@csioscorp.com
(803) 338-7295

ARL

INTEZER

GENETIC MALWARE ANALYSIS

Detect code reuse among files to:

1. Identify new forms of malware
2. Classify threats to their relevant malware families
3. Reduce false positives
4. Prioritize alerts according to risk and severity

Join our Community.
Try it now for free

intezer.com | @IntezerLabs

CSIOS Corporation: Scaling New Heights of Cybersecurity Services

By Cesar Pie, President and CEO of CSIOS Corporation

Home to the U.S. Cyber Command, the National Security Agency, the Defense Information Systems Agency, the National Institute of Standards and Technology, and many other cyber mission driven entities, the state of Maryland has quickly become the epicenter of the U.S. cybersecurity ecosystem. At the heart of the cyberspace domain, pumping needed products and services to U.S. Federal customers are several top notch cybersecurity firms looking to contribute towards building a safer and more secure future in the cyberspace domain—one of those firms is CSIOS Corporation. The Maryland—based veteran—owned and small—disadvantaged business provisions full—spectrum cyberspace operations and cybersecurity services to U.S. Federal customers worldwide. Its distinction: The firm's cyber services are certified under quadruple ISO certifications: ISO 9001:2015 (Quality Management System), ISO/IEC 20000—1: 2011 (Information Technology Service Management System), ISO 22301: 2012 (Business Continuity Management System), and ISO/IEC 27001: 2013 (Information Security Management System). Equally impressive is the one—of—a—kind scope of its accreditation: "The Provision of Cyberspace Operations (Defensive, Offensive, and Information Network Operations) and Cybersecurity services to U.S. Federal customers worldwide." No other company has achieved this service delivery level.

Due to the criticality and sensitivity of the U.S. government organizational missions it supports, CSIOS Corporation saw the need to formalize a process to continually assess and improve the cyberspace operations and cybersecurity services it provisions. In essence, in its pursuit of excellence and higher standards of cyber services to U.S. Federal customers, CSIOS baked—in its cyberspace operations and cybersecurity services with applicable Executive, National, and Federal cybersecurity requirements and overlaid four proven and globally recognized ISO standards for continuous improvement. The result: regulatory—compliant—and—mission—ready cyberspace operations and cybersecurity services capable to morph in accord with the differing attack—surfaces and operational threat environments and classification levels it supports.

By integrating a plan, do, check, act best practice approach, CSIOS has facilitated a continual assessment and improvement process that introduces, verifies, and validates needed process changes and corrective actions to maintain high level objectives of protection, monitoring, detection, analysis, diagnosis, and response. CSIOS' cost—effective and custom—tailored technical and non—technical solutions have helped its customers identify, prioritize, and defend their most important networks and data, so that they can operate within a degraded and disrupted cyber environment in the event that an attack on their networks and data succeeds, or if aspects of the critical infrastructure on which they rely for its operational and contingency plans are degraded or disrupted.

Through its unique cyber service delivery construct, CSIOS has been able to: identify more efficient, effective, and time—saving management processes; improve incident response times; and minimize disruptions to cybersecurity services—all while reducing operating costs and continuing to maintain compliance with customer's legislative and regulatory requirements. Equally important, as an organization, through its demonstrated accomplishment, CSIOS has reached new high levels of confidence when delivering its services. Simply put, CSIOS' attainment of quadruple ISO certifications has relayed a message of excellence to staff and stakeholders.

CSIOS' culture of top—service—delivery—levels and right—first—time approach has also instilled a higher degree of trust and credibility with and among its U.S. Government customers. CSIOS' customers have benefited from its improved quality and service, quality assurance, and always—on—time delivery. Overall, CSIOS continual assessment and improvement process has allowed the company to persistently introduce, verify, and validate needed process changes and corrective actions to maintain high—level objectives of availability, integrity, authentication, confidentiality, and non—repudiation.

As the only provider of cyber services with quadruple ISO standards, CSIOS has rapidly taken a leadership position in the cyber market becoming one of the preferred U.S. government choices and global leaders in provisioning cybersecurity services to multiple DOD Cybersecurity Service Providers (CSSPs) protecting and defending DOD information systems, networks, warfighters globally in more than 145 countries, 15,000 classified and unclassified networks, and 7 million computers and IT devices worldwide.

Year after year, the company has been scaling new heights of cybersecurity services and the unique level of cyber services provisioned by this veteran owned—small business is not going unnoticed—earlier this year, CSIOS was recipient of the Maryland's 2018 Cybersecurity Defender of the Year Award. CSIOS also landed a spot among the 50 Most Valuable Brands of the Year 2018 by "The Silicon Review" Magazine. Further, CSIOS Cyberspace Operations Team was named winner of a Gold Stevie® Award in the Information Technology Team of Year category in The 16th Annual 2018 American Business Awards®.

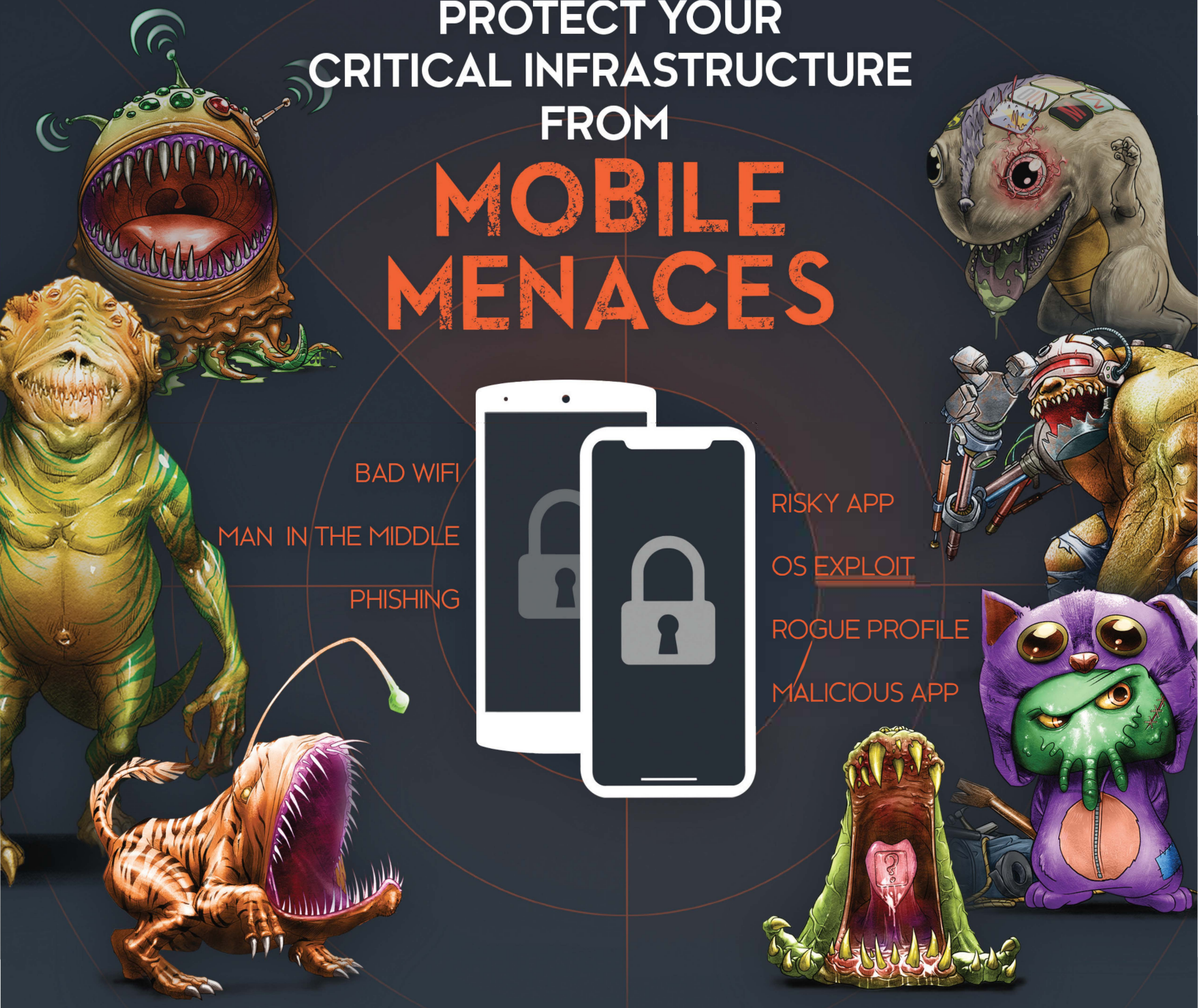
A veteran of the U.S. Marine Corps, Mr. Pie is an established corporate officer with a demonstrated record of success and unyielding commitment to teamwork, honesty, integrity, excellence, and dedication to employees and the U.S. Federal government customers he serves.

Mr. Pie was named CSIOS President and Chief Executive Officer in December 2015. Since, he has assumed executive oversight and day—to—day leadership of CSIOS.

Mr. Pie holds a Master of Science degree in Computer System Management and Information Assurance from the University of Maryland University College and a myriad of professional certifications to include Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Information Systems Security Engineering Professional (ISSEP), and Project Management Professional (PMP).



PROTECT YOUR CRITICAL INFRASTRUCTURE FROM MOBILE MENACES



When it comes to mobile security, what you can't see really can hurt you. In fact, there are mobile menaces creeping around your employees' devices right now just waiting to pounce. And when they do, you better be prepared!

Zimperium protects mobile data, apps and sessions against dangerous mobile menaces. To date, Zimperium has detected 100% of zero-day mobile exploits without requiring an update.

Visit www.zimperium.com to learn more.

ZIMPERIUM®
MOBILE THREAT DEFENSE



Fraud Protection and AI in the Financial Markets

The 'Black Box' Problem of AI

by Davide NG Fania, MD, XTN Cognitive Security

Powerful machine-learning techniques have taken the tech world by storm in recent years. AI-based technologies continue to improve and enhance processes in many fields of application, such as voice and image recognition, machine translation, medical diagnostics, customer interaction and even the way we buy and sell, particularly online.

Machine learning (ML) is a subfield of artificial intelligence (AI) interested in making systems autonomously learn how to perform tasks (based on examples, generally speaking – training datasets), and this has resulted in many people believing AI and ML are the same things. However, there is much more to AI than ML alone, just as there are many more aspects of biological intelligence than independent learning skills.

The financial market is one of the key industries expected to be thoroughly transformed by these technologies. Financial institutions are introducing AI into many areas, such as fraud analysis, loan related risk evaluation, and customer support relations. Having AI support existing processes can produce cost efficiencies combined with better and far more secure service experience for most users; however, new technological opportunities may be hindered by a significant problem. It's often impossible to explain how ML algorithms (for example deep learning) reached a confident decision. From a service provider perspective, being able to pinpoint the reason for an AI-driven decision is crucial. Furthermore, some regulatory agencies are turning their attention to algorithmic accountability; this is absolutely the case for GDPR (or PSD2 even if limited to the EU) where financial institutions are required to explain why a specific decision has been taken by one of their algorithms.

Comprehensively deploying AI into financial services environments requires keeping in mind intelligibility of results as part of the equation and approaching ML as always evaluating costs and benefits in solving specific problems. In the case of fraud protection, there are several areas of interest in applying AI technology to support human processes:

1. Behavioral analysis: many ML algorithms are very useful to detect patterns or anomalies through vast amounts of data (events, transactions) that allow rapid (or near real-time) recognition of typical behaviors and the identification of suspicious ones.
2. Digital identity validation: ML can be used to implement passive biometrics analysis. These techniques are used to identify users based on biometrics information coming from sensors (e.g., keyboard, mouse or smartphone embedded sensors). Thanks to these checks the end-user could benefit from having less identity-related challenges while accessing the service (no pin codes or 2FA, if not required).



3. Replicating human decision flow: AI can be used to substitute a human analyst evaluating a suspicious event. Training these ML algorithms can be done by feeding the system with actual decisions made by the analyst and then engaging the algorithm to continue the task autonomously. As previously mentioned, this is surely an area where the decision rationale needs to be crystal clear and tracked as part of the evaluation process.

To put this in a context in the real world, think about an end user that is unable to perform an ATM withdrawal, unable to access the online services or to use the mobile app due to some fraud protections restrictions, while the bank (usually help desk) is unable to explain why. Alternatively, think about a potential customer applying for a loan and being rejected without any understandable reason.

These scenarios could have serious impact to the financial institution's reputation (mobile app adoption and trust in the service) and produce damaging business impacts. In regulated markets, companies need to be able to explain both internally as well as to external parties (auditors and end-customers) why they're making decisions and above all for the right reasons.

There are open debates about the use of AI. For example, the AI Now Institute at NYU pressed the core social domains, such as those responsible for criminal justice, healthcare, welfare, and education, to halt black-box AIs because their decisions cannot be clearly explained. This situation is further exacerbated by business innovation because the majority of products and services of artificial intelligence companies use complex neural networks. Decisions are taken by a "black-box" solution, whose companies declare their algorithms a trade secret and typically do not disclose their operation, where even their designers cannot explain how they arrive at the answers.

Consider for a moment the rationale of why a hybrid approach should be used to comply especially in relation to the financial services market requirements. A modern working AI system often contains parts based on some symbolic, logic-based framework and elements based on ML. IBM's Watson is a typical example, as much as Google search engine whose search results are enriched by a knowledge base called Knowledge Graph.

ML is undoubtedly a good practice, but we do not consider it a silver bullet problem solver. In XTN we believe ML solves specific problems extremely well, but at the same time other issues can be better addressed with alternative approaches (for example rules-based or statistical models).

Being able to understand the decision of an AI system, avoiding the "all-black-box" approach, is one of our main goals. Using an extreme example, if a neural network is being used for medical diagnosis and comes up with a "you have cancer" result, you would absolutely want to know how it came up with that!

XTN provides products that can evaluate unusual events from the very beginning, starting from day one. Up and running ability is achieved thanks to the default training dataset that comes from our decades of expertise and experience in fraud prevention and protection. Over time our technology will always improve its ability and refine accuracy, but we'll still be watching the customer's back because our designers can surely explain how they get the answers, and that's what the market wants and more importantly, demands!

Especially in the financial industry, we believe the customer should always manage the countermeasure, the reaction could impact user experience and should be as limited as possible on the client side. We have designed our solutions to provide risk and behavioral evaluations to react dynamically modulating the service or activating awareness campaigns without impacting user experience. The service provider always has to be able to analyze the case, to understand the issue and eventually engage the end-user.

For this reason, we at XTN believe that using several ML algorithms (both supervised and unsupervised) to solve specific problems while maintaining visibility on partial results (i.e. detecting "anomalous behavior" due to a new attack scenario, typically a zero-day attack), and a rule-based last line of defense, is the best approach from the business standpoint. A holistic framework to consider fraud protection with a multi-channel and multi-layer approach we call Advanced Behavioral Fraud Prevention. This means the ability to benefit from AI power with a new generation of digital identification dynamic indicators (used to ensure digital users are who they say they are), providing superior protection using non-invasive frictionless solutions (specifically designed for every single endpoint).

By taking this approach you are able to trust the digital customer and protect the business, while granting an unparalleled result speed for real-time services, reducing false positives, time-consuming activities for fraud teams, and guaranteeing significant containment of management costs.

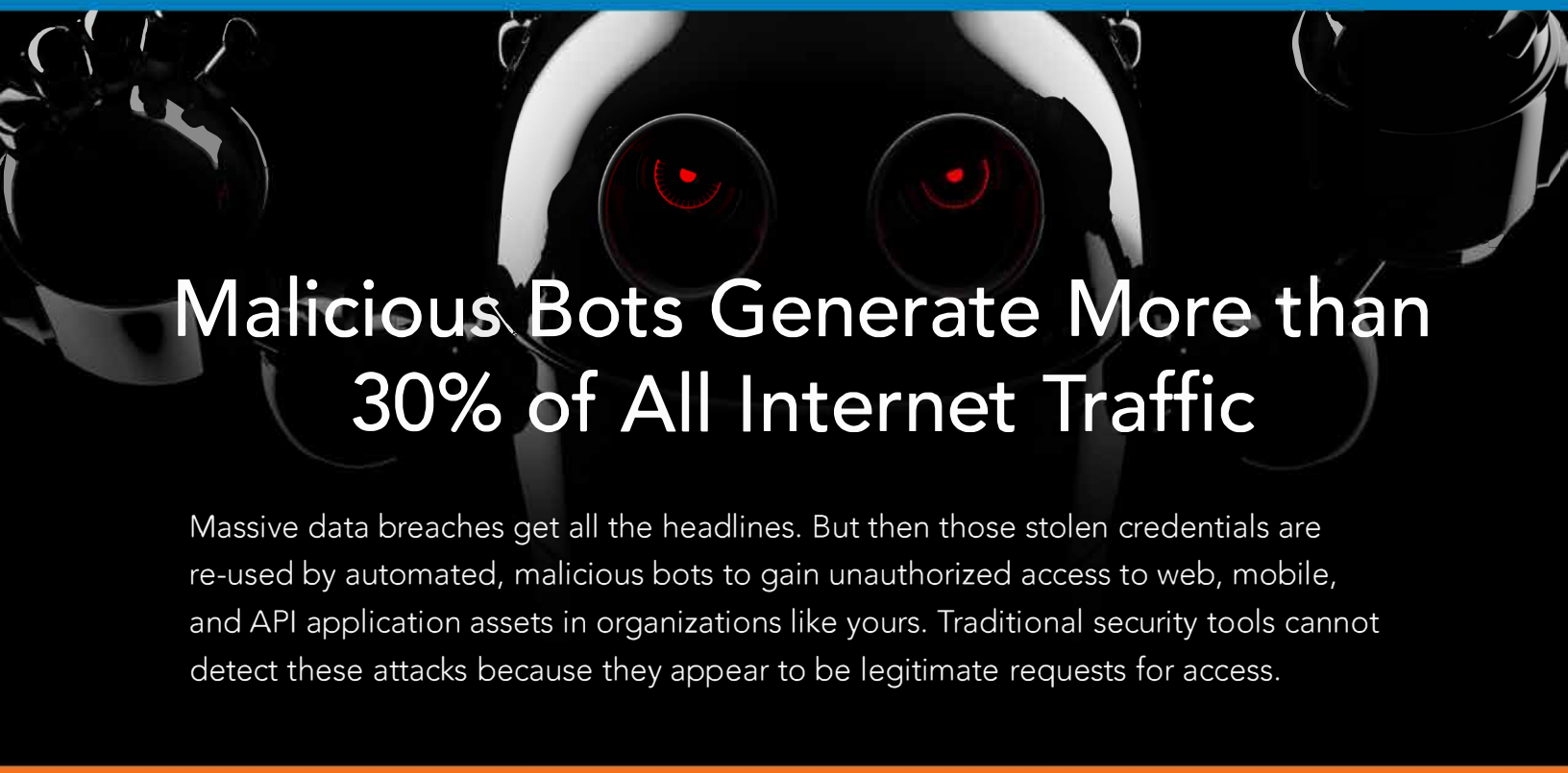
Davide NG Fania is the Managing Director of XTN Cognitive Security.

He's a manager with proven decades experience in the areas of Information Technology, Biomedical eMedical Devices Automation, and that bases its success stories on strong creativity to innovation and holistic view of the business, a supporter of the global market and strategic partnerships.

Davide can be reached online at linkedin.com/in/dngfania and at our company website https://www.xtn-lab.com



Cequence Security Stops the #1 Cyber Threat Facing Today's Digitally-Connected Organizations



Malicious Bots Generate More than 30% of All Internet Traffic

Massive data breaches get all the headlines. But then those stolen credentials are re-used by automated, malicious bots to gain unauthorized access to web, mobile, and API application assets in organizations like yours. Traditional security tools cannot detect these attacks because they appear to be legitimate requests for access.

How do you know if you're a target?

