CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

2018 GLOBAL ANNUAL EDITION

Sponsored By

TREND MICRO™

WELCOME ABOARD

In my sixth year since we founded CDM as Editor-in-Chief, I am delighted to welcome our readers to the 2018 Global Print Edition of Cyber Defense Magazine (CDM), which is now exclusively in print at IPEXPO Europe 2018. Every aspect of IPEXPO Europe touches upon something related to cybersecurity – whether its writing better code, as developers, to rolling out internet of things (IoT) devices to blockchain or artificial intelligence – we see the need for more cybersecurity professionals who can respond to and plan for the next wave of threats and exploitations by cyber criminals.

It's now projected that there will be some 2 million new jobs created in the cyber security industry over the next 3-5 years. Indeed, some reports even project greater growth than that. In any case, what's clear is that the threats of cyber attacks are not going away; if anything, they will grow in intensity and pervasiveness as the potential payoffs get richer.

Although the three principal reasons for cyber criminals to operate remain the same, their relative growth may become skewed toward financial and political gain. Only the thrill-seekers with little to gain other than some warped sense of power appear to have leveled off. Rich targets of financial assets in the billions have come into play with the proliferation of cryptocurrencies and exchanges. The use of cyber means to penetrate and influence political processes is only beginning to be fully investigated. The challenges for the defenders of cyber integrity continue to grow.

Nonetheless, the "good guys" are in the hunt, with new and creative technological developments to counter the spread of cyber attacks. AI, ML, IAM, and Cyber Risk Management as a Service (too new for its own acronym) are among the coming techniques of cyber defense. Without attacking the attackers, there are new deception-based techniques to at least slow them down and try to document their attacks in more detail.

Therefore, only by keeping up to date with the broad array of developments is it possible for the cyber defense professional to operate effectively. That's the job of Cyber Defense Magazine – to be the principal repository and distribution channel for the vital information flow to keep us all informed and ready to respond to the threats as they emerge.

On behalf of our entire team, we thank you for being a part of the CDM community, and for supporting our mission – to help you get one step ahead of the next threat.

Respectfully,

Pierluigi Paganini

Editor-in-Chief

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CONTENTS

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

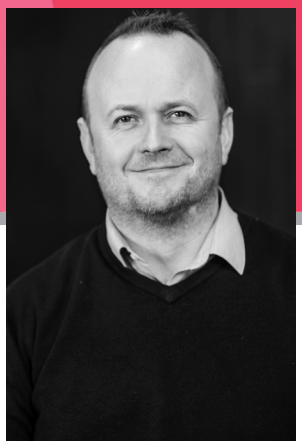
EDITOR-IN-CHIEF
Pierluigi Paganini
Pierluigi.paganini@cyberdefensemagazine.com

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

To Reach Us Via US Mail:
Cyber Defense Magazine
PO Box 8224
Nashua, NH 03060-8224
EIN: 454-18-8465
DUNS# 078358935



Welcome to IP EXPO Europe 2018

By
Bradley Maule-ffinch,
EMEA Portfolio Director
Imago Techmedia

Our umbrella event theme this year is Digital Transformation. In the race to become more agile, people-oriented, innovative, customer-centric, streamlined and efficient, Digital Transformation is profoundly transforming technology strategies for all types of institutions.

With new opportunities presented by cutting edge technologies such as Blockchain, AI and Internet of Things, IT teams are increasingly challenged to work together efficiently and keep the lights on, whilst innovating to deliver cost and operational efficiencies and competitive advantages. Across all these innovative and engaging technologies, we have Cyber Security as something that must be considered, up front – in code, in design, and in our investments.

This year, IP EXPO Europe rises to the proverbial challenge to "be all things to all people" in the context of six key aspects of IT practice. With six top IT events under a single roof, including 300+ exhibitors and 300+ free to attend seminar sessions, the Digital Transformation taking place in the IT world is fully captured in our multi-disciplinary structure.

The event showcases brand new exclusive content and senior level insights from across the industry, as well as unveiling the latest developments in IT. IP EXPO Europe now incorporates:

- IP EXPO
- Cyber Security X
- Developer X
- AI-Analytics X
- Internet of Things X
- Blockchain X.