Assume you are if your organization has one or more of the following:

- **Web** – Externally-facing web pages that require an authorized username/password combination to access protected data
- **Mobile** – Applications deployed on smartphones and tablets used by customers to access their accounts
- **APIs** – Internal applications that connect with various partners and suppliers to allow the secure exchange of data

Cequence Security, recently named a Gartner Cool Vendor, protects organizations from these attacks with its innovative CQ botDefense software solution, powered by patented AI technology. It can be deployed on-premises or in the cloud and delivers three important benefits:

- **Automatically discovers all web, mobile, and API** application assets deployed across your organization
- **Automatically detects malicious bot attacks** that may be targeting your application infrastructure
- **Automatically stops these attacks** by creating rules that can be enforced by Cequence or your existing WAF

Gartner Cool Vendor 2018™

Learn more about how Cequence Security can protect your organization.
Visit us and request a demo at www.cequence.ai/demo

CEQUENCE™ SECURITY



Thanks to Human Expertise, Companies Are Stopping Phishing Attacks in Minutes

by Tonia Dudley, Security Solution Advisor, Cofense

In a recent 60 Minutes interview, Tesla founder Elon Musk said, "Humans are underrated." His company had just boosted production by creating an extra assembly line, a makeshift affair in a parking lot, powered by people more than machines.

The human factor made the critical difference. Which brings us to phishing attacks.

Companies are seeking faster, more efficient phishing response.
CofenseTM has spent years training users how to identify a malicious email, plus we've given them an "easy button" to report the message. But now what? We've overwhelmed our security operations teams with a flood of emails that contain anywhere from 10 to 15 percent of potential threats to the organization. And while it's true that our phishing defense solutions make use of automation, customers, prospects, and the marketplace at large are showing a keen interest in human expertise.

They mainly want results, of course—whatever stops phishing attacks in minutes, not hours or days, without blowing through human resources, time, or budget dollars. Following are two examples of how businesses are succeeding.



This company stopped a phishing attack in 19 minutes.

When they got an email from their CEO, employees of a leading healthcare company took heed. Except the CEO hadn't sent it. A crafty phisher had.

The email asked employees to click on a link, taking them to a website to confirm their agreement with a corporate policy. First, though, they had to login with their network credentials. The attacker aimed to harvest passwords, gain file system access, and reroute electronic payroll deposits.

And the attacker almost succeeded. Many employees took the bait. The email was extremely convincing, using the company's logo and echoing language from its website.

Fortunately, other employees remembered their security awareness training—the human factor at work on the front end of phishing defense—and reported the email within a minute of the attack.

Those reports went directly to the Cofense Phishing Defense Center (PDC), which provides 24/7 monitoring and response—the human factor on the back end, where response cues mitigation. The emails underwent automated analysis before being vetted by the PDC team. Within a couple of minutes, they verified the attack.

The attacker "had really done his homework," the healthcare company's VP of Information Security would later say. "The email looked and sounded exactly as though our CEO had sent it." It was a sophisticated twist on business email compromise (BEC), which according to the FBI defrauds businesses of over $12 billion annually.

A few more minutes ticked by, with more employees reporting the email. Using Cofense TriageTM—a platform that groups emails by malicious attributes and enables response to entire campaigns, versus numerous one-off responses—the PDC now had enough evidence to alert the customer.

After a quick consultation, the healthcare company blocked the phishing site and began mitigation. "We removed the email quickly," the VP of Information Security told us. "Once we contained the threat, we started on repair and recovery work, seeing who clicked and mitigating problems linked to their accounts."

He added, "All of this was the result of a single well-crafted phishing email. If we hadn't been prepared, the damage would have been worse."

Only 19 minutes elapsed from the moment the attacker struck to phishing response and mitigation. Thanks to a balance of man and machine, with humans providing insights automation can't, the company stopped an attempted breach before it could succeed, instead waiting weeks or months before the alarm bells rang.

Another company took just 10 minutes to block an active threat.

Our second example comes from another Cofense customer. Employees at a multinational company reported emails sent, allegedly, by a credit card provider. The email landed in hundreds of inboxes and, as in the previous example, used counterfeit branding so employees would drop their guard.

The email told recipients that the credit card company had noticed unusual "recent activities" in their accounts. It then instructed employees to click a link to a My Account page, where they could verify and protect their personal information. The landing page asked for a wealth of personal data: name, social security number, email address, and more.

This credential phish aimed to gather personal data, not company information, though armed with employee's personal details the attacker could have connected the dots and targeted the corporate network.

Using a similar blend of automation and human intuition, this company's incident responders were able to identify the threat and block the phishing domain—before a single employee entered data.

Automated email analysis and clustering sped the response, but human verification and decisions stopped the threat. This time, it took only 10 minutes to detect, respond, and mitigate. According to the SOC analyst who managed the response, previously the cycle would have taken days.

In the end, "set it and forget it" does help to block phishing attacks, but automation merely enables humans to do the job better. Conditioning employees to recognize and report phishing, plus equipping SOC teams to respond faster, is a more complete approach.

Threat actors constantly tune their attacks to evade the security controls organizations like yours deploy. Technologies like email gateways miss phishing attacks all the time. That means your people need to be your last line of defense, general users as well as incident responders. Again, Cofense is finding that more companies value human expertise, both the home-grown variety and the kind delivered in managed services.

If your organization needs help, don't just push a button. It's smart to count on humans with the smarts to work the machines.

Tonia Dudley joined Cofense in 2018 as Director, Security Solution Advisor. In this role, she focuses on phishing defense advocacy while demonstrating how Cofense solutions help organizations across the globe minimize the impact of attacks while reducing the cost of operations. Tonia evangelizes Cofense's approach to phishing defense and incident response to new and existing customers, prospects, and the information technology market through speaking engagements, publishing platforms and media opportunities. Tonia also advises Cofense product teams on specific customer and market-driven needs to help streamline product roadmaps and create Cofense's inaugural international customer advisory board.

With more than a decade of cybersecurity experience, Tonia has managed programs in cybersecurity incident response, security awareness, and IT compliance for large global organizations. Her diverse career includes 14 years in finance roles at a national automotive retail chain, transitioning into IT roles over the next 12 years for a global manufacturing enterprise where she developed an interest in Cybersecurity. In 2011, she began building a robust security awareness program to focus on behavior instead of compliance. She then moved into the Financial Services industry for 3 ½ years to build a security awareness program. While working in the financial services industry, she participated in a working group to assist small firms with implementing a cybersecurity program to protect their firms. She has spoken at several cybersecurity and industry conferences on building successful security awareness and phishing programs. Her anti-phishing training programs have received three awards.

Twitter: @_tdudley



HERJAVEC GROUP

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



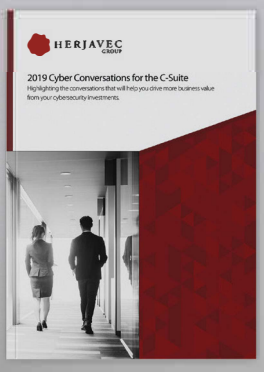
Robert Herjavec
Star of ABC's Shark Tank
CEO & Founder of Herjavec Group

Top Ranked MSSP & Global Cyber Operations Leader

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

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNER

- Security Company of the Year
- Identity and MSSP Leader



Drive More Business Value From Your Investments In Cybersecurity

Download HG's 2019 Cybersecurity Conversations for the C-Suite Report

HerjavecGroup.com

Why Major Data Breaches Will Continue in 2019

Confidential Database Data is at Risk to Data Theft by Hackers
by Randy Reiter, CEO, Sql Power Tools

Landscape: There have been a multitude of data breaches where hackers or rogue insiders have stolen confidential data over the past five years. In 2017, more than 1,500 data breaches were reported.

Equifax had the personal information stolen for 148 million customers in 2017. Most recently Marriott had the personal information exposed for up to 500 million people in 2018. Many other organizations have recently been hacked including LinkedIn, Anthem, Yahoo, British Airways, Target and Uber. In some instances, hackers were active over several months once inside the network. IBM's 2018 Cost of Data Breach study noted that companies took 197 days on average to identify a data breach and 69 days to contain it.

The financial impact to businesses is significant. According to IBM, the average cost of a US data breach in 2018 was $7.9 million with fines dwarfing initial costs. As an example, Uber paid a $148 million-dollar settlement in 2018 for concealing a 2016 data breach.

Executive leadership is also focused on the risks presented by cyber security weaknesses. A CEO of a large US bank recently stated that the three things that could destroy his bank overnight were data breaches, meteors, and nuclear weapons. In 2018, a US Senator proposed jailing execs for data breaches. Corporate boards are becoming increasingly involved as Gartner notes that by 2020 100% of large enterprises will be asked to report to their board of directors on cybersecurity and technology risk at least annually, up from 40% today.

Risks: Data has become increasingly important as currency for each company; it is critical to their day to day operations. This currency is stored in relational database systems such as DB2, Informix, Microsoft SQL Server, MySQL, PostgreSQL, Oracle and Sybase. This data has become increasingly at risk for three key reasons: 1) the security industry is largely focused on network-based security rather than on protecting the data stored within databases, 2) the movement of companies' infrastructure to Cloud, which creates a greater chance of data exposure to the public internet and 3) the mistakes of non-malicious employees whom Forrester research recently determined are responsible for 36% of all security breaches.



Current security software does not properly protect against the theft of confidential database data once the security perimeter has been penetrated. Once a rogue insider or hacker is inside the network, the theft of confidential database data is straightforward. Readily available vendor and public domain database utilities allow database data to be easily queried by hackers using a simple SQL database query.

An important solution to these types of security lapses is security software capable of detecting and stopping the theft of confidential database data from the inside out.

Background. Sql Power Tools has monitored the end-user response time of 10,000+ databases over the past several years using non-intrusive network sniffing technology. We have monitored everything from high volume online sports betting databases processing 15,000 SQL requests/sec to very large database servers having 64 CPUs servicing 20,000 concurrent online users. The usage of non-intrusive network sniffing has the advantage of having no impact on the database server plus allows for 100% of the database SQL query activity to be captured 7x24 for analysis.

What we have continually found over the years is that database activity is very predictable. Databases typically process a pattern of 2,000 to 20,000 SQL queries/requests that run millions of times a day. The key to detecting an intruder or possible data exfiltration from the inside is looking for abnormalities in these SQL queries.

What is needed. Security software that non-intrusively monitors the real-time database SQL activity using non-intrusive network sniffing and learns what the normal SQL activity is. Applying Advanced SQL Behavioral Analysis to the known SQL activity allows rogue SQL queries to be detected and shut down in a few seconds. This type of security software can be inexpensively run from network tap or proxy server so that there is no impact upon production servers. Consider the following SQL query of customer information. SELECT NAME, ADDRESS, PHONE_NO, SOCIAL_SECURITY_NO, CREDIT_CARD_NO FROM CUSTOMERS. It would be a very, very rare application that would query the entire CUSTOMERS table containing tens of millions of customers, yet most security software would be unaware that this differs from another more typical query.

The Advanced SQL Behavioral Analysis of the SQL query activity can go even further and learn the maximum amount of data queried plus the IP addresses all queries were submitted from for each of the unique SQL queries sent to a database. Security software containing this functionality can detect never before observed SQL query activity, SQL queries sent from a never observed IP addresses and SQL queries sending more data to an IP address than the query has ever sent before.

This type of important security software architecture/program can in real-time detect hackers, 3rd party cyber risks, SQL injection attacks and rogue insiders attempting to steal confidential database data. Once detected the security team can be immediately notified within a few seconds so that an embarrassing and possibly expensive data breach is prevented.

Conclusion. Data breaches will continue until organizations protect confidential database data from hackers and rogue insiders from the inside of the security perimeter using Advanced SQL Behavioral Analysis of the real-time database query and SQL activity. This will protect private and public sector confidential data in DB2, Informix, Microsoft SQL Server, MySQL, Oracle, PostgreSQL and Sybase databases.

Randy Reiter is the CEO of Sql Power Tools. He the architect of the Database Cyber Security Guard product, a database data breach detection and prevention product for DB2, Informix, Microsoft SQL Server, Oracle and Sybase databases. He has worked extensively over the past 25 years with real-time network sniffing and database security. Randy can be reached online at rreiter@sqlpower.com or at www.sqlpower.com/cyber-attacks.



DROP BY OUR BOOTHS @ RSA

WE'LL SHOW YOU HOW TO...

STOP PHISHING ATTACKS IN THEIR TRACKS

Phishing is the #1 way threat actors attempt breaches. And Cofense™ (formerly PhishMe) is the #1 provider of phishing defense solutions. We invented the phishing simulation industry and now help thousands of customers stop phishing attacks in minutes, not hours or days. Come see us at Booth #4436 (North Hall) or #1243 (South Hall) to learn about protection from the inbox to the SOC, from threat intelligence and awareness to response and mitigation. When malicious emails get past your perimeter—and they always will—be ready with the tools and expertise to stop them cold.

BOOTH #4436
NORTH HALL

BOOTH #1243
SOUTH HALL

COFENSE™



The Impact of the Marriott Breach and Chinese Mass Surveillance

Lessons Learned from the Recent Marriott Breach
by Richard Blech, Founder & CEO at Secure Channels Inc.

Marriott International, the world's largest hotel chain, recently announced a massive data breach. The information of upwards of 500 million Starwood Hotel guests was copied and removed. Investigators are pointing towards Chinese hackers, potentially ones working at the behest of the Chinese government. There's more information coming from the attack, but in these situations it's always worse than originally reported. The breach is a disastrous event for Marriott, as they will face regulatory fines, lawsuits and a branding hit.

In the Marriott case the extent of the breach was heightened by the resources of the hackers. A nation state such as China has access to the best tech and sophisticated hackers who work in concert to tackle tough jobs. The hackers took personally identifiable information and grabbed encrypted data. This points to their capabilities, as they were confident in their ability to de-crypt the data. They don't care about the encryption strength because they have the tools to break it. Marriott likely used outdated 128-bit encryption which is exploitable.

Reactive Cultures

Companies often view breaches with an air of "it won't happen to us." But then it does. The affected company then sends out communications about how they care about the customer and are doing everything they can to remedy future situations. Unfortunately, the damage is done. The information is out there.

Marriott responded by expressing its regrets. It also setup a website and call center for guests to ask questions about the breach and impact on their personal data. It's the logical response, but it's of course completely reactive. Companies holding personal data must act proactively in regards to their cyber defenses. We don't know the particulars of the Marriott's setup and system failures in terms of both their technology and the human element. They did not properly protect the most crucial data such as passports, credit cards, emails, among others.

Advanced Safeguards

Secure Channels Inc. is not the global panacea for such a sophisticated attack; however, our solutions are part of a strategy that can make a company's data a very undesirable target. We offer advanced encryption to protect sensitive information at all points. So from the database to the end point in the workflow, the data is deeply encrypted and features strong access controls to said data. It's encryption that's many factors more robust and efficient than 128-bit encryption that was used by Marriott.

The Secure Channels encryption protocol XOTIC is a patented software and hardware implementation of the multi-family symmetric block cipher cryptosystem. The XOTIC cryptosystem comprises two elements, a key generation scheme and an encryption primitive. The XOTIC cryptosystem employs digital techniques to ensure information confidentiality.

XOTIC offers improvements in security properties including system or user definable keyspace (for keyspace values comparable to standard symmetric block ciphers such as AES) size ranging from 256 bits to 130,000 bits without any compromise to performance or execution times. Encrypting a file with XOTIC adds no more than 5 bytes to the size of the original file regardless of the selected encryption strength.

XOTIC is applicable to any data type. It provides increased protection against both "brute force" attacks and any threats posed by advances in quantum computing. Improved encryption such as that offered through XOTIC would require a nation such as China many years or even centuries to break.

Large global companies must be in tune to the risks posed by sophisticated hacking groups. Ignoring the threats means the potential brand and compliance risks are too great. Stronger encryption, improving human cybersecurity processes, and other proactive responses are needed.

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



Database Cyber Security Guard

Prevents data theft by Hackers, Rogue Insiders, Phishing Email Attacks, 3rd Party Cyber Risks, Dev Ops Exploits and SQL Injection Attacks when the security perimeter has been penetrated.

Average data breach in US costs $7.3 million dollars. Would have immediately shutdown the Equifax and Marriott hackers.

- Product Features -

- **Detects Oracle, SQL Server, DB2, Informix and Sybase data theft within seconds and immediately shuts hackers down.**
- **Dashboard view of hacker activity over any time frame.**
- **View all suspicious hacker SQL activity and data theft.**
- **Runs from a network tap or proxy server for non-intrusive detection of Data Breaches. Has no impact on databases.**

Advanced SQL Behavioral Analysis of the SQL activity learns what the normal SQL/query patterns are and stops the theft of data.

www.sqlpower.com/cyber-attacks

www.securechannels.com

Protect Your Business, Protect Your Future!

Secure Channels provides innovative, effective security solutions designed to complement existing investments in security. Our products offer advanced data protection, adaptable encryption, authentication, enterprise confidentiality solutions and proximity-based monitoring and intelligence capabilities. We help you meet your security challenges.

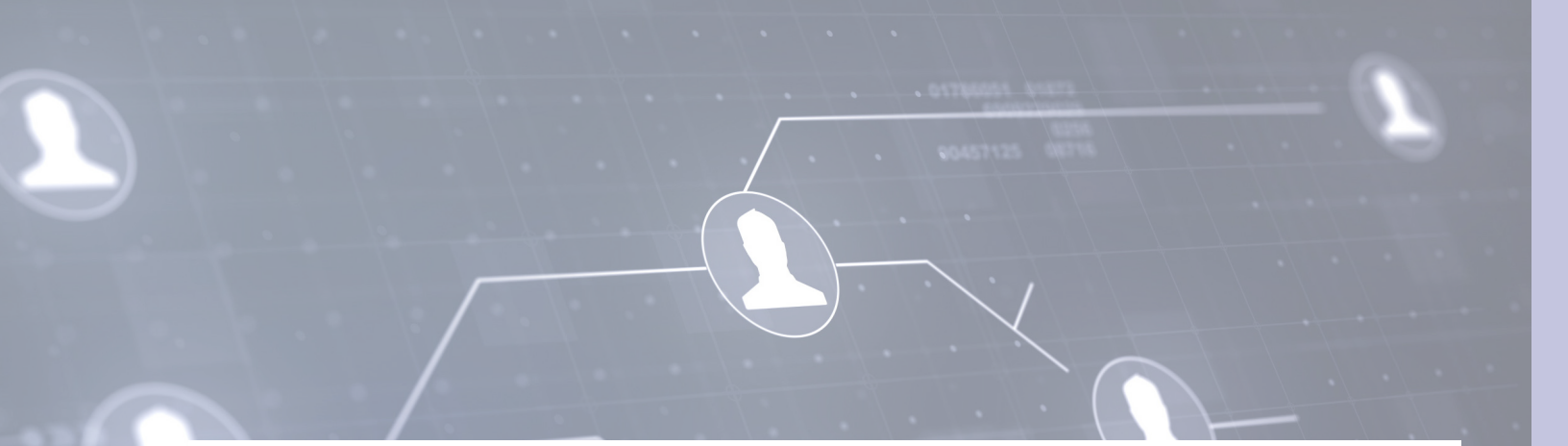
SECURE CHANNELS

QBOX: Quantum powered, portable, multiport data encryption transfer appliance offering exceptional speed and strength before data / media is moved to the Cloud

XFA MAIL: Next-generation, ultra-secure email solution with"one look" facial recognition for opening mail

SCIFCOM: Multi-platform, privileged access, Quantum-resistant Encryption-as-a-Service portal for emails, files, or bulk files

SECURE CHANNELS 16400 Bake Parkway, Irvine, CA 92614 / 949.679.5702



For better protection, stop buying security products

by Stan Black, Chief Security and Information Officer, Citrix

Do the security products you're buying make you feel any safer? Are you fundamentally improving your security posture, or are you still just one hacker innovation away from disaster? If only questions like these were harder to answer. In reality, the traditional approach to cybersecurity just doesn't work. Point solutions add complexity. Hackers will always move faster than their targets. Constantly-changing digital environments add potential vulnerabilities every day—and a single compromised app can bring your whole business to its knees. We can't keep using the same tired security strategy hoping to get different results. There has to be a better way to do this.