IP EXPO Europe has evolved alongside the modern enterprise IT department for over 10 years, uniquely covering the entire IT stack. Regardless of your role or responsibility within your organization, if you are into any aspect of IT, this is the event for you, and we appreciate your active participation.

You will learn about the latest Cyber Security developments in expert-led sessions, inspiring keynotes and in-depth seminars. At the exhibit hall, you can demo innovative products and solutions, network with information security insiders and peers, and help move the industry forward as part of an engaged and empowered global community.

We're thrilled that you are joining us here on 3-4 October 2018 at ExCeL London, as IP EXPO Europe is Europe's number ONE IT event for those looking to find out how the latest IT innovations can drive their business forward. We're expecting a record attendance of over 16,000, and every participant has something of value to share with others and also to take away and put into practice.

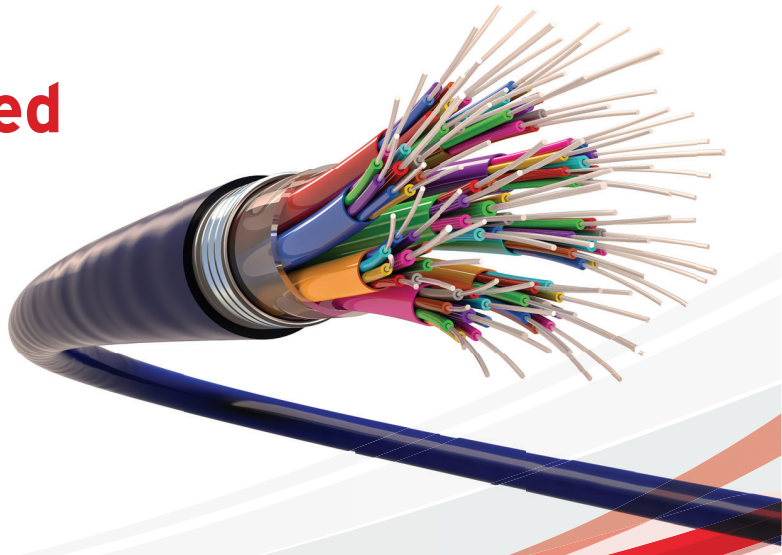
IP EXPO Europe is the must-attend IT event of the year for CIOs, heads of IT, security specialists, heads of insight and tech experts. The Digital Transformation EXPO brings together the full range of technologies needed for a business to successfully embrace digital change.

Arrive with challenges, leave with solutions!

In partnership with the Cyber Defense Media Group – you'll find opportunities within this Cyber Defense Magazine, or to be interviewed or watch Cyber Defense TV and see many winners on the show floor of the prestigious Cyber Defense Awards and with a big thanks to you, to all of our sponsors and exhibitors, welcome to IP EXPO Europe 2018!

The IP EXPO Europe Team

Detect and prevent breaches at wire speed



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

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

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

Proven capability

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

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

Industry leading threat intelligence

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

www.trendmicro.co.uk/xgen-cyber

Firefighter or Bricklayer? The Right Approach to InfoSec

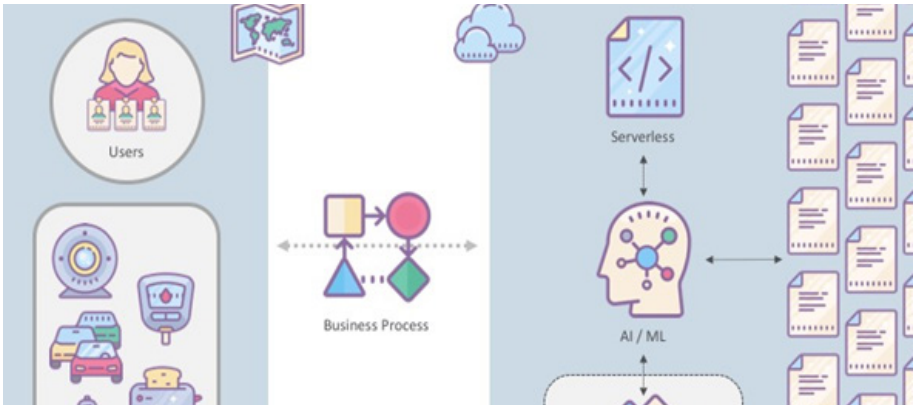
by Rik Ferguson, Vice President Security Research at Trend Micro

The professional life of a security practitioner is a fast-paced one. Constantly having to respond to the shifting tactics of the adversary, having to understand and secure new infrastructural implementations and delivery platforms, and both facilitating and yes, mitigating the changes in user behaviour over time. All too often the enterprise still thinks of the security function as a bolt-on one. The business is structured, the architecture implemented, and the employees are hired. The fires are started and then someone calls the security team; "Secure this".