There is. Instead of throwing dozens of security products at thousands of individual apps and hoping for the best, we can take a better approach to cybersecurity. Make security frustrating for hackers—not users and IT

Traditional security takes a tool-by-tool approach to protection. Any user can tell you what this does to productivity; a high-friction security experience makes it harder to get work done at a time when innovation and agility have never been more critical for business success. The resulting patchwork security infrastructure also adds complexity and overhead for IT, slows threat detection, and makes it easier for attackers to find and exploit vulnerabilities.

Now consider a different approach. Instead of fighting a losing battle to protect thousands of apps one-by-one, what if you built security into your infrastructure as a whole? By changing the way services are delivered, you can get security out of users' way, simplify life for IT, and achieve a much smaller, more easily defended attack surface—no matter how much change digital transformation drives in your environment.

It's all about the pipes

One of the most appealing aspects of hacking is the huge return on effort you can achieve. With 1,000 — 3,500 apps running in the average organization, many of them lacking the latest security patches, it's never hard to find a soft target to exploit. Once you breach a single app, you're in—and you can roam the enterprise environment at will. Life is good.

Hacking would be a lot less fun and rewarding if a breach only affected that individual session. You might ruin that employee's day, but that's about it. For the rest of the organization, it's still business as usual.

To understand how this can work, think of how water delivery works. Everyone in the community shares the same water main. If there's a crack, everyone downstream gets dirty water. But what if we replaced that shared main with a dedicated pipe for each customer? Then a single pipe means a single person gets dirty water while everyone else is unaffected. It's a nuisance, not a community-wide crisis.

Now apply that model to the way we deliver IT services like apps, networking, and cloud. By giving each user their own dedicated, secure session—or pipe—we can limit the impact of a breach to that specific session and prevent it from spreading across the IT environment and organization. It's a simple concept: we define user identity by role, not device or location. That individual identity determines the set of services each user receives. Because identities and services are assigned individually, one user's compromised session can be terminated without affecting other users. It's a bad experience for one person—not the whole business. Two people, actually; the hacker will be pretty frustrated as well.

Keeping it simple

Remember, part of our goal is to make security both simpler and more effective. Shifting focus from apps to infrastructure does both. Instead of worrying about thousands of unique and diverse points of entry—your apps—you can focus on creating the best pipe possible, test it thoroughly, and then roll it out across your organization. As patches become available, a standardized pipe makes them easier to test before deployment; meanwhile, your individualized delivery infrastructure acts as a buffer to keep any breaches from infecting the whole network. That holistic approach means you're dealing with one delivery infrastructure, not a constantly-growing, ever-changing set of apps and services. And you don't have to worry about buying, configuring, and managing an endless stream of security point solutions.

It's not hard to make the change from app-centric security to a secure delivery infrastructure. First, make sure you have consistent visibility across your infrastructure, and take an inventory of the way services are delivered in your business. Then use this knowledge to figure out the best way to ensure end-to-end protection from services to user.

For too long, hackers have held structural advantages that make cybersecurity tenuous at best, as well as costly, labor-intensive, and frustrating for users and IT alike. It's time to stop playing this losing game of cat-and-mouse. By focusing on a secure delivery infrastructure, you can make breaches harder to accomplish, less rewarding for hackers, and less damaging for users and your business.

Stan Black, Citrix SVP, chief security and information officer

Stan Black, CISSP, is the SVP and Chief Security and Information Officer at Citrix where he is in charge of the secure delivery of applications and data. A key component of that is creating a security strategy to deliver experience, security and choice to customers and employees. That flexibility enables workers to be secure and productive from anywhere, anytime.

Black and his global technology and security team, a combination of security and IT teams, stop 54 billion attacks per quarter. His organization also monitors the global threat landscape and manages incident response and physical security to protect the safety of Citrix employees. Black is a seasoned security veteran with more than twenty five years of experience in cyber security, reducing business risk, threat intelligence, corporate data protection, infrastructure simplification and crisis management. His experience has provided him the opportunity to deliver durable security and risk solutions to global 1000's, countries and public agencies around the world.

Follow Stan on Twitter: @StanBlack19 or visit the Citrix website!



Don’t let your data end up in the wrong hands

Government certified, PIN activated, hardware encrypted data storage devices up to **14TB**



Without the **PIN**, there’s no way **IN**!



FIPS 140-2
Level 2 / Level 3

CESG Certified Product
Foundation Grade
HME1433053936-1257

Commercial Product Assurance (CPA)

NATO OTAN

NATO Restricted Level

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

Baseline Security Product Assessment (BSPA)

www.istorage-uk.com | info@istorage-uk.com | +44 (0) 20 8991 6260

iStorage®



Instead of just stopping threats, learn why human-centric security is not just the fastest way to proactively identify risk and protect your people, critical data, and networks —it's the only path to long-term success.

Forcepoint Speaking Session

Who Watches the Watchers: IP Protection for Privileged Users

- Dr. Richard Ford, Chief Scientist at Forcepoint
- Location: Moscone Center
- Wednesday, March 6 from 2:50 to 3:40 p.m.

It's time for **Human-centric Cybersecurity**

Visit us at RSA booth
N5969

FORCEPOINT

DLP | NGFW | Web | CASB | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email | Data Guard | Cross Domain

Attivo Networks and Deception Market Overview

Why Threat Deception Technology Adoption is Soaring
by Carolyn Crandall, Chief Deception Officer, Attivo Networks

Attivo Networks Company Profile:
Attivo Networks, an early innovator in commercial-grade threat deception technology, has seen growth soar as enterprise, midmarket, and government agencies rapidly adopt deception technology. Customers commonly cite that they have successfully reduced cybersecurity risks by closing detection gaps and reducing attack dwell time experienced when an adversary is able to bypass perimeter defenses. Attivo Networks leads in deception technology innovation and over the last 2 years has been recognized with over 70 awards for its products, leadership, and market impact. The company has also received elite recognition as a Cool Vendor by Gartner, Inc. and was recognized in 2018 as #31 on the Deloitte Technology ™ Fast 500 list, which recognizes companies for their growth, cutting edge technology, and ability to transform the way we do business.
Deception Market Profile:
Customers across all industries are deploying Attivo technology as part of their overall digital risk management strategies and for IT risk reduction related to detecting threats within cloud shared-security models, legacy and emerging technology environments, and to address today's threatscape in which attackers are using more targeted and sophisticated attack methods. It is forecasted that deception technology adoption will soar 684% in 2019 as it becomes a de facto security control for both enterprise and government entities. The breadth and depth of the Attivo Networks portfolio positions the company exceptionally well to address this growing market demand.
What Drives Attivo Deception Technology Adoption:
Unlike other security solutions, Attivo focuses on detecting the threats that have bypassed perimeter security controls, which all determined attackers eventually do. Highly authentic deception traps, along with data, application, and credential lures are deployed to attract an attacker into engaging and revealing their presence. This is quick, efficient, and customers have cited being able to detect and respond to threats in 15 minutes, a dramatic difference compared to the 100+ days of dwell time that many organizations contend with. The solution also adds continuous detection value throughout the phases of the kill chain.
Additionally, innovation continues to outpace security, as evidenced by IoT devices outnumbering humans and cloud deployments winning on economics over security. Industrial control and medical device technologies are now being connected to the internet with high vulnerability profiles and inadequate security controls, presenting tremendous risk to human safety. Deception technology provides continuous visibility into security control efficacy from legacy environments to the most modern attack surfaces. Lures will entice, and decoys will alert on attackers targeting these devices, mitigating risk within these inherently less secure environments.

Prior investments made for in-network threat detection have been historically low, driven by detection technologies that generated false alarms or were limited to only detecting known attacks. Attivo brings forward a different approach to detection, which provides tremendous value based on its ability to accurately detect threats, raise only high-fidelity substantiated alerts, and provide native integrations for automated incident response.

Deception technology provides organizations the ability to create a proactive defense against the adversary. This includes setting decoy landmines lying in wait for the attacker, proactive luring for revealing in-network attackers, and the ability to collect rich adversary intelligence that can be used to verify eradication of threats, mitigation of returning perpetrators, and fortifying overall defenses. DecoyDocs can also be insightful for understanding what an attacker is targeting and the geolocation of opened documents.

Attivo commercial-grade deception has removed prior scalability and operational management barriers that had limited the adoption of earlier deception technologies. The company's use of machine self-learning automates the preparation, deployment, and ongoing maintenance of the deception environment and the solution's flexible architecture makes deploying across datacenters, cloud, user networks, remote locations, and specialized networks quick and easy. It is now so simple that customers report that it takes less than 5% of one FTE's time to manage the Attivo deception platform.

It is notable that Gartner is recommending deception technology as a top 10 strategic technology trend for 2018 and views Attivo Networks as a market leader with the most mature and comprehensive portfolio.

Attivo ThreatDefend™ Deception and Response Solution:

The ThreatDefend™ Platform provides a powerful security control for early threat detection and for applying a proactive defense that can be used to change the asymmetry of an attack. As the most comprehensive and scalable platform on the market, Attivo dynamic traps, bait, and lures provide threat deception for today's evolving attack surfaces including networks, cloud, data centers, remote offices, and specialized environments such as IoT, medical IoT, ICS-SCADA, POS, infrastructure, and telecommunications. By creating attractive and believable decoys, the solution turns the network into a virtual "hall of mirrors," that disrupts an attacker's reality and imposes increased cost as they are forced to decipher real from fake. One small mistake will reveal the attacker's presence and force them to start over or abandon their efforts altogether. The ThreatDefend architectural approach also removes the debate of whether deception is best suited at the endpoint or within the network by providing both. Deployment at the endpoint and at the network level provides early and accurate detection of attacks from all threat vectors including reconnaissance, credential theft, Active Directory, and complex man-in-the-middle attacks. The company has also pioneered machine self-learning which automates the preparation, deployment, and maintenance of the deception environment. Ease of management combined with actionable high-fidelity alerts make the ThreatDefend solution simple for organizations of all sizes to operate, without the need for adding incremental resources.

Attivo ThreatDefend Solution Differentiation

Unlike traditional detection offerings, the ThreatDefend platform doesn't stop with detection alerts and goes further to provide organizations with tools for an Active Defense. Organizations also gain attacker threat intelligence for simplified incident response, threat hunting, and returning adversary risk mitigation. The ThreatDefend high-interaction attack analysis engine automatically correlates information, generates incident tracking reports along with insight into attack path and lateral movement. The collection of attacker TTPs, IOCs, and counterintelligence deliver invaluable intel into attacker capabilities, goals, and the information they are seeking to exfiltrate, which can be applied to stop perpetrators and to fortify defenses. The platform's extensive native 3rd-party integrations automate the sharing of IOC information, accelerate incident handling, and create repeatable incident response playbooks for efficiency in threat remediation.

Throughout history, deception has been used in military warfare, sports, and gambling to outsmart adversaries. Attivo Networks is now successfully applying threat deception in cybersecurity and empowering organizations of all sizes and industries to gain the upper hand against attackers. Please visit www.attivonetworks.com for more information or read the company blogs here.

Carolyn Crandall is the Chief Deception Officer/CMO of Attivo Networks. She is a technology executive with over 25 years of experience in building emerging technology markets in security, networking, and storage industries. She has a demonstrated track record of successfully taking companies from pre-IPO through to multi-billion-dollar sales and has held leadership positions at Cisco, Juniper Networks, Nimble Storage, Riverbed, and Seagate. Carolyn is recognized as a global thought leader in technology trends and for building strategies that connect technology with customers to solve difficult information technology challenges. Her current focus is on breach risk mitigation by teaching organizations how to shift from a prevention-based security infrastructure to one of an active security defense based on the adoption of deception-based technology.

As the Chief Deception Officer at Attivo Networks, she is an active evangelist on security innovation and speaker at CISO forums and industry events. She has been a guest on Fox News and has presented at the CSO50 Conference, ISSA International, NH-ISAC, ISMG Healthcare Summit, Santa Clara University, and on multiple technology education webinars. She is also an active blogger and byline contributor.

2018 Reboot Leadership Honoree (CIO/C-Suite): SC Media

2018 Marketing Hall of Femme Honoree: DMN

2018 Business Woman of the Year: CEO Today Magazine

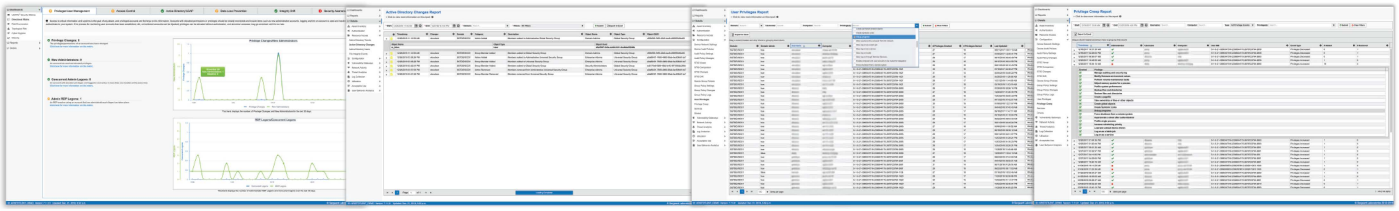
Power Woman: Everything Channel (CRN): 7 years

Carolyn Crandall can be reached online at (email: marketing@attivonetworks.com, Twitter: ctcrandall, LinkedIn: https://www.linkedin.com/in/cacrandall/ and at our company website http://www.attivonetworks.com/

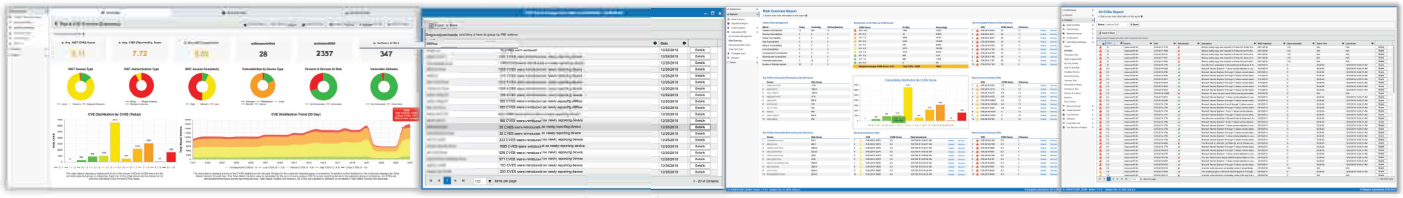


AristotleInsight® Cyber Diagnostics

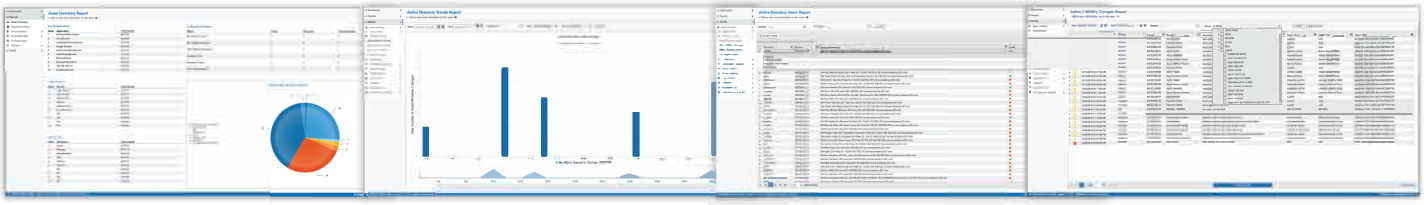
Configurations: Privilege Alert → Local Admin Creation → GPO Change → List of Machines by GPO → Admin Who Errored



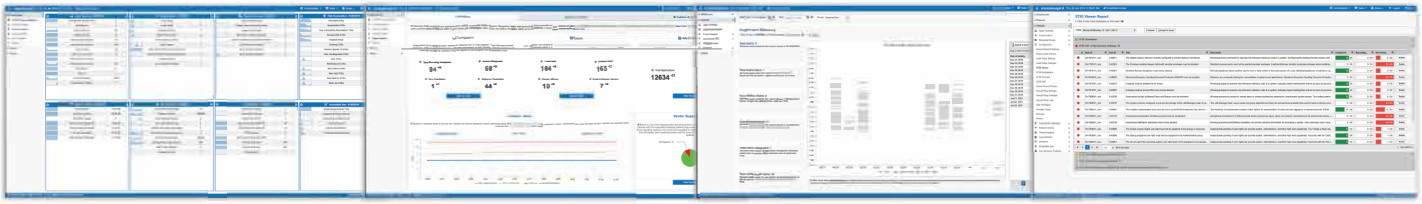
Data Loss Prevention: Data Alert → Gmail Identification → User Identification → Data



Privileged Users: Remote Access Alert → RDP/VPN → Determine Access Point → Audit History (down to keystrokes)



Drift: Drift Alert → Determine Configuration Changes → What Machines Changed → How Was it Changed → Determine if Exploited



Usable, Accessible, and Comprehensive

Our Integrated Visibility Platform, AristotleInsight,
collects and reports on vast amounts of data from Users, Devices, Applications, Processes, and Endpoints.
Revolutionary machine learning and UDAPE® technology continuously reduce noise and false positives.

RSA® Conference2019
San Francisco | March 4–8 | Moscone Center

Ask Us About DevOps
Booth #3114

www.AristotleInsight.com / 866-748-5227 / Info@AristotleInsight.com



Your selfie unlocks...

your rental	your password	your gig	your transaction

your digital identity.

Authentication simplified.

jumio.com/authentication

Five Things You Need to Know About Next-Gen Authentication

By Dana Tamir, VP Market Strategy at Silverfort

Currently four out of five breaches involve the use of compromised or weak credentials. Enforcing multi-factor authentication (MFA) has been proven as the most effective measure against these attacks. Yet mainstream MFA solutions, that were designed to be implemented for specific systems, make it difficult to protect many resources in today's complex and dynamic networks.

The next generation of authentication introduces a new approach to enable seamless MFA that can protect any organizational resource, no matter what it is, or where it is. It no longer requires deployment of software agents on protected systems, or proxies in the network, enabling organizations to protect any sensitive resource on-premises or in the cloud with a holistic adaptive authentication approach.

Here are five things you need to know about Next-Gen Authentication:

1. It's easier to deploy and maintain: Since it doesn't require deployment of software agents or network proxies, the deployment is very quick (typically hours) even in large complex networks. In addition, there is no need to patch or update agents on protected systems which minimizes ongoing maintenance.

2. It can protect systems you couldn't protect until today: Many sensitive systems aren't supported by mainstream MFA solutions including proprietary, homegrown and legacy systems, IoT and critical infrastructure. With an agentless, proxy-less approach, for the first time it's possible to protect these systems without any special or costly customizations.

3. It unifies protection across on-premises and cloud environments: The holistic nature of the agentless approach enables you to unify MFA management and consolidate auditing across all sensitive systems, regardless of their location.

4. It continuously adapts to risk levels: By continuously monitoring and analyzing all access requests, across on-premises and cloud environments, it leverages an advanced AI-Driven risk-engine to dynamically calculate the most accurate risk-score per user, device and resource, and can automatically step-up authentication requirements when risk levels are high.

5. It improves security while reducing disruptions: Until now, threats detected by security solutions weren't blocked because false-positive alerts could result in unwanted disruptions to legitimate users. Next generation authentication enables you to trigger step-up authentication in response to detected threats, allowing legitimate users to authenticate and continue working while blocking true-positives.

With identity-based attacks on the rise, can you afford to leave your mission critical resources unprotected? Next-Gen Authentication opens a new chapter in enterprise security, offering organizations a new way to protect more systems than ever before, with less effort and disruptions.

Dana Tamir, VP Market Strategy at Silverfort



YScanner Web Application Scan

YOUNKER

Protect your cloud assets

Built on cloud-based security and compliance platform, YScanner keeps you away from substantial cost, excessive resources, sudden deployment issues. Upon unique methodology, fast deployment, ease of use and maintenance, plus incomparable scalability, it ensures organizations are capable of securing web applications and keeping attackers at bay.



YScanner is a professional scanning suite for web application vulnerability detection, fully supports OWASP Top 10 detections, based on lasted browser engine technology and powerful crawlers, excellent detection algorithms, with higher detection rate plus FP rate being effectively suppressed. Being developed and optimized on Linux, it demonstrates the innate high performance and large concurrency, especially is skillfully to dig out hidden storage XSS flaw which listed into second XSS flaw in OWASP Top 10. YScanner has been successfully supplied to market, and stands the test of time, runs effectively and steadily with limited supports, or even maintenance-free.

Key Features

Comprehensive discovery

WAS engine enable users to discover and catalogue all applications in their network, especially for those new and unknow ones, that scale from a few to thousands. Furthermore, you also can tag applications with your own pre-defined labels leveraged by reporting and access controlling on scanned data.

Deep scanning

Dynamic and deep scanning effectively detects all apps on the perimeter of production or ever-changing R&D environment. It sheds a new light to unknown web vulnerabilities, such as SQL injection and XSS, etc., as an enhancement and advantage, authenticated, complicated and progressive scans is fully supported

Probe zero-day threats via behavioral analysis

YScanner is adapt to open source software and custom-built applications, approach the topmost level detection rate on critical vulnerabilities. Good at unique behavioral technology, it can quickly and effectively identify and alert 0-days.

Disclose vulnerabilities and misconfigurations

Adhering to professional and distinct observation methodology to sites, customer can be targeted to and focused on vulnerabilities and misconfigurations due to human errors, poor coding, especially hidden faulty hardening policy.

www.yscanner.com email:service@yscanner.com

Alibaba Cloud | H3C | QINGCLOUD



Unlocking Your Users' Digital Identities with a Selfie

by Dean Nicolls, VP of Marketing, Jumio

In the world of digital identity verification, there are two distinct realms: the realm of identity proofing and the realm of authentication. These realms have been separate and distinct for decades.

Companies use a variety of identity proofing techniques to remotely establish the identities of users (instead of requiring them to visit a branch office). As more people use the internet and apps on their computers, tablets and smartphones to create accounts online and access those services, modern enterprises are exploring online ways to "identity proof" new customers without requiring an in-person visit.

Identity Proofing Methods

Historically, the function of "identity proofing" was based on the premise that if a person was able to provide a name, address, date of birth and a government identifier (e.g., Social Security number), he or she must be that person. This was never very sound, but it was deemed "good enough."

When this approach proved insufficient, knowledge-based verification was introduced. This prompted a user to answer questions based on more extensive public records or credit history. This also proved problematic as legitimate customers frequently failed these questions, and it introduced a high rate of friction and abandonment.

More recently, enterprises are starting to require that new online customers capture a picture of their government-issued ID (drivers license, passport or ID card) and a selfie with their smartphone or webcam, and then compare the face in the selfie to the picture on the ID.



Authentication Methods

After the user is approved and given their account credentials, they need to authenticate themselves every time they log into their online accounts. In most cases, all that's needed is a simple username and password. But, in some situations, businesses need higher levels of assurance to ensure that the person making the request is who they claim to be. These include:

- Logging in from a foreign IP address
- Password resets (in light of account takeovers)
- Large money or wire transfers
- Multiple unsuccessful logins
- Requested change on authorized permissions
- High-risk transactions (car rentals, hotel room keys)

For these types of transactions, companies use a variety of authentication technologies including:

- Knowledge-based authentication
- Multi-factor authentication
- Out of band authentication (e.g., SMS-based codes sent to the user's smartphone)
- Hardware and software tokens

A New Paradigm for Identity Proofing and Authentication

Unfortunately, there's very little overlap between the technologies used for identity proofing and the technologies used for authentication. Making matters worse, many of these traditional forms of identity proofing and authentication have proven to be hackable, insecure and unreliable thanks to large-scale data breaches, the dark web and man-in-the-middle exploits.

This is both unfortunate and inefficient.



A Better Way: Jumio Authentication

"By 2023, identity corroboration hubs will displace existing authentication platforms in over 50% of large and global enterprises." - Gartner

There is a better way that leverages the same set of technologies for both identity proofing and authentication that's fast, reliable and easy to use. It leverages face-based biometrics and liveness detection — here's how it works.

Step 1: Identity Proofing

A new user goes through a simple two-step process when creating an online account:

1. Government-Issued ID: The user captures a photo of their government-issued ID via their smartphone or computer's webcam.
2. Selfie Capture and Liveness Detection: The user is asked to capture two selfies: one about 12 inches away and another closer up, around 6 inches from the smartphone. The check for liveness detection is to ensure that the person behind the enrollment is physically present and to thwart fraudsters who are increasingly using spoofing attacks by using a photo, video or a different substitute for an authorized person's face to acquire someone else's privileges or access rights

In addition to checking the authenticity of the ID document, the 3D selfie is compared to a government-issued ID to reliably establish the digital identity of the new user. This simple and increasingly familiar process provides businesses with a higher level of identity assurance.

Step 2: Authentication

The real breakthrough happens downstream when authentication is required. Because a 3D selfie was captured at initial enrollment, the user only needs to take a fresh selfie (one close up and one a little further away). This new 3D selfie is then compared to the original selfie captured during enrollment and a match/no match decision is made. But, this time, the authentication step takes just seconds to perform. The elegance of this solution is that the user does not need to be subjected to the entire identity proofing process again — they just need to take a new selfie.

Emerging Use Cases

By using your users' selfies as their second authentication factor, organizations can now envision entirely new use cases that go well beyond suspicious logins.

- Hotel Room Access: Instead of waiting in a long check-in line at a hotel, customers could open their doors with just a selfie.
- Car Rentals: Customers could bypass the long lines at airports and unlock the door of their rental car with just a selfie.
- Lost Passwords: Instead of reverting to vulnerable methods, such as KBA or two-factor authentication, companies reissue lost or forgotten credentials by having their users take a selfie.
- High-Risk Transactions: If there's a significant wire transfer from one account to another, financial institutions could simply require the user to take a selfie to authorize the transaction.
- Continuous Authentication: Think about continuous authentication in the e-learning space. Professors want to ensure that legitimate students are enrolled online and that they are the same people taking the exams online. Think about the need to identity proof Uber drivers upfront, but also to continually re-authenticate them on the job to ensure that the person claiming to be the Uber driver is, in fact, the Uber driver that was approved to drive.

As identity proofing and authentication processes converge, we think the role of face-based biometrics will enable broader adoption, provide higher levels of identity assurance, improve the customer experience and conversion rates, and better protect online accounts from identity theft and account takeover.

Dean Nicolls is Jumio's most recent addition to the executive team. He has 25+ years experience in B2B marketing focusing on cloud services. These include roles at Starbucks, Microsoft and variety of early stage cloud-based security companies including LiveOffice (acquired by Symantec), TeleSign (acquired by BICS) and, most recently, Infrascale. At Jumio, Dean is responsible for all branding, PR/analyst relations, product messaging, demand generation, and sales/channel enablement. He holds a Bachelor of Science degree in Business Administration from Pepperdine University and an MBA from the University of Washington.

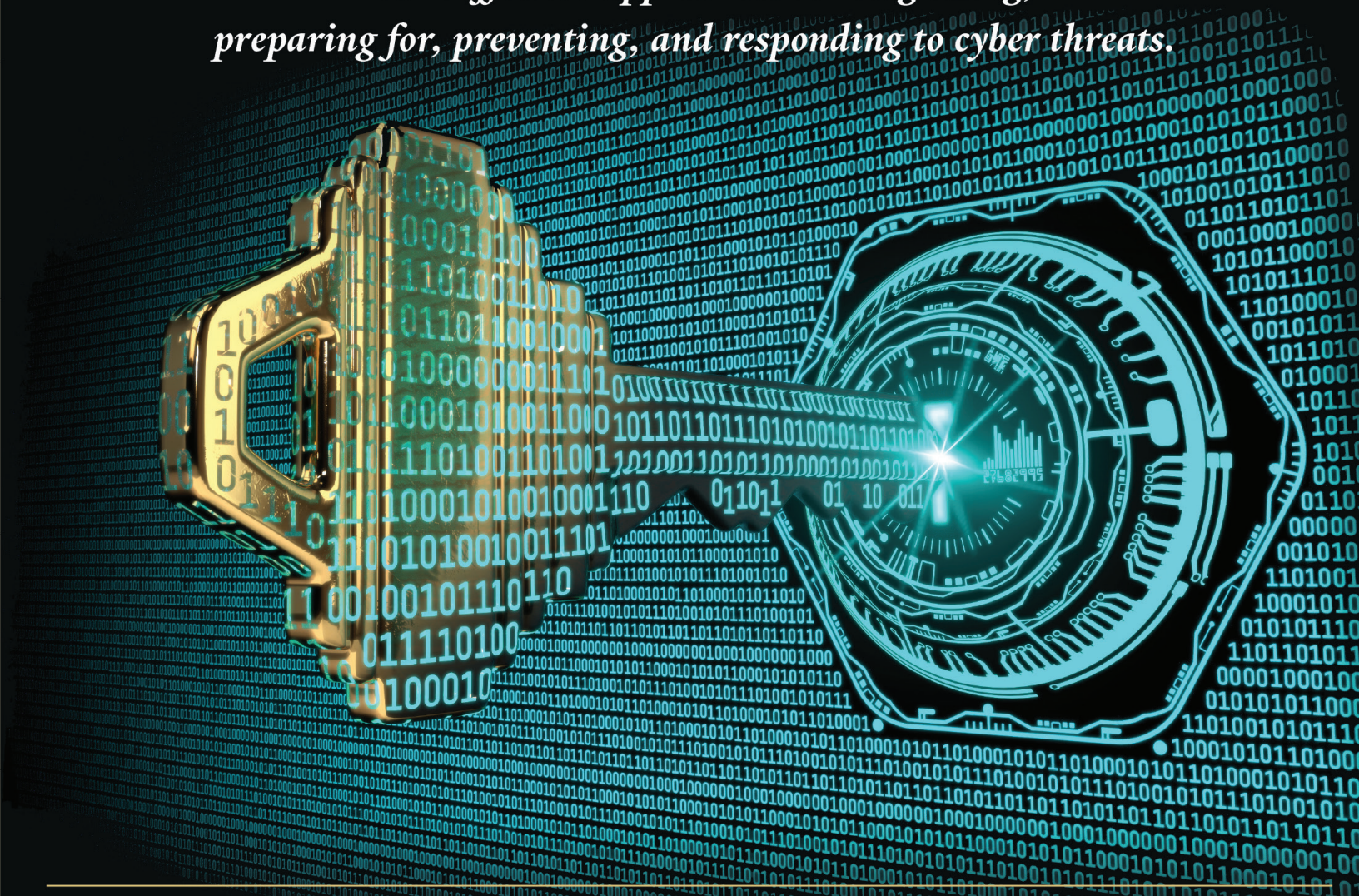


YALE CYBER LEADERSHIP FORUM

THE LAW, TECHNOLOGY, AND BUSINESS OF CYBER SECURITY

Yale University • New Haven, Connecticut

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



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

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

Scholarships and discounts are available for a limited time, each year.

Learn more at:

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

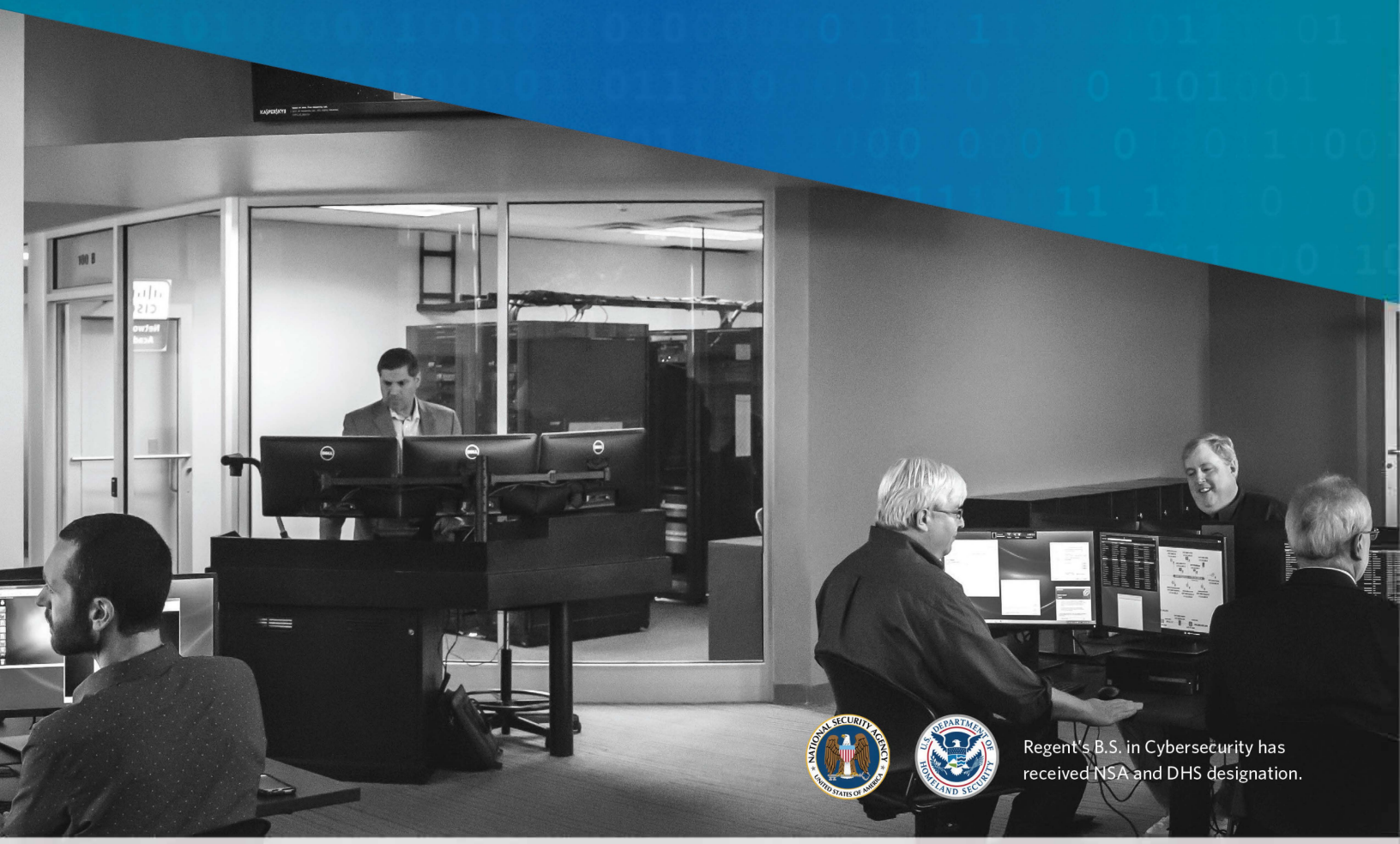
Setting the Standard

in Cyber Defense Training & Education

Partner with Regent's Institute for Cybersecurity to develop your workforce credentials, manage your cyber risks and defend your assets. We'll help you disrupt and transform your cyber defense capabilities.

CORPORATE | GOVERNMENT | MILITARY | EDUCATION

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



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

Customize Your Experience Today

regent.edu/cyber | 757.352.4590

REGENT UNIVERSITY | Institute for Cybersecurity



What do Organizations Need to Build a Security Minded Culture?

by Larry Cates, President and CEO, Global Learning Systems

As many organizations struggle with ongoing phishing attacks, data breaches and lapses in physical security, they continue to wonder why employees are making poor security decisions despite the availability of training. The answer is that merely offering security training once or twice a year doesn't build the habits, mindset and motivation needed for employees to care about protecting the organization.

Instead of offering "check the box" training, organizations of all sizes should look at continuous learning programs that focus on building users' ownership and responsibility for safeguarding the organization's data and IT assets. That sense of ownership and responsibility is one component of a security-minded organizational culture.

At its simplest level, organizational culture is the sum of everything that affects what and how things get done in the business, including: organizational strategy; the behavior of leaders and how well they communicate their vision; and the values, attitudes and behaviors of employees. A strong organizational culture is rarely an accident — it's pursued intentionally and cultivated with purpose.

Security culture focuses on the shared recognition that security issues are an integral part of every employee's job. It fosters practicing good security habits and rewards security-minded decisions. Security culture is about instilling patterns of behaviors, values, attitudes and beliefs that support protecting organizational assets.

At its foundation, any thriving culture relies on behaviors. For a security culture, individuals must adopt the behaviors that protect the organization and learn specific skills that enable them to make smart security decisions. Once a baseline of skills has been achieved in security, phishing and compliance topics, a training program can dive more deeply into areas that target specific roles or pertain to a particular industry.

For a security culture to take hold, there need to be structures within the organization to support it. These structures include:

- Established avenues for two-way communication
- Regular review and maintenance of policies and procedures
- Strong IT infrastructure to automate security whenever possible
- Visible leadership by example
- Integration of security into organizational goals
- Employee performance objectives that include security practices

To be successful, a security awareness program should take a multifaceted, phased approach to changing behavior by using communication, training and assessments. When done properly, a continuous security awareness program helps build and maintain security culture by educating and motivating the individual, while also engaging the organization in dialogue, establishing norms and appealing to the natural human need to conform socially.



Larry Cates is the President and CEO of Global Learning Systems, a leading provider of security awareness and compliance training solutions for organizations of all sizes. Larry advises and consults with GLS customers on the design and implementation of continuous learning and behavior management programs. Prior to joining GLS, Larry held executive positions in corporate finance, development and operations w ith leading national homebuilders. He is a former US Marine Corps officer and a graduate of the United States Naval Academy.

Larry can be reached at lcates@globallearningsystems.com and at our company website, globallearningsystems.com



Attivo
NETWORKS

What's Lurking in Your Network?

Malware, advanced threats, and malicious insiders are evading your prevention and traditional detection systems. The Attivo Networks® ThreatDefend™ Platform unmasks attackers with deception-based detection that efficiently deceives attackers into revealing themselves and provides evidence-based alerts to accelerate incident response.

attivonetworks.com



O2, Ericsson, and Equifax: How Certificate Expirations Led to Some of the Largest IT System Failures of the Last Two Years

By Tim Callan, Senior Fellow, Sectigo

Our modern IT landscape depends fundamentally on digital certificates. Certificates are nearly ubiquitous in contemporary computing systems and permeate every aspect of our digital lives. They are essential to the secure functioning of our business processes, communication, retail purchasing, utilities, transportation systems, personal electronics, and so much more. Virtually no digital process or device would securely operate without the use of certificates.

Each certificate authenticates the identity of a machine, device, or software operation to ensure that only the intended connections are occurring, and most systems won't enable encryption unless certificates are available. This latter fact is because encryption on its own does not constitute protection if the encrypted information might wind up in the hands of the wrong party.

Certificates must be issued by a Certificate Authority (or CA), which is the trusted authority for identity on that particular network. For internal uses like IoT networks or enterprise device certificates, the company that owns the devices can be the Certificate Authority. But for the public internet (including use for web sites, server-to-server connections, or email) certificates need to come from a public CA that has roots universally trusted by the systems on the internet.

With so much depending on certificates, it may not be surprising that an unexpected expiration can cause an application to stop working or security to lapse. in fact, it was revealed in December that the expiration of two certificates disrupted the lives of hundreds of millions of people. Early in the month, mobile service outage for tens of millions of customers using O2, Softbank, and other services ultimately owed itself to the expiration of a certificate that was part of the backend data service Ericsson provided to mobile service providers around the world. And then the following week, the House Oversight Committee released its report on 2017's Equifax data breach.

December's mobile outage affected carriers in eleven countries for as long as a day. The consequences to the carriers were huge. O2 gave all affected customers a credit worth two days of their data plans. Softbank experienced this outage a day before its IPO — a tremendous black eye exactly when the technology giant was looking for investor confidence. And it is reported that O2 could penalize Ericsson up to $100 million for failure to meet its SLA.

The Equifax breach, among the largest thefts of PII in history, involved the loss of 148 million people's data; nearly 45% of the US population. The thieves sat inside Equifax's infrastructure and harvested data on 265 occasions during the course of roughly 70 days. This extended attack was possible due to a lapse in service from a data exfiltration monitoring tool set up to guard against this kind of theft, and that tool's failure to operate owed itself to an expired certificate. It turns out this service was offline for an astounding 19 months and that the certificate in question was one of at least 324 expired certificates operating in the Equifax infrastructure.

So how did these errors happen? Certificate management is a tricky business. All certificates have expiration dates to ensure they are current, and these expirations are indispensable to the security certificates provide. That means administrators must track and renew certificates to prevent expirations form creating the kind of errors described above.

This administration has always been a headache; one that only gets worse as the scope and complexity of the enterprise's digital applications and computing ecosystems continue to increase. Virtualization, containerization, public and private cloud, and "software-defined everything" just add to the complexity of what must be managed. Furthermore, as centralized IT breaks down into embedded functions within lines of business using DevOps methodologies, it becomes harder and harder to even know the full set of certificates running in the enterprise's systems. Even the most diligent network administrator can be caught unaware of previously unknown certificates.

Automated monitoring and replacement of certificates is essential for protecting against unexpected expirations. Such a system can make administrators aware of upcoming expirations and can take hassle and error out of lifecycle management and renewal for all certificates in an environment. These benefits only apply to certificates that are under management, of course, so a certificate discovery system is a key component of the successful enterprise certificate management strategy.

A certificate discovery system crawls the organization's network and catalogs all certificates it finds. Discovered certificates are now available for monitoring and automated replacement just as any other certificate. Some IT organizations build certificate automation functionality for themselves, and some employ third-party certificate management platforms to handle these needs for them.

By using software to automate the discovery, lifecycle management, and renewal of certificates, IT departments can vastly mitigate the risk of expiration-based outages, potentially saving their companies embarrassment, customer service problems, lost revenue, data loss, and even millions of dollars in financial penalties. All enterprises should be evaluating how to put automated certificate management.

As Senior Fellow, Tim Callan contributes to Sectigo's standards and practices effort, industry relations, product roadmap, and go-to-market strategy. Tim has two decades of experience in the SSL and PKI sectors, and has served extensively as a strategic marketing and product leader for successful B2B software and SaaS companies. A security blogger since 2006, he is a frequently published author of technology articles and has spoken at many conferences including the RSA Security Expo, ClickZ, Search Engine Strategies, Shop.org, and the Internet Retailer Conference and Expo.

Tim Callan can be reached online at tim.callan@sectigo.com, on Twitter @TimCallan, and at www.sectigo.com





More than 100 top-notch experts from over 30 countries participated in ISC, made their debuts in Asia and delivered inspiring speeches

OFFICIAL REGISTRATION AT



"To Be or Not To Be": Here's How SMBs Can Affordably Protect Themselves

aiMSSP Enables Managed Security Service Providers to Deliver Comprehensive, Affordable, Integrated Security Services to Small-to-Medium Businesses and Enterprises

by Arun Gandhi, Director of Product Management, Seceon

Today threat surfaces have broaden significantly and security teams have to defend against sophisticated cyber-attacks, such as, Ransomware, Distributed Denial of Service (DDOS), Inside threats, Vulnerability exploits, Advanced Persistent Threats (APTs), Email phishing, to list few. Cybercrime is developing much faster than security tools, adoption and proliferation of Internet of Things (IoT) increasing the risk of a breach, and cloud and virtualization trends are set to be main pain points for organizations in three years' time. Many small-to-medium businesses (SMBs) and enterprises think they're flying under the radar of cyber-attackers. But the reality is very different. Perpetrators specifically target smaller, more vulnerable businesses because of their lack of security expertise and fragile infrastructure, and because they often provide easy entryways to larger companies with whom the SMBs work. Empirical data shows SMBs have high security-related risks that can be extremely detrimental to their existence, compared to larger organizations. According to Hiscox's Cyber Preparedness Report 2017, small businesses lose an average of $41,000 per cybersecurity incident. They are the hardest hit most often, although their breaches may not make headline news. More alarmingly, over 60 percent of the SMB enterprises go out of business within six months of devastating cyberattacks.

SMBs typically have a shoe string IT & security budget and very limited expertise with cutting-edge tools. Therefore they must lean on Managed Security Service Providers (MSSPs) to help them attain a shield of protection that small-to-medium businesses need for their very existence. MSSPs offer superior protection, cost savings, customer support, advanced technology to the SMBs without the need of making significant investments, and enables businesses to focus on their core competency to increase their bottom-line. Key MSSP services include:

- Outsourced, advanced-tier 24x7 monitoring of security events and management. This is a cost-effective alternative to having dedicated in-house staff managing security events.
- Deep threat intelligence covering a wider security landscape, such as device management, breach monitoring, data loss prevention, insider threat detection, phishing attacks, web exploits, and more.
- Incident response to contain and eliminate cyber threats in near real-time and keep your business running.

- Flexibility of deployment. The MSSP's services should be available over the Internet, via on-premise systems that are managed remotely, or through a hybrid model. SMBs may choose to implement some security capabilities in-house alongside other services from their trusted MSSP.
- Consulting on industry specific requirements and know-how pertaining to your business. This helps the MSSP implement best-practice processes and the right technologies for you.

The Seceon Approach to Empower and Elevate the Managed Service Providers

Seceon® aiMSSP empowers managed security service providers the ability to address a wide range of client cybersecurity requirements at speed and scale, delivering data protection and differentiated services on their path to profitability. It enables MSSPs to deliver comprehensive, affordable security services to enterprises and SMBs and maximize revenue-generating opportunities for providers. MSSPs can now provide radically new managed Internet security services to SMBs, Enterprises, and other smaller MSSPs as a master MSSP, which transcends and outperforms traditional SIEM solutions, delivering the functionality of SOC at a fraction of the cost. Seceon's innovative aiMSSP solution combines the benefits of SIEM and MDR, and dramatically extends defense-in-depth approach for businesses of all sizes, from the micro-SMB to Enterprise.



Key benefits include:

- Reduces Mean-Time-to-Identify (MTTI) and Mean-Time-To-Response (MTTR) with automated, real-time detection and response (viz-à-viz, 24x7 SOC Monitoring and Threat Management) focusing on known and unknown "threats-that-matter".
- Enables organizations to achieve continuous regulatory compliance with continuous monitoring and reporting.
- Decreases CAPEX/OPEX significantly.
- Empowers SOC analysts to become more efficient.
- Flexible and Scalable Deployment

aiMSSP is built on a Big/Fast Data Architecture with Machine Learning and AI as its cornerstones. It performs large-scale, robust data collection from cloud and other modern IT data sources to provide organizational wide situational visibility, incorporates threat intelligence feeds for correlation and enrichment, provides continuous learning about normal network activities via machine learning and enhanced data analytics beyond rules, and uses advanced Artificial Intelligence for actionable remediation. According to Grigoriy Millis, Chief Technology Officer of Richard Fleischman & Associates, "RFA is currently processing over 700 million events per day. On average, Seceon aiMSSP solution generates 20-25 alerts per day with less than 1% of false positive. Also, quite often it isn't really a false positive as it is the activity that is being flagged. It has also increased the efficiency of our IT and SOC personnel by 37%"

	On-Premise Model (Hosted by SMEs)		MSSP Model	
Internal Support Staff 1	At least 5 for 24x7 operations	Min. $1M (fully loaded)	MSSP staffs shared across customers. Seceon aiMSSP scales to 1000's of customers	$10K/Year –$300K/ Year based on number of employees or assets
Software Tools 2	Multiple tools needed (for e.g., SIEM,	In excess of $500K	MSSP's goes with Seceon aiMSSP and scales to 1000's of customers using 5–6 staffs	$0
Facilities 2	Space and utility charges	Min. $25,000	Outsourced to MSSPs	$0
Total		Min. $1.53M / Year		$10K –$300K/Year

1 – Assuming salary of one person to be $200,000 per annum (fully loaded)
2 – These are estimated charges

In this digital era, where cyber-attacks happen at all times around the world, security breaches can be devastating to a small business that has significant resource constraints. Cyber-attacks, such as, Ransomware, DDOS, point-of-sale malware, etc., specifically target smaller, more vulnerable businesses with a lack of security expertise and fragile infrastructure leading to a huge payout for the attackers. MSSPs are an increasingly popular choice for SMBs who need a simple, cost-effective solution for cyber threat protection that leverages the latest innovations and provides 24x7 access to security experts. MSSPs are a great resource for either supplementing your existing security team or starting your security practice. aiMSSP enables service providers to deliver affordable, reliable, differentiated security services that protect SMBs and enterprises. It empowers MSSPs to address a wide range of customer's security requirements related to protection and compliance at speed and scale, and enables them to create revenue-generating services for providers.

Arun Gandhi is the Director of Product Management of the Seceon. He has more than 17 years of experience with startups and global brands and his experience includes product management, business strategy, high profile customer engagements, product marketing, sales enablement, positioning of emerging technologies, strategic analysis, development & test for security, networking, and cloud technologies in the Service Provider and Enterprise Markets. At Seceon, he is responsible for driving strategic go-to-market initiatives, positioning, product roadmap, and executive engagements with customers & partners. Prior to Seceon, Arun held various technical and leadership roles in Product Management, Strategy, Marketing and Engineering at Juniper Networks, NetBrain Technologies, and Misys Plc (now Finastra). Arun can be reached online at arun.gandhi@seceon.com and at our company website http://www.seceon.com/



Best Certificate Management and Device Security for Enterprises

SECTIGO

FORMERLY COMODO CA

20+
years of experience in digital trust solutions

#1
market leader in commercial SSL certificates

100M +
Certificates issues. Critical to businesses worldwide

Industry best 99.9% trust recognition from browsers

Used by over
700,000
businesses worldwide

35%
Fortune 1,000 companies use our solutions

Visit RSA Booth #2333
March 4-8 | San Francisco



FRONTLINE DEFENSE AGAINST CYBERWAR:

Educate End Users

Mison Riggins, Cybersecurity SME / Tech Writer, Inspired eLearning

We hear of nuclear, religious, and political wars on the news every day; however, news of the raging cyberwar is becoming more prevalent. Since it is waged on the invisible battle lines of cyberspace, the average end user has no idea that there is even a war going on much less how to protect themselves. The main frontline defense strategy against this all-pervasive war is to go beyond just security awareness: To educate, train, and equip end users with the knowledge and skills to defend themselves and their organizations' networks.

UNDERSTANDING THE THREATS WE FACE

Social engineering, phishing, and adware are all methods attackers use to try to trick us into giving them information to launch further attacks. Not only are we faced with targeted social engineering and phishing attacks, but we are also bombarded with faceless attacks by bots through social media, click baits, laced ads, fake apps, and so on.

By gaining admin login credentials through social engineering, attackers do not have to go out of their way to hide their tracks. They already have easy access into a company's network that traces back to an official admin user. Depending on the end goal, this could be a one-time hack attempt, but often, it is an initial access point to install a backdoor. When the "cyber battle" commences at a later date, the information gleaned through this backdoor and will have given an "enemy" considerable advantage. In general, regardless of position, best security practices dictate that these administrator permissions should only be granted on a needs basis. "Admin Rights" is like having the combination, key, and palm scan to open the vault at the National Security Bank. You do not hand the keys to the kingdom to just anyone. Since executives are especially targeted, they also need cyber security training and restricted "needs only" access.

Moreover, we have already witnessed weaponized social media attempts with Russian military operatives assuming fake identities and trolling 126 million Americans through

Facebook to influence political votes. Singer (2018) goes on to describe the "combined tentacles of Russia's massive online army" as being made up of four groups:

- Thousands of sock-puppet accounts, where Russian human agents pose as trusted commentators and online friends.
- Tens of thousands of automated bots manipulating search algorithms to drive overall online trends.
- Legions of "fellow travelers" driven by partisan reasons planted inside the target countries.
- A plethora of "useful idiots" who echo out propaganda and disinformation.

How do we as organizations fight against cyberwarfare tactics? How do we equip our end users with the defense mechanisms against an attack?

CULTIVATING A SECURITY- CONSCIOUS SOCIETY

Organizations can install the best security devices and products, but it all boils down to the end user's ability to recognize and thwart threats. "All security products are only as secure as the people who configure and maintain them" (Vacca 2017). Only end users can learn to avoid the pitfalls of drive-by downloads, clickbait, and targeted phishing attacks. Only end users can employ security strategies to help protect their own as well as their organizations' digital assets.

By raising our collective "cyber-maturity" level, we can stand on the frontlines of defense against the cyberwar that is an invisible tangled web around us. It starts with the individual—we must evoke a change in our very mindset concerning cybersecurity. Dr. Eric Cole, renown online security expert and "cyber ninja," points out that we as Internet users must take responsibility for our own protection by implementing security if we want to win in cyberspace (2018, Ch. 1).

Cybersecurity is not just for conglomerates or the government. Access to Internet-capable devices is starting at earlier age groups, so the importance of security and secure online practices must be ingrained at every age level from the primary school student to the boardroom executive. We need to dispel the mystery shrouding the inner workings of the digital age so that we can protect our private data, our homes, and our workplaces. In short, we need to cultivate a security-conscious society.

BUILDING A CYBERSECURITY TRAINING PROGRAM

Organizations can kick-start this movement by mandating their employees at all levels to attend regular workshops and online training sessions. Additionally, CEOs and CISOs should be encouraged to invest in cybersecurity training for their employees. Meaningful and relevant training will make a lasting impact. "If you do it correctly, user awareness training can go a long way in educating employees on why security is important and what they can do to help resolve the problem" (Cole 2018).

So, what can we do to protect our digital assets from the threats of cyberwarfare? The first line of defense is educating end users with cybersecurity learning solutions. Then, end users can gain knowledge and skills to recognize hidden threats and wade through the "landmines" of malicious links and manipulations of social engineering attempts. We need to cultivate a cybersecurity-conscious society with lessons that also include the benefits of hardening systems and other security measures we can implement to protect the integrity and availability of our digital assets.

The bottom line: All the security products in the world cannot work effectively without proper configurations and maintenance by end users. Therefore, education and training to build a security-conscious society is one of the key layers of a well-rounded defense strategy.

WORKS CITED

Cole, Eric. 2018. Online Danger: How to Protect Yourself and Your Loved Ones From the Evil Side of the Internet. New York, New York: Morgan James Publishing. Accessed March 19, 2018.

Singer, Peter W. 2018. "The 2018 State of the Digital Union: The Seven Deadly Sins of Cyber Security We Must Face." War on the Rocks. January 30. Accessed February 20, 2018.

https://warontherocks.com/2018/01/2018-state- digital-union-seven-deadly-sins-cyber-security-must-face/.

Vacca, John R., ed. 2017. Computer and Information Security Handbook, Third Edition. 3. Cambridge, MA: Morgan Kaufmann. Accessed February 20, 2018.
https://www.elsevier.com/books-and-journals/book- companion/9780128038437.

Weise, Elizabeth. 2017. "Russian Fake Accounts Showed Posts to 126 Million Facebook Users." USA Today. November 1. Accessed February 20, 2018.

https://www.usatoday.com/story/tech/2017/10/30/russian-fake-accounts-showed- posts-126-million-facebook-users/815342001/.



Mison Riggins, with certifications in CHFI and SSCP, is a Tech writer by day and a slayer of cyber security ignorance by night. Her contributions span from the engineering department to the content development house for Inspired eLearning, a leading provider of the most effective Security Awareness eLearning solutions.

Mison can be reached online at mison.riggins@inspiredelearning.com and at our company website https://www.inspiredelearning.com/

Global Learning Systems

Global Learning Systems provides security awareness and compliance training programs that promote behavior change, protect your organization and

STRENGTHEN YOUR HUMAN FIREWALL®

1-866-245-5224

www.globallearningsystems.com

Recognized for four consecutive years in the Gartner Magic Quadrant for Security Awareness Computer-Based Training

Contact us today, or visit us at RSA, booth 3304 to discuss your security awareness training needs.

©2019 Global Learning Systems, LLC. | All rights reserved.
Strengthen Your Human Firewall and SecureGenius are registered trademarks; GLS OnDemand Learning Management System and Human Firewall 2.0 are trademarks of Global Learning Systems, LLC. PhishTrain and all other trademarks are property of their respective owners.



Attacked on All Sides

Why Enterprise Businesses Must Evolve from Controls-Based Approach to a Cybersecurity Ecosystem.

by Otavio Freire
CTO & Co-Founder, SafeGuard Cyber

If you work in information and cyber security, you could be forgiven for a lack of sleep in 2018. Last year felt like a daily parade of headlines about massive data breaches and ever more complex hacks. Facebook, LinkedIn, Quora, Marriot, to name just a few. Not only are the breaches growing in number and in scope and sophistication, but the attack vectors are multiplying as new technologies are adopted: social media, email, cloud applications, and so on. This has always been the Sisyphean task of information security: find a vulnerability, find a fix. These fixes are focused on controls. Over time, this controls-based approach has led to a patchwork defense that is wholly unprepared for today's more sophisticated attacks. Here's a typical list of capabilities most CISOs must account for:

- Network
- Firewall
- In-line
- Endpoint
- CASB
- Insider Threats
- IAM
- MDM

Now add to this list, Digital Risk Protection; a solution to monitor and secure all of the digital channels that are now critical front office operations but sit outside a company's perimeter: social media, mobile chat, collaboration platforms, and enterprise cloud applications.

So, how long will the list be in five years? The patchwork defense is outdated. Today's attacks are more sophisticated and multi-channel. A bad actor can build a relationship with your employees on Facebook while they're at home, and then phish them through LinkedIn at work. Or, an attacker might not even have to go after your employees directly. Thinking back to 2018, the four hacks listed above comprised more than 816 million records! At this rate, bad actors can simply collect data from existing breaches to correlate PII and identify the easy targets in your company.

The time has come to move away from the patchwork model and think of your organization's cybersecurity as an ecosystem. Move away from focusing on controls to looking at the full picture of the threat landscape. Partners and resources should work harmoniously by either integrating easily with your SIEM or enhancing workflows between different teams to take action in real time. For example, new threats, like brand impersonation or bot campaigns that spread disinformation about your brand are not direct attacks on network infrastructure. Who will address the threat, marketing or IT? State actors, hacker groups, and criminals are constantly innovating their attack strategies. Security teams must meet the challenge with innovation in technology as well as thinking. If your enterprise strategy is predicated on acquiring controls as threats arise, you're only applying patches. Instead, look to build a system comprised of best of breed capabilities for greater resilience in today's risk landscape.

Otavio Freire, CTO & Co-Founder.

Mr. Freire is a Brazilian-born American entrepreneur and inventor. He guides the development and innovations within SafeGuard Cyber's enterprise platform that empowers clients to impact their sales, marketing and business efforts via better cyber protection in social and digital channels. Mr. Freire has extensive experience in company strategy and R&D, product development, business development and engineering for cyber and risk based scalable platforms. He brings rich experience in social media applications, internet commerce and information technology serving the pharmaceutical, financial services, high-tech and government verticals.



IS YOUR SECURITY AWARENESS TRAINING PREPARING YOU FOR

THE GOOD, THE BAD, AND THE PHISHY?

Stop by our Booth at **RSA #4234** and join us for a special Booth **Happy Hour Tuesday, March 5th 4-6pm.**

1.800.631.2078 inspiredelearning.com

inspired eLearning®

THE PHISH



THE VISH



THE SMISH



THE USB



High-Level Strategies for Third-Party Risk Mitigation

By Phil Won, Product Manager, Owl Cyber Defense

High-Level Strategies for Third-Party Risk Mitigation
There are so many technologies and strategies and buzz words around cybersecurity these days that it can be difficult to know where to start. It's hard enough thinking about the myriad threats that can find their way into your organization without even broaching the subject of third-parties and trusted connections. However, there are a few fundamental, high-level strategies to consider applying in your third-party risk mitigation plan. They can be used individually or in tandem to create a strong cybersecurity framework for your organization.

• Defense in Depth
The primary principle of defense in depth is to build layers of security into your organization's digital architecture, so that if one layer fails, there will be others to back it up and maintain security. It is essentially a "fail-safe" strategy that assumes threats will most likely eventually find a way through one or two layers of defense (a safe assumption in most cases). There are no limits to the types of security involved, just those that best fit your organization. Role-based access controls, authentication, data encryption/tokenization, firewalls, data diodes, SIEM, and other technologies can all be used together to create a sophisticated, hardened defense.
• Risk-Based Security
Assuming that threats will eventually breach your network's defenses (you may be sensing a theme), a risk-based strategy applies more security resources to your most sensitive assets while less resources are applied to the lower risk assets. Risk-based strategies also typically assume that there is not a way to eliminate risk — there will be a need for multiple sophisticated connections to external networks, for a large number of users to access or collaborate on (sometimes sensitive) data, legacy or outdated equipment in use, or other complex issues that complicate traditional security methods. Over time, larger and higher performing companies have evolved the idea of a risk-based strategy into a more comprehensive method of protecting their organizations known as "zero trust."

• Zero Trust
A zero-trust strategy assumes that a threat can come from anywhere inside or outside your organization, and therefore a continual assessment of every request or attempt to connect or access networks, devices, or information is required. This can be highly resource intensive, and typically requires sophisticated authentication schemes as well as some sort of SIEM automation in the form of cloud data collection, systems monitoring, etc. User and systems data are monitored continually to develop a baseline of what is considered "normal" activity, which then allows for alerts if any abnormal activity occurs. Reducing the number of your external connections, applying the least privilege principle, and having dedicated resources to monitor and calibrate the results are all key to making this strategy effective, and while it is theoretically a great strategy for complex, highly-connected organizations, in practice it is very difficult to fully achieve today.

Phil Won, Product Manager
Phil is a product and technology leader, with years of experience in product development enabling the merge of business and technology needs of diverse industries (connected consumer devices, IIOT, automotive, cyber security and telecom).
He brings strategic and technical proficiency in new product planning, development, and deployment initiatives. Phil is on the Product Management team at Owl Cyber Defense. His main product line is OPDS, focusing on growing existing products and innovating future solutions. Phil can be reached at pwon@owlcyberdefense.com or our company website is: www.owlcyberdefense.com — twitter handle: @owlcyberdefense.com



SafeGuardCyber

Missing a piece of your cybersecurity ecosystem?



CLOUD APPLICATIONS

COLLABORATION TOOLS

MOBILE CHAT

SOCIAL MEDIA

Get a complimentary digital risk assessment today

www.SafeGuardCyber.com



See. Stop. Secure.

Seceon provides a simple, fully-automated approach to detecting and stopping the threats that lurk in the murky depths, just waiting to menace your enterprise. Leveraging an unmatched combination of behavioral analysis, machine learning and dynamic threat intelligence, Seceon delivers rich visibility, holistic threat detection and rapid threat containment—in minutes, not months. Whether you face compromised credentials, advanced persistent threats, insider activity or other threat sources, Seceon helps you surface and stop the threats that matter. **Right now.**

seceon

seceon.com

WHAT TO LOOK FOR WHEN SELECTING AN MSSP

by Brad Taylor, CEO, Proficio

Medium to large-sized organizations increasingly rely on managed security service providers (MSSPs) to deliver security monitoring, threat detection and incident response functions. This trend is driven by the shortage of cybersecurity professionals, the complexity of the threat landscape, and the acceptance of managed and co-managed models by IT leadership.

Proficio is an award winning MSSP serving customers from its global Security Operations Centers or SOCs in San Diego, Singapore and Barcelona. Proficio invented the concept and first coined the term – SOC-as-a-Service – whereby their customers benefit from the simplicity of a fully staffed SOC and a managed cloud or on-premise SIEM with the flexibility and responsiveness of an inhouse operation. Proficio's mission is to deliver a level of security defense equivalent in value to inhouse security operations of a F100 company, but at an affordable subscription fee.

Alert Accuracy, Relevance, and Context

At its core an MSSP's job is to notify their customers of threats, attacks, and compromises. Dissatisfaction with the quality of an MSSP's alerts is a common reason for buyer's remorse. Complaints can include too many or too few alerts, high false positive rates, and alerts that lack context and cogent recommendations. Ask your prospective MSSP the following:

1. What percentage of alerts are investigated, validated, and triaged by a SOC Analyst before they are sent to the user? The answer should be over 50% and the MSSP should track how this percentage changes over time.
2. What SIEM technology does the MSSP use to filter events and detect indicators of attack? If the MSSP developed the software themselves, is it realistic that they can sustain a team of developers to maintain a state-of-the-art SIEM tool?
3. What content has the MSSP built to enhance the accuracy of their SIEM tool? Ask for details around use cases, correlation rules, and integrated threat intelligence.
4. View actual examples of alerts and ensure the full context of the event is described and understandable. Look for recommended next steps with each alert. Alert notifications should be relevant and actionable?
5. Understand the SLAs associated with priority alerts. Do they start from when the event occurred or when a SOC Analyst was assigned the event? Are SLAs measured and reported on?

Insight into Your Security Posture

The best MSSPs do more than identify, notify, and report on threatening events. To be effective IT leaders need to understand their risk profile, identify where gaps exist in their existing security controls and understand the priorities to improve their defenses. While security assessments help organizations understand their security posture, many IT leaders prefer to continuously understand their strengths and weaknesses and be able to articulate their risk profile to management. Ask your prospective MSSP the following:

1. Does your MSSP provide you with executive level information on the strength of your security defenses?
2. Are you able to understand how risks apply to different parts of your network, endpoints and the cloud?
3. Is it easy to understand how gaps in your security controls map to different stages of the Cyber Kill Chain?
4. Does your MSSP provide you with a risk score and compare it to your industry peers?

Managed Detection and Response (MDR)

Leading MSSPs have transitioned their services from security monitoring to managed detection and response. Organizations need to automate the response to suspicious attacks and contain the threat before data is exfiltrated or malware propagates through the network. Ask your prospective MSSP the following:

1. Does your MSSP provide you automated and semi-automated endpoint detection and response services?
2. Does your MSSP automate blocking of suspicious inbound and outbound traffic at the perimeter?
3. Can your MSSP work with a range of industry leading security tools to orchestrate containment actions?
4. Can your MSSP provide customized MDR services based on unique use cases and correlations rules?

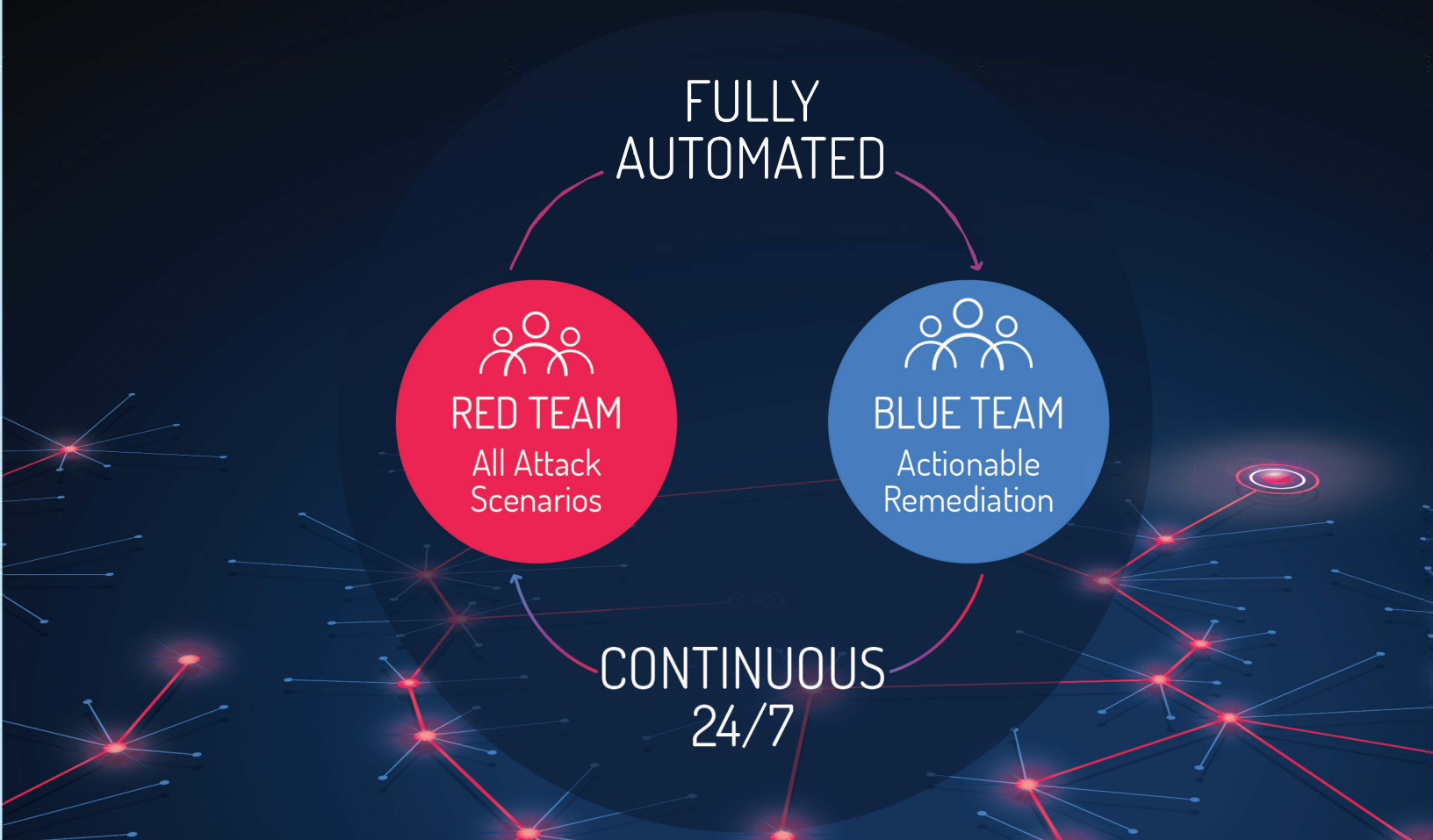
Brad Taylor is the CEO and CTO of Proficio. Brad has 30 years experience in the enterprise security, networking, and enterprise software. Brad is co-founder of Proficio, leads the company's security architects and strategic planning. He is a frequent speaker at industry events and expert commentator on all aspects of the security industry. Prior to Proficio, Brad led marketing, business development, acquisitions, operations, and venture capital functions. He has built and managed multiple sales teams as a VP of Sales and assisted in two highly successful IPO's with RSA Security (RSAS, now EMC) and ArcSight (ARST). In addition, he has helped many early stage companies become successful including: elQnetworks, SOA Software, and AirTight Networks. Brad can be reached online at www.proficio.com.



XM CYBER

DEFENSE BY OFFENSE®

YOUR FIRST
FULLY AUTOMATED
PURPLE TEAM



XM • DEFENSE BY OFFENSE

www.xmcyber.com

Quis custodiet ipsos custodes?

(Who watches the watchers?) by Dr. Richard Ford, Chief Scientist, Forcepoint

Over the last few years, I think every CISO has become painfully aware of the so-called "insider threat" — that is, the risks posed by a malicious employee who intends to harm the company in some way. While we don't like to think about our co-workers like that, there have been so many high-profile cases where an employee has decided to take an action that causes harm that this threat to the business cannot be ignored.

Operationally, there are important differences between an insider and an outsider. The traditional "moats and walls" security stance isn't effective against those who are already inside, and while concepts such as Zero Trust (there's a lot of material here, if you want to read more: https://go.forrester.com/blogs/category/zero-trust/) embrace segmentation and separation of duties, technologically we continue to move toward a more nuanced world. Thus, our goal is to use different forms of monitoring and analytics to detect — or, ideally, predict — various forms of employee misbehavior. These techniques are especially valuable when dealing with safety-critical systems or high-value data, but are applicable everywhere: most large companies need to make a data-driven decision around how rigorously they protect themselves from attacks that originate from within.

While these approaches can be very effective, they are less useful when attempting to identify users who have a legitimate requirement to use and modify the data they intend to steal. Analytically, it is easy to detect when a Project Manager is suddenly showing intense interest in collecting source code, it's infinitely harder to detect when a developer, who works with source code every day, actually is abusing that access. Typically, the data user or producer has by far the most extensive access and rights — and legitimately uses that data in her day job frequently. Thus, CISOs are left scratching their heads trying to figure out how to protect your information from those with legitimate access?

To put this in perspective, let's take a quick look at a real-world case. According to an affidavit filed in the US District Court for the State of New York, these things happen and be quite unpleasant. From Case 1:18-MJ-434-CFH (see: http://online.wsj.com/public/resources/documents/GE_Niskayuna_Complaint.pdf), we read about a Principal Engineer working for GE; as this case is pending, we'll just randomly call them "Dr. Ford". Dr. Ford is alleged to have collected Matlab files and encrypted them... and then used vim to append this data to an image file. This image was then sent to an email address external to the company.

When seen as a sequence of actions, this story is pretty easy to understand. However, when we view it at the individual event level, it is much harder to spot. A cursory examination of the image file, for example, would not have shown much amiss. Compressing files isn't particularly unusual, and if the files were ones that Eve worked with most days, it's hard to detect that their access is anomalous... because it isn't! Only when viewed end-to-end does the full picture emerge.

Over the last few years, I think every CISO has become painfully aware of the so-called "insider threat" — that is, the risks posed by a malicious employee who intends to harm the company in some way. While we don't like to think about our co-workers like that, there have been so many high-profile cases where an employee has decided to take an action that causes harm that this threat to the business cannot be ignored.

When seen as a sequence of actions, this story is pretty easy to understand. However, when we view it at the individual event level, it is much harder to spot. A cursory examination of the image file, for example, would not have shown much amiss. Compressing files isn't particularly unusual, and if the files were ones that Eve worked with most days, it's hard to detect that their access is anomalous... because it isn't! Only when viewed end-to-end does the full picture emerge.

Operationally, there are important differences between an insider and an outsider. The traditional "moats and walls" security stance isn't effective against those who are already inside, and while concepts such as Zero Trust (there's a lot of material here, if you want to read more: https://go.forrester.com/blogs/category/zero-trust/) embrace segmentation and separation of duties, technologically we continue to move toward a more nuanced world. Thus, our goal is to use different forms of monitoring and analytics to detect — or, ideally, predict — various forms of employee misbehavior. These techniques are especially valuable when dealing with safety-critical systems or high-value data, but are applicable everywhere: most large companies need to make a data-driven decision around how rigorously they protect themselves from attacks that originate from within.

While these approaches can be very effective, they are less useful when attempting to identify users who have a legitimate requirement to use and modify the data they intend to steal. Analytically, it is easy to detect when a Project Manager is suddenly showing intense interest in collecting source code, it's infinitely harder to detect when a developer, who works with source code every day, actually is abusing that access. Typically, the data user or producer has by far the most extensive access and rights — and legitimately uses that data in her day job frequently. Thus, CISOs are left scratching their heads trying to figure out how to protect your information from those with legitimate access?

To put this in perspective, let's take a quick look at a real-world case. According to an affidavit filed in the US District Court for the State of New York, these things happen and be quite unpleasant. From Case 1:18-MJ-434-CFH (see: http://online.wsj.com/public/resources/documents/GE_Niskayuna_Complaint.pdf), we read about a Principal Engineer working for GE; as this case is pending, we'll just randomly call them "Dr. Ford". Dr. Ford is alleged to have collected Matlab files and encrypted them... and then used vim to append this data to an image file. This image was then sent to an email address external to the company.

Dr. Richard Ford is the Chief Scientist of Forcepoint. Ford has over 25 years' experience in computer security, having worked with both offensive and defensive technology solutions. During his career, Ford has held positions with Virus Bulletin, IBM Research, Command Software Systems, and NTT Verio. In addition to work in the private sector, he has also worked in academia, having held an endowed chair in Computer Security, and worked as Head of the Computer Sciences and Cybersecurity Department at the Florida Institute of Technology. Under his leadership, the University was designated a National Center of Academic Excellence in Cybersecurity Research by the DHS and NSA. He has published numerous papers and holds several patents in the security area.

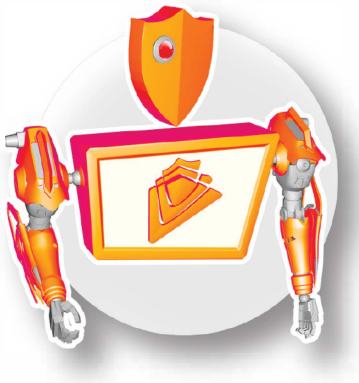
Ford holds a Bachelor's, Master's and D.Phil. in Physics from the University of Oxford. In addition to his work, he is an accomplished jazz flutist and Instrument Rated Pilot

Richard can be reached online at Email: Richard.a.ford@forcepoint.com and Twitter: @rfordonsecurity and at our company website https://www.Forcepoint.com/



ATAR®

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE PLATFORM



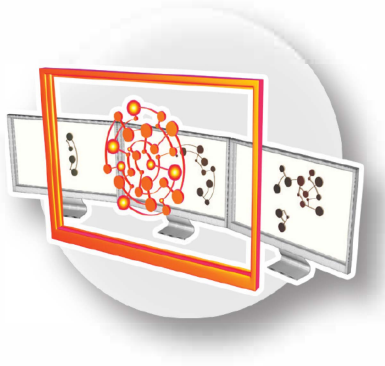
Automate
Repetitive Activities

- Scenario driven automation
- Complex logic support
- Connectors for 100+ platforms
- Full & semi automation support



Improve
Analyst Efficiency

- Unified investigations interface
- Collaborative investigations
- 1-click evidence collection & actions
- Evidence vaulting



SOC
Analytics

- Metrics collection from SOC processes
- SLA monitoring
- Workload monitoring
- Reports & dashboards
- Savings

Award Winning SOAR ATAR®

Cyber Defense Magazine Global
Cutting Edge SOAR Platform 2018

Red Herring Global 2018
Top 100 Award Winner

Bilkent Cyberpark MIS Awards 2018
Fastest Growing Company

Red Herring Europe 2018
Top 100 Award Winner

LONDON: 24 The Shard 32 London Bridge St. LONDON SE1 9SG +44 203 026 94 32
www.atarlabs.io | atar_labs | atarlabs | info@atarlabs.io

atarlabs

WE STOP CYBER THREATS DEAD IN THEIR TRACKS.



OWL Cyber Defense

Data Diode Cybersecurity Solutions

Meet us at RSA Conference 2019
March 4-8 • Booth #6140

owlcyberdefense.com
@owlcyberdefense



Aligning Cybersecurity Effectiveness with Core Business Objectives

CYBERSECURITY PROGRAMS ESTABLISH DEFINED GOALS BUT LACK MEASURABLE INDICATORS TO GAUGE EFFECTIVENESS.

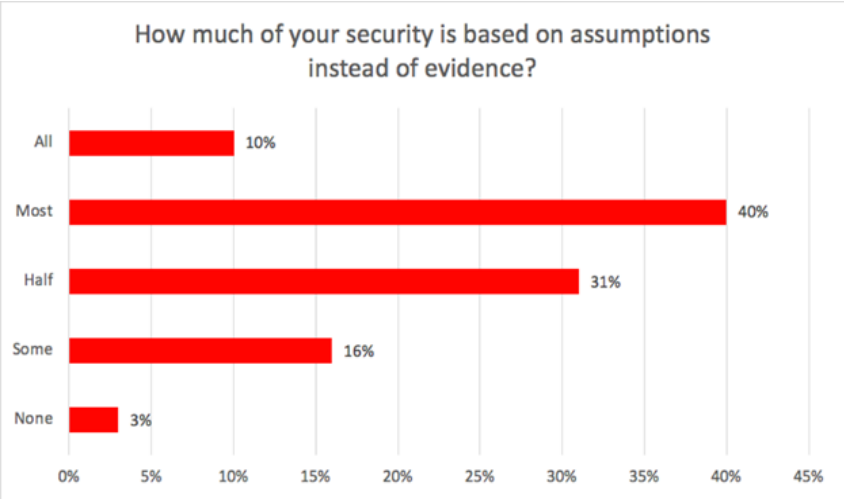
by Brian Contos, CISO, Verodin Inc.

From an objective perspective, it is easy to become desensitized by the current state of cybersecurity. Every headline-grabbing breach plays out like a rerun of a bad sitcom. Still, recent incidents beg the question: why are even the most sophisticated and well-funded cybersecurity programs struggling?

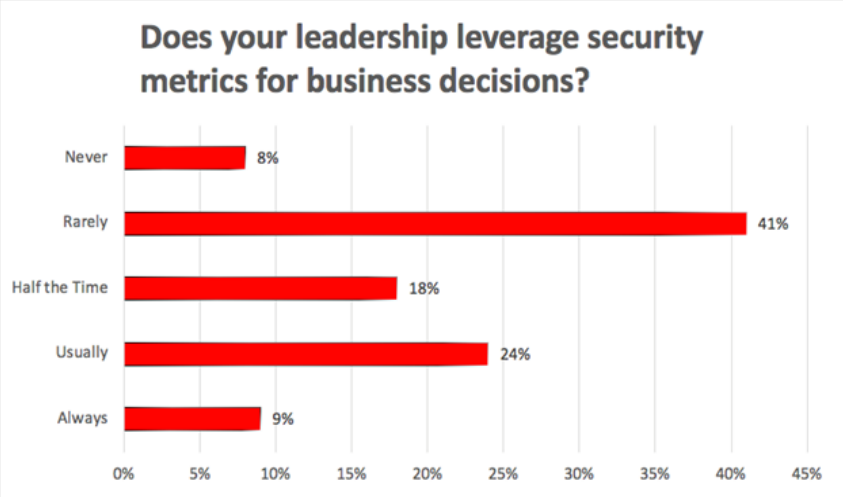
The margin of error in cybersecurity is unprecedented. Modern IT environments are complex and unique, with intricate combinations of products, configurations, and architectures. The fact, a lot has to go right for dozens of disparate tools to work together in concert and be effective. Known and unknown changes in tools, infrastructure, and configurations introduce the risk of unintended errors and blind spots. To add to the complexity, environments are constantly shifting, so there is no guarantee that defenses working today will remain effective tomorrow.

The harsh reality is that cybersecurity as we know it is fundamentally flawed. Unlike other essential business units such as finance and operations, cybersecurity is not measured with quantifiable metrics and optics predicated on evidence-based data. Instead, cybersecurity success criteria is loosely defined and principally based on assumptions. Over the years, cybersecurity infrastructures have ballooned without the instrumentation necessary to dynamically measure and manage their effectiveness. This has resulted in product redundancies, unnecessary complexity, overwhelmed analysts, and wasted dollars. Bottom line: the cybersecurity value perceived is not the value being realized.

Assumption-based cybersecurity is rampant. In a recent poll from Verodin Inc., a broad audience of InfoSec professionals including red and blue teams, auditors, and executives, were asked, “How much of your security is based on assumptions instead of evidence?” Not surprisingly, a whopping 97% of responders admitted to managing by assumption to some degree.



In a separate poll, the audience was asked, "Does your leadership leverage security metrics for business decisions?" Only 51% voted for "half the time," "usually," or "always."



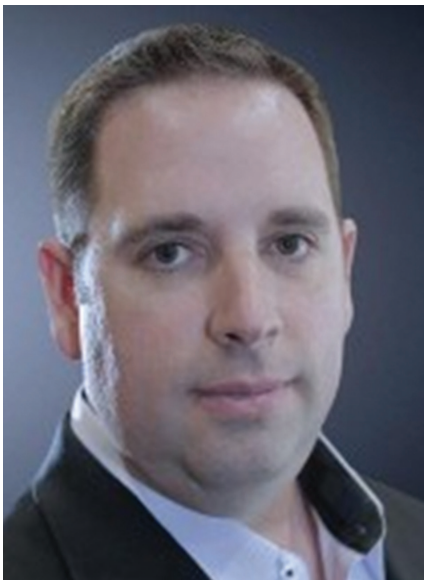
If you cannot measure it, you cannot manage it.
A holistic understanding of cybersecurity effectiveness can only be achieved with key performance indicators to measure people, processes, and technology. Today, many

enterprises do not have the systems in place to stress-test and continuously validate the protection of their critical assets and business operations. Furthermore, programs cannot produce the evidence required to determine if their efforts and investments are meeting defined goals and satisfying regulatory obligations.

Security Instrumentation elevates cybersecurity to the same standards as other metrics-driven business units.
Verodin Inc. offers the first business platform purpose-built to measure, manage, improve, and communicate cybersecurity effectiveness. The Verodin Security Instrumentation Platform (SIP) provides the evidence required to determine if an enterprise's layered defenses are effective across endpoint, email, cloud, and network tools, enabling organizations to continuously validate the protection of their business-critical assets. From the boardroom to the CISO to the SOC, Security Instrumentation empowers the business to understand and communicate cybersecurity effectiveness with quantifiable metrics.



Prove that core business objectives are being achieved. Large enterprises report having 30 to 70 cybersecurity vendors deployed in their environment. Once the shift is made from assumption-based to evidence-based cybersecurity, it becomes possible to start rationalizing investments. Programs can address questions like, "what's working, what's not, what should be replaced, where do we need to allocate resources, and how should we be prioritizing changes?" As we enter 2019, cybersecurity programs would be wise to focus their efforts on maximizing the effectiveness of the investments they already have in place before purchasing that next buzzword. After all, if the foundation is broken, everything is broken. Learn more at verodin.com. (RSA booth #4214)



Brian Contos is the CISO & VP of Technology Innovation at Verodin. With over 20 years of security industry experience, working across more than 50 countries and six continents, he is a seasoned executive, board advisor, security company entrepreneur & author. After getting his start in security with DISA and later Bell Labs, he began the process of building startups and taking multiple companies through successful IPOs & acquisitions including Riptech, ArcSight, Imperva, McAfee and Solera Networks. Brian is frequently interviewed by the press and is a speaker at conferences like Black Hat, BSides, RSA, Interop, SOURCE, SecTor, and OWASP.
Brian can be reached online at (brian.contos@verodin.com, @BrianContos, etc..) and at our company website https://www.verodin.com

APCON
Solutions for Networks

Illuminate Your **Network Security**

APCON's Series 4000 next-generation hybrid visibility platform provides data access and virtual monitoring integration of high-speed data networks running in private cloud, public cloud and on-premise infrastructures.



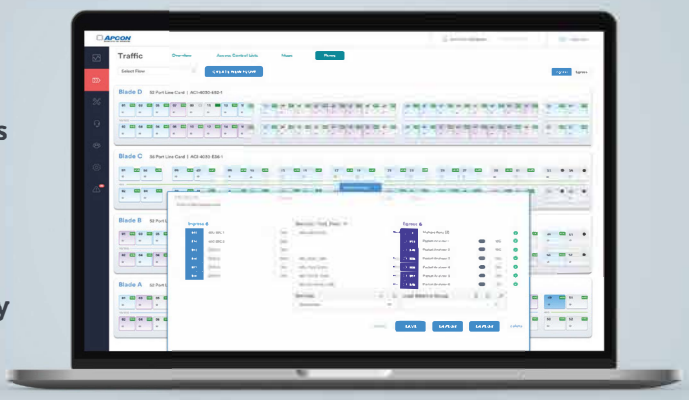
Secure Your Hybrid Data Center with APCON's State-of-the-Art Visibility Technology

Future-ready for hybrid networks

High-density design that scales

Up to four times lower TCO

Maximize security intelligence



Series 4000 delivers the right traffic to your security & network monitoring tools. Advanced features include deduplication, packet-slicing and protocol header stripping.

Return on Investment: Get scale and investment protection with high density 1/10/25/40 and 100G ports.

www.apcon.com



DEFENSE BY OFFENSE

Purple Team: The Meeting Point of Red and Blue Teams Meet
by Maya Schirmann, VP Marketing, XM Cyber

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."
—Sun Tzu, The Art of War

For millennia, military strategists around the world have recognized that thinking like the enemy is one of the best ways to anticipate what they're going to do and so defeat them. With the numbers of attacks rising year-over-year, traditional lines of defense just aren't good enough anymore. Breaches appear everywhere, with attackers steadily advancing, and no organization should neglect approaches that look at their defenses from the viewpoint of the attacker.

PROACTIVE SECURITY STRATEGIES

A large number of organizations are coming to see that a proactive security strategy is one of the best defenses. You need to see where the threats are coming from, how they can move within your network, where the vulnerabilities in your defenses are, find them and close them before cyber attackers take advantage of them.

To become proactive on the security front, it's vital that you identify in advance the vectors of attack that will be utilized and remediate security issues as they are created and before they are exploited. For that, you need a continuously running campaign of tests running against your current defenses with simulations in your real environment: that's where breach and attack simulation comes in. Generally, an organization won't realize where exactly it was vulnerable in terms of its defenses until the attack comes, by which time it's too late to fix these vulnerabilities. If you are continually testing your security, you can uncover the attack paths and remedy these failings before attackers find out about them. Proactive vs. Reactive.

Modern militaries have been known to galvanize opposing forces during defense-offense exercises to increase a unit's success rate. The U.S. Air Force, for instance, works with fighter squadrons, the red team, that use Tactics, Techniques and Procedures (TTPs) of an attack force.

Cybersecurity, for many firms, has started to resemble a military drill. It really is a war zone out there, and only the latest proactive practices and processes will keep you from defeat. The military keeps their soldiers on their toes by continuously running wargames; cybersecurity experts should be doing the same by running simulated cyber-attacks.

ENTERING THE AUTOMATED PURPLE TEAM ERA

By mimicking enemy tactics, the red teams make the blue teams better at defense. At least, that was the idea. The red/blue approach fits well with a structured, episodic win/lose paradigm of defense—like an air battle. One side attacks. The other defends. Then, it's over and there's a discussion of what worked and what didn't. The blue team gets busy improving their defenses for next time.

A new approach, known as a "purple teaming" has emerged as a middle ground solution. A purple team blends the activities of both red and blue teams. The purple team enables both attack and defense to exchange ideas, observations and insights more productively than is possible with the "us vs. them" ethos of the red/blue battles.

An automated purple team truly accelerates the advantage of this approach: it can continuously simulate attacks such as Advanced Persistent Threats (APTs). This automated platform can also validate and provide a remediation plan to thwart an attackers' path(s) to critical assets. It never stops performing the red/blue cycle and helps augment the team's tool kit. This is helpful, given the constant changes in user activity, network infrastructure, network settings, and patches that characterize IT in real life. Vulnerabilities open and close round-the-clock. It's best to detect and respond to them in a timely fashion. It is inhuman to do this manually, but machines and software (built correctly) can and should perform these tasks to aid in the fight against APTs.

With an automated purple team running continuously, organizations will finally be able to follow prioritized remediation guidelines and know as soon as an issue has been resolved. The move to automation empowers organizations with the ability to gain a worm's eye view into new back doors and blind spots as soon as they appear and move to remediate them immediately without delay.

Combining the best of all worlds, an effective automated purple team can ameliorate the security of all critical assets through 24X7 real-time exposure, and automatically deliver prioritized and actionable remediation without disrupting networks and users' day-to-day activity. Addressing real user behavior, security vulnerabilities and shadow IT, it can deliver the big lift in digital hygiene. By doing so the automated purple team enable organizations to bolt the windows, as well as insert a lock on the cyber door.
End.

Maya Schirmann is the VP Marketing of XM Cyber
With over 15 years of extensive experience as a marketing, strategy, and sales executive, Maya Schirmann has a proven track record in creating markets and guiding technology corporations to market leadership positions. Prior to XM Cyber, Ms. Schirmann served as CMO of a cybersecurity company Deep Instinct. She also held various senior strategic marketing and sales positions with Amdocs and Comverse, where she led the launch of innovative products and services and oversaw large complex deals with global telecom operators.

Ms. Schirmann originally hails from France, where she worked for telecom operator SFR, leading the successful launches of numerous innovative services including the first mobile email, MMS, and Vodafone Live. She holds a M.Sc. in Mathematics from Jussieu Paris 7 University.

Maya can be reached online at maya.schirmann@xmcyber.com and at our company website https://xmcyber.com/





NOZOMI NETWORKS

Real-time Cyber Security and Visibility for Industrial Control Networks

Superior Operational Visibility

Accurately visualize your industrial networks and improve resilience with real-time asset inventory and network monitoring.

Best-in-Class ICS Threat Detection

Rapidly manage cyber threats and process risks with a solution that correlates multiple, advanced detection techniques.

Most Global Installations

Centrally monitor hundreds of facilities with a solution proven to scale across continents and integrate with IT/OT systems.

FROST & SULLIVAN

2019 BEST PRACTICES AWARD

GLOBAL INDUSTRIAL CYBERSECURITY SOLUTIONS ENABLING TECHNOLOGY LEADERSHIP AWARD

#thosewhoknowpicknozomi

www.nozominetworks.com

Third Party – Minimizing Organizational Exposure by Mitigating the Wild Card in Security Strategies

2019 Shared Assessments Third Party Risk Management Toolkit Helps Organizations Replace FUD with Actionable Insight, Risk Management Best Practices and Invaluable Tools.

by Catherine A. Allen, Chairman and CEO
The Santa Fe Group

The list of major data leaks caused by third parties grows almost daily. Third party vulnerabilities, exposure incidents and hacks have been at the root of many of the last three years' most troubling breaches.

"Third party IT security risks can cause millions of dollars in loss and damage, and possibly irreparable harm to an organization's reputation," said Glen Sgambati, risk management expert with Early Warning Services.

Bad actors are increasingly organized, well-funded, determined and patient. They'll apply the time and resources to successfully breach their chosen potential victim. They occasionally strike for political reasons, but more often their goal is financial gain.

The IT infrastructures of partners and other trusted third parties are one of a cyber criminal's preferred pathways into a chosen target's domain. This burdens organizations with thoroughly assessing and addressing the potential risks and vulnerabilities of all partners, vendors and other third parties, as well as their own in-house vulnerabilities — an overwhelmingly broad intelligence-gathering mission for even the largest company, given the inventiveness and diligence of bad actors.

Diligence obligates that the C-Suite ensure that their organizational risk management strategies and practices anticipate and manage the full spectrum of risks that result from interactions with physical and digital ecosystem partners, while sustaining the agility to adapt to the ever-changing threat landscape. Assessing and addressing the current state of corporate readiness and minimizing the organization's exposure to unplanned events and their consequences is crucial.

Many of the world's top financial institutions, energy and critical infrastructure entities, consumer goods corporations, manufacturers and security-minded organizations of all sizes combat the problem together as part of the Shared Assessments member community. The member-driven consortium leverages the collective intelligence and risk management experience of a diverse cohort of practitioners, spanning industries and perspectives. The 'intelligence ecosystem' produces independent research, and drives best practices, tools and certification standards that are used by thousands of organizations.

It's latest creation – the 2019 Shared Assessments Third Party Risk Management Toolkit – enables organizations to manage the full vendor assessment relationship lifecycle — from planning a third party risk management program, to building and capturing assessments, to benchmarking and ongoing evaluation of a program.

Vendor Risk Management Maturity Model (VRMMM) Benchmark Tools:

The VRMMM evaluates third party risk assessment programs against a comprehensive set of best practices. The VRMMM has always been the go-to place to understand the major building blocks of any vendor risk management program. Broken into eight categories the model explores more than 200 program elements that should form the basis of a well-run third party risk management program. The VRMMM's eight categories are: Program Governance; Policies Standards, and Procedures; Contract Development, Adherence, and Management; Vendor Risk Assessment Process; Skills and Expertise; Communications and Information Sharing; Tools, Measurement, and Analysis; and Monitoring and Review.

The VRMMM has been updated and improved annually since 2013, and is the longest running third party risk maturity model, vetted and refined by hundreds of the most experienced third party risk management professionals and the basis for an annual published study. The VRMMM Benchmark Tools are free and available at: www.sharedassessments.org/vrmmm.

Standardized Information Gathering (SIG) Questionnaire Tools:

The SIG employs a holistic set of industry best practices for gathering and assessing 18 critical risk domains and corresponding controls, including information technology, cybersecurity, privacy, resiliency and data security risks. Think of it as the "trust" component for outsourcers who wish to obtain succinct, scoped initial assessment information on a third party's controls. It also lets partners reduce initial assessment duplication and assessment fatigue by supplying their own SIGs to outsourcers.

Standardized Control Assessment (SCA) Procedure Tools:

The SCA assists risk professionals in performing onsite or virtual assessments of vendors. This is the "verify" component of a third party risk program. It mirrors the 18 critical risk domains from the SIG, and can be scoped to an individual organization's needs

GDPR Privacy Tools:

Timely and immediately useful components that help organizations meet regulatory requirements on "controllers" (i.e., the organization who outsources services, data, etc. to third parties), who must appoint and monitor Data Processors (i.e., third parties/vendors). The Privacy Tools can be used as part of a holistic privacy management program that reaches beyond the scope of GDPR, and can be used both to assess service providers and to manage an outsourcer's privacy data controls. The GDPR Privacy Tools cover both Trust and Verify for Privacy and tracks the inventory of where data is located.

New and Lighter Architecture, Custom Scoping, Assessment Streamlining

The toolkit's lighter architecture supports new speed and flexibility in creating, administering and storing risk assessments. It also features a new Content Library of standardized questions and vertical-specific questions, and the opportunity to add custom questions and build questionnaires on the fly — ensuring standardization while also allowing customization. Among other updates are:

- Custom Scoping allowing organizations to scope by Domain, by Category, by Authority Document, by Tiered Scoping or by Individual Question Scoping. ssments.
- SIG and SCA Integration enabling outsourcers to create a Standardized Control Assessment (SCA) Procedure Tool for onsite or virtual assessments.
- Constant Regulatory and Privacy Legislation Updates: The Toolkit is constantly updated with the most relevant and current US and International regulatory and privacy content such as NIST 800-53r4, NIST CSF 1.1, FFIEC CAT Tool, the EU GDPR and PCI 3.2.1.

The Toolkit was designed to work together to help third party risk practitioners with all aspects of the third party risk management lifecycle — an Olympic-level task made considerably less daunting and far more efficient and programmatic by Shared Assessments.

Sgambati notes: "The continually escalating pace of attacks and the innovation that bad actors now employ means that organizations must be continuously vigilant. Given the scope of the threat, no one organization can go it alone. The Shared Assessments 2019 Third Party Risk Management Toolkit is an asset that affords risk management professionals speed and flexibility in creating and conducting vendor assessments."

For more than 30 years, Catherine A. Allen has been an outstanding leader in technology strategy and financial services and a key thought leader in business innovation.

Today, Catherine is Chairman and CEO of The Santa Fe Group, a strategic consulting company based in Santa Fe, NM. The Santa Fe Group specializes in briefings to C-level executives and boards of directors at financial institutions and other critical infrastructure companies, and provides management for strategic industry and institutional projects, including the Shared Assessments Program, focused on third party risk.



Catherine currently serves as a board member of Synovus Financial Corporation and El Paso Electric Company and is a member of the Risk, Energy and Natural Resources, Public Policy and External Affairs, and Nominating and Governance Committees. She chairs the Security Committee for El Paso Electric. She is co-chair of the University of Missouri's Capital Campaign and sits on the Research and Development Committee. She is also on the board of Women Corporate Directors and the Executive Women's Forum. She sits on the Advisory Committee for Houlihan Lokey and chairs the Board of Trustees for the National Foundation for Credit Counseling and the board of Appleseed NM. She is also a member of the Museum of New Mexico Foundation, International Folk Art Alliance, Lensic Center for Performing Arts, Communities for Schools in New Mexico, Valles Caldera Trust, and the Mark Twain Research Foundation boards. She was a former board member and Chair of the Technology Committee for Stewart Information Services.



Filling the Public Relations Void for Security Innovators

Exclusive Interview with Dan Chmielewski, agency principal, Madison Alexander PR, Inc., an InfoSec Focused High Tech Communications Agency, by Gary S. Miliefsky, Publisher, Cyber Defense Magazine

When it comes to communicating the credibility of your brand to the world, PR (Public Relations) is very simply, hands down, the best channel.
Contrary to what most people think, PR is one of the most cost-effective methods of raising brand awareness for your business and, in essence, increasing sales.

Product placements in popular magazines, newspapers, trade journals, and social media outlets or radio/TV stations help cement brands as trusted authorities within their categories.

Madison Alexander PR, Inc. (MA PR) is a boutique technology communications consultancy that specializes in public relations, analyst relations, marketing communications and social media services for technology companies. The agency caters to start-ups to mid-size technology firms in security, networking, cloud computing, enterprise software, SaaS, managed services, search technologies, and technology platforms that solve business problems.

MA PR was established in 2004 and is based in Southern California. The firm has additional offices in Boston, Silicon Valley, South Florida and has international partners all over the word.

Dan Chmielewski, agency principal, did a Q&A with the publisher of Cyber Defense Magazine, Gary S. Miliefsky:



Why was the company set up? And how did you expand your company and its offerings over the years?
The company fills a void for start-up and smaller technology companies, mostly in cybersecurity, to provide senior PR representation to help them grow to the next level. PR is a relationship business and we have developed great relationships with the media by delivering on what we promise when we pitch. MA PR does not have minimum monthly retainers and has a team approach to accounts allowing senior, experienced PR representation that generates coverage, awards, and speaking ops.

There is nothing more important for a successful small business than a well-defined mission and vision statements. Can you explain your M&V statements in brief?
The professionals at MA PR who pitch your business will also service your account. There's no bait and switch. Additionally, we won't take on new clients that compete with existing clients; the notion of 'firewalls' between account teams for handling clients who compete against each other in the same market is, quite frankly, not realistic, and we don't do that. We service a small group of clients that benefit from our complete focus and attention. We build account teams of public relations, marketing communications, web/graphics, and social media professionals based on the needs of the client.

Strategically and tactically, we understand the business of B2B and B2C security technology better than most agencies. We provide detailed context for developing a campaign including industry initiatives for technology frameworks and issues advocacy; launching a product, company, or new business unit; managing a product review; crisis communications situations; and helping an executive deliver a great interview—all based on what we know about how messaging and media work in the technology space. A solid understanding of the editorial process is critical to our success, and helping clients understand this process ensures that our combined efforts are extremely effective and generate results. Our team has significant newsroom experience so we can put on our "editor's hat" to help a client clarify their message.

Additionally, as the first US-based representative of the CodeRed Network of global PR firms with an IT security focus (by invitation only — http://www.coderedsecuritypr.com/), MA PR collaborates with accomplished international agencies for targeted international communications when the need arises.

PR is a relationship business; it makes sense to build an experienced team. Our relationships with influencers are positive so when we pitch a new company, they do pay attention and offer feedback the client needs to hear. We are a results-oriented PR firm; we track earned coverage, we never rest on our laurels, we always have irons in the fire for our clients. We are an idea machine.

Is your company a leader or a follower?
My company is a leader when it comes to gauging how a newsroom reacts to a pitch and the anticipated coverage. We have no problem telling a client their announcement isn't going to garner widespread coverage, but we lead them to where they need to go outside of the realm of traditional PR. We are a leader in turning clients into technology thought leaders.

Trust takes a long time to build and can be destroyed in an instant. We work hard towards developing long-term trust with the public we work with so they can count on the information we pitch.

As a question on sustainability, where do you see your company a couple of years from now?
Our clients are loyal, and we're loyal to them in return; hopefully, we continue to do great work for them. We are not trying to be the biggest agency but focus on being one of the best.

PR is a relationship business; it makes sense to build an experienced team. Our relationships with influencers are positive so when we pitch a new company, they do pay attention and offer feedback the client needs to hear. We are a results-oriented PR firm; we track earned coverage, we never rest on our laurels, we always have irons in the fire for our clients. We are an idea machine.

Is your company a leader or a follower?
My company is a leader when it comes to gauging how a newsroom reacts to a pitch and the anticipated coverage. We have no problem telling a client their announcement isn't going to garner widespread coverage, but we lead them to where they need to go outside of the realm of traditional PR. We are a leader in turning clients into technology thought leaders.

Trust takes a long time to build and can be destroyed in an instant. We work hard towards developing long-term trust with the public we work with so they can count on the information we pitch.

As a question on sustainability, where do you see your company a couple of years from now?
Our clients are loyal, and we're loyal to them in return; hopefully, we continue to do great work for them. We are not trying to be the biggest agency but focus on being one of the best.

Mad•i•son Al•ex•an•der
Public Relations, Inc.

Welcome to the InfoSec Awards for 2019



It's been nearly six months in the making — our annual review by our expert judges all over the globe who all share in one belief — that it's not the biggest, richest company — it's the hottest, most innovative — some are big and some are small but they all have something in common — a passion to stop breaches.

Whether you see a market leader name you recognize or a newcomer — startup or early stage — you'll find cutting edge products, services and solutions you might not have seen before and will need to consider in your portfolio.

We've also begun inviting universities and educational outfits that focus on or have a cybersecurity specific course offering. In addition, you might see a PR firm or marketing outfit receiving an award from us for one reason — without them, how would we all know about these innovators? Please join us in congratulating the winners — stop by their boot at RSAC 2019 or visit them online and ask for a demo.

We've decide to create a website that will be permanently dedicated to our award winners at www.cyberdefenseawards.com so please visit and bookmark the page.

Gary S. Miliefsky, CEO
Cyber Defense Media Group



InfoSec Awards for 2019

Access Control
Citrix, Market Leader
ERP Maestro, Cutting Edge

Adaptive Risk-Based Authentication
Silverfort, Most Innovative

Advanced Persistent Threat (APT) Detection and Response
Vectra, Editor's Choice
Resecurity, Hot Company
Attivo Networks, Best Product

Continuous Threat Intelligence
AlienVault, an AT&T company, Market Leader

Anti-Malware
Ericom Software Inc., Hot Company
PC Pitstop, Editor's Choice

Anti-Phishing
KnowBe4, Editor's Choice
Avanan, Cutting Edge
Vadesecure, Most Innovative
EdgeWave, Market Leader
Cofense, Best Product

Application Security
ShiftLeft, Most Innovative
WhiteSource, Best Product
Denim Group, Cutting Edge
XTN Inc, Hot Company
Checkmarx, Market Leader

Artificial Intelligence and Machine Learning
Vectra, Best Product
XTN Inc., Publisher's Choice

Authentication and Verification Technology
GEOACL LLC, Cutting Edge

Identity and Access Management
Ping Identity, Editor's Choice
Herjavec Group, Cutting Edge

PR Firm for Infosec Companies
ARPR, Publisher's Choice

Biometrics
Jumio, Best Product

Breach and Attack Simulation
XM Cyber, Hot Company
Cymulate, Cutting Edge

Breach Prevention
Sql Power Tools, Most Innovative

Bring Your Own Device (BYOD)
360 Enterprise Security Group, Next Gen

Browser Isolation
Light Point Security, Hot Company

Chief Executive of the Year
Darren Guccione, Keeper Security, Cutting Edge
Bill Holtz, Sectigo, Most Innovative
Mr. Ceasar Pie, CSIOS Corporation, Next Gen

Chief Technology Officer of the Year
Sourabh Tiwari, Overseas Infrastructure Alliance, Cutting Edge

www.cyberdefenseawards.com



InfoSec Awards for 2019

Cloud Security
Twistlock, Next Gen
360 Enterprise Security Group, Cutting Edge
Securonix, Most Innovative
AlienVault, an AT&T company, Market Leader
Equinix, Hot Company
Fortanix, Best Product

Code Variant Analysis
Semmle, Hot Company

Compliance
Global Learning Systems, Hot Company
SafeGuard Cyber, Next Gen
Jumio, Market Leader
TrueVault, Most Innovative

Container Security
Tigera, Best Product

Continuous Security Validation
Verodin, Editor's Choice

Critical Infrastructure Protection
Ampex Data Systems, Cutting Edge
Owl Cyber Defense, Best Product

CSO of the Year
Stan Black, Citrix, Publisher's Choice

Cyber Security
Barrier1, Cutting Edge
Bufferzone Security, Market Leader

Cybersecurity Analytics
Sergeant Laboratories, Most Innovative
Awake, Next Gen

Cybersecurity Artificial Intelligence
Vectra, Market Leader
Senseon, Hot Company

Cybersecurity Password Management
Keeper Security, Publisher's Choice

Cybersecurity Service Provider
CSIOS Corporation, Hot Company

Cybersecurity Training
Global Learning Systems, Best Product
Circadence, Editor's Choice

Data Loss Prevention (DLP)
DB CyberTech, Best Product
CoSoSys, Hot Company
Altaro, Cutting Edge
GTB Technologies, Most Innovative

Database Security
Sql Power Tools, Hot Company

Deception Based Security
Ntrepid, LLC, Cutting Edge
Attivo Networks, Market Leader
CounterCraft, Next Gen

Deep Sea Phishing
Inky, Most Innovative
Sectigo Next Gen
EdgeWave, Best Product
IRONSCALES, Editor's Choice

www.cyberdefenseawards.com



InfoSec Awards for 2019

Digital Footprint Security
Ntrepid, LLC, Best Product

Email Security and Management
Secure Channels, Most Innovative
EdgeWave, Hot Company

Encryption
Secure Channels, Next Gen
iStorage, Best Product
Fortanix, Most Innovative
SafeLogic, Market Leader

Endpoint Security
Cylance Inc., Market Leader
Adaptiva, Hot Company
Nuspire Networks, Next Gen
Ericom Software Inc., Cutting Edge
Resecurity, Editor's Choice
Carbon Black, Best Product

Enterprise Mobile Threat Defense
Zimperium, Publisher's Choice

Enterprise Security
Resecurity, Hot Company
ThreatQuotient, Market Leader

Firewall
Untangle, Best Product

Fraud Prevention
Experian, Market Leader
Jumio, Best Product
XTN Inc., Hot Company

Hot New Startup
Sql Power Tools, Most Innovative

Hybrid Network Visibility
APCON, Next Gen

ICS/SCADA Security
Nozomi Networks, Best Product

Identity & Access Management
Ping Identity, Editor's Choice
Herjavec Group, Market Leader

Identity Management
Sectigo, Hot Company

Incident Response
D3 Security, Editor's Choice
Intezer, Cutting Edge
Demisto, Most Innovative

InfoSec Startup of the Year
XM Cyber, Next Gen

Insider Threat Detection
ObserveIT, Best Product
CSIOS Corporation, Most Innovative

Internet of Things (IoT) Security
MACHINE-TO-MACHINE (M2MI) CORPORATION, Most Innovative
Sectigo, Publisher's Choice

Malware Analysis
Intezer, Cutting Edge

Managed Detection and Response (MDR)
Proficio, Market Leader

www.cyberdefenseawards.com



InfoSec Awards for 2019

Managed File Transfer
HelpSystems, Market Leader

Managed Security Service Provider
Proficio, Hot Company
Herjavec Group, Most Innovative

Mobile Endpoint Security
Zimperium, Market Leader

MSSP Platform
Seceon, Inc., Hot Company

Multi-factor Authentication
WatchGuard Technologies, Market Leader
iovation, Most Innovative

Network Access Control
Forescout, Market Leader
Portnox, Best Product

Network Security and Management
FireMon, Cutting Edge
Corelight, Most Innovative
Untangle, Market Leader

Open Source Security
Semmle, Publisher's Choice

PR Firm for InfoSec Companies
AxiCom US, Hot Company
ARPR, Publisher's Choice

Privacy Management Software
BigID, Cutting Edge

Privileged Account Security
Secure Channels, Most Innovative
Thycotic, Publisher's Choice
CyberArk, Market Leader
Centrify, Best Product

Risk Management
Digital Shadows, Cutting Edge
The Santa Fe Group, Hot Company

SaaS/Cloud Security
SafeGuard Cyber, Cutting Edge
Equinix, Publisher's Choice
Hornetsecurity, Most Innovative

Security Analytics
Securonix, Editor's Choice

Security Company of the Year
Herjavec Group, Publisher's Choice
Verodin, Most Innovative
Cylance Inc., Market Leader
WatchGuard Technologies, Editor's Choice

Security Information Event Management (SIEM)
LogRhythm, Market Leader
Seceon, Inc., Next Gen

Security Instrumentation Platform (SIP)
Verodin, Most Innovative

Security Investigation
ThreatQuotient, Hot Company

www.cyberdefenseawards.com

InfoSec Awards for 2019

Security Orchestration Automation and Response (SOAR)
ATAR LABS, Next Gen

Security Software
Lastline, Editor's Choice

Security Software
XM Cyber, Publisher's Choice

Security Training
Global Learning Systems, Market Leader
Inspired eLearning LLC, Cutting Edge
KnowBe4, Next Gen

Security Training & Awareness for Employees
InfoSec Institute, Editor's Choice

Security Training for InfoSec Professionals
InfoSec Institute, Publisher's Choice

SOC-as-a-Service Provider
Proficio, Most Innovative

Social Media, Web Filtering, and Content Security
SafeGuard Cyber, Best Product

Telecoms Fraud Protection
Oculeus , Most Innovative

Threat Intelligence
Recorded Future, Editor's Choice
360 Enterprise Security Group, Best Product
AlienVault, Market Leader
Resecurity, Most Innovative
ThreatQuotient, Publisher's Choice
EclecticIQ, Next Gen

Threat Modeling
ThreatModeler, Editor's Choice

Unified Threat Management (UTM)
WatchGuard Technologies, Best Product
Untangle, Market Leader

User Behavior Analytics
LogRhythm, Market Leader

Vendor Risk Management Platform
iTrust, Cutting Edge

Vulnerability Assessment, Remediation and Management
Denim Group, Editor's Choice

Vulnerability Management
Kenna Security, Hot Company

Web Application Security
WhiteHat Security, Best Product
Cequence Security, Next Gen
Threat X, Hot Company

Website Security
Cloudbric, Hot Company

Women in Cybersecurity
Gigi Schumm, SVP Worldwide Sales, ThreatQuotient, Publisher's Choice
Dr. Ambareen Siraj, WiCyS Founder & Board Member, WiCys.org, Editor's Choice
Mischel Kwon, MKACyber, Hot Company

Late entry winners (those that won, but late in the judging and did not make it into this print edition) are listed on **www.cyberdefenseawards.com** please check them out and visit their websites as well.

www.cyberdefenseawards.com

Take Your Cyber Defense Marketing



To The Moon and Back!

Only with Cyber Defense Media Group

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefensenewswire.com
www.cyberdefensemagazine.com
www.cyberdefenseprofessionals.com

Global Cyber Security Network



A new kind of talent agency.



Join us now at www.GCSNO.com

R9B

DELIVERING THE NEXT EVOLUTION IN MANAGED SECURITY WITH HUNT



R9B is changing the way companies **think** about managed **cybersecurity**.

We take a **proactive approach** that combines rapid, **real-time data analysis** with **human-led** threat hunting operations. The era of **passive security is over**.

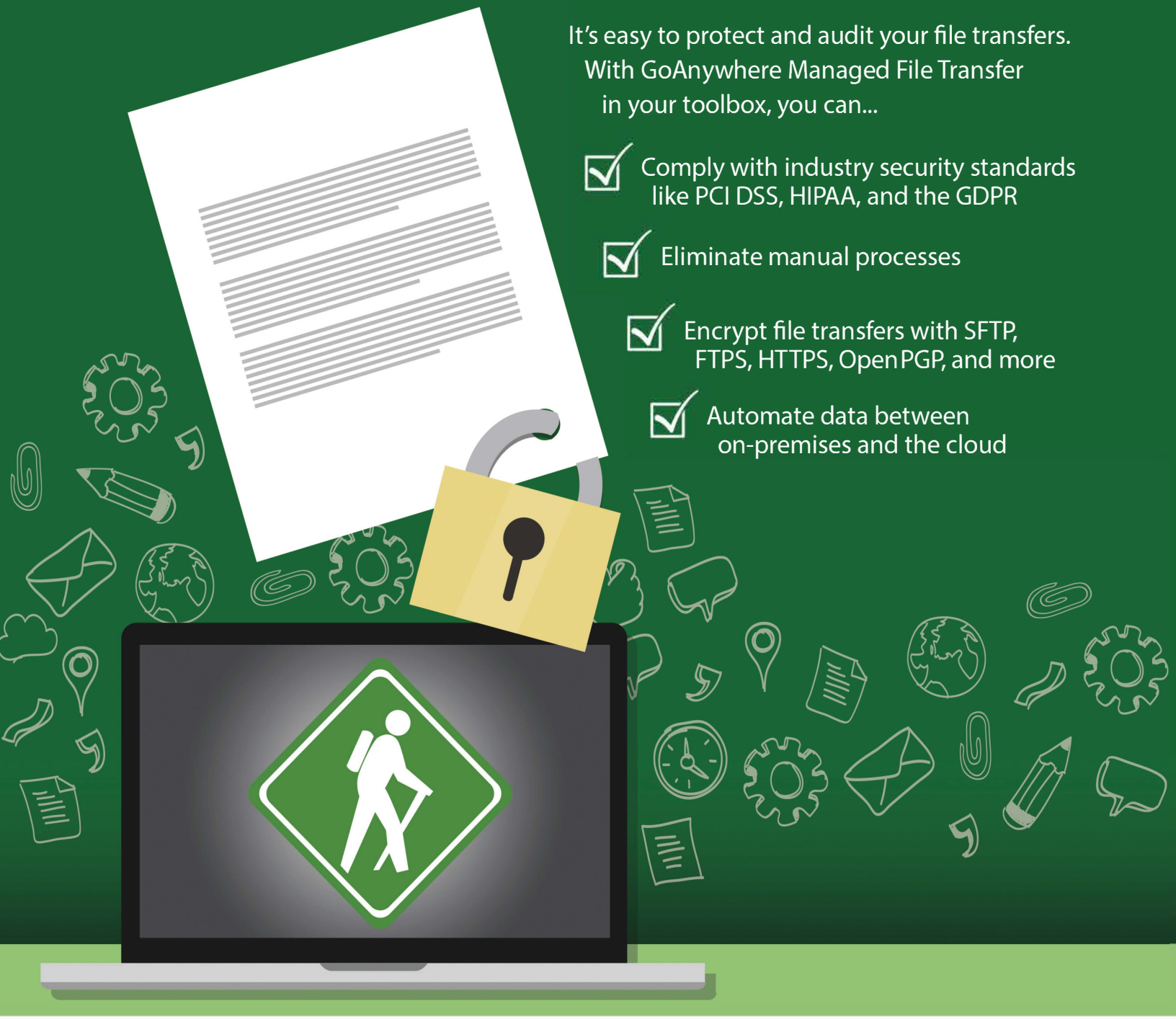
Join the **HUNT**.

FOR MORE INFORMATION

ROOT9B.COM/RSA

HUMAN-LED. TECHNOLOGY-ACCELERATED.

Simplify and Secure Your File Transfers



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

- ☑ Comply with industry security standards like PCI DSS, HIPAA, and the GDPR
- ☑ Eliminate manual processes
- ☑ Encrypt file transfers with SFTP, FTPS, HTTPS, OpenPGP, and more
- ☑ Automate data between on-premises and the cloud

See what GoAnywhere MFT can do in your organization.

Stop by RSA booth 150 in the South Hall.

GO ANYWHERE®
Managed File Transfer

www.goanywhere.com/managed-file-transfer