"Firefighting" for many years has been the default operational mode of an information security department. To borrow from Bono, we are running to stand still. Securing infrastructure as it is implemented, responding to breaches after they happen, patching vulnerabilities once the exploit is already in the wild, auditing inventory already in use is barely workable now, what of the enterprise of the future?

The single biggest infrastructure change just over the horizon is the advent of 5G in 2020. 5G promises a wealth of benefits (many of which we have experienced more than once before) much greater bandwidth, faster connectivity with lower latency over a wider geographic area to many more devices, in the same way achieved by previous iterations (2G, 2.5G (GPRS & EDGE), 3G, 4G/LTE). While standards are still being finalised, what is important to note with 5G is that it follows the same KPI trend as those previous iterations, so we can expect an order of magnitude improvement over 4G in things like data rate, and critically in latency.

What 5G promises is a scaled-up infrastructure that in itself will drive change in many other areas, just as the advent of 3G drove the advance of the smartphone, and 4G the streaming services that are steadily replacing conventional media. Except this time 5G with its really low latency and high bandwidth has caught the attention of industry and not just the consumer. We will be connecting not only the traditional "fixed internet", today's "mobile internet" but also every sensor and actuator, every vehicle, traffic management system, smart city, smart home and factory on the planet. 5G will be the foundation of a truly immersive interconnected experience.



From a security perspective, therein lies the real challenge.

A greater volume of traffic, a greater number of endpoints (many with no user interface at all) and an ongoing explosion of data means not only that we have more to secure, but more to secure it from. This is already driving a huge shift in the way we do business, driving adoption of IPv6 (to accommodate all these new devices), Software Defined Networks, big data and cloud services to store and process the volume of data, and Artificial Intelligence and Network Function Virtualisation to provide scale and speed of response and an ability to integrate security functions at carrier level, rather than relying on an ability to enforce at every endpoint in this new interconnected world.

One vision of the enterprise of the future looks like this. Your organisation ignores the network infrastructure from a security perspective, all infrastructure is considered as hostile and a zero-trust model is applied. You have multiple thousands of end-users spread across the globe and every user has multiple profiles that need to be automagically applied in the correct circumstances (where are they, what are they using, what task are they working on, what time of day is it?). On top of that you have hundreds of millions of connected "things", devices, sensors, actuators, vehicles, factories each with its own unique use case, environment and vulnerabilities. IT solutions are tied directly to business requirements, stripped to the essentials required for the job, no more "IT for IT's sake".

Of course, an inevitable outcome of this is a continued exponential growth in data generation. Consider that 90% of all the data ever generated by the human race has been generated in the last two years and extrapolate from there…

Our future business will rely on the scale and speed of Artificial Intelligence and Machine Learning to cope with these mountains of data and the Security Operations Centre will be no exception. Integration of Machine Learning into the SOC of the future is critical for a number of reasons, not only related to the volumes of data, but also to address the so-called "cyber skills gap" (a concept I'd love to dissect in a future article maybe). We need to leverage the power of machine learning to collect and correlate data from across the enterprise, carry out triage of generated events, forensic investigation and evidence capture, and yes even mitigation; surfacing only those urgent or high-priority event to the humans who remain at the top of the security tree.

Firefighting as means of maintaining a secure enterprise is not a workable model for the future, or even the present. No one can deny, that even if your firefighting is of the highest calibre, you will systematically end up with fewer trees to burn in the long run. In our field of information security, it's so much better to be a brick layer than a firefighter. Measure twice, even three times if you have to, and then lay the bricks once.

About the Author

Rik Ferguson Vice President Security Research at Trend Micro, is one of the leading experts in information security. He is also a Special Advisor to Europol's European Cyber Crime Centre (EC3),. In April 2011 Rik was inducted into the Infosecurity Hall of Fame.

As a presenter at global industry events such as RSA, Mobile World Congress, Milken Institute, Virus Bulletin, RUSI and the e-Crime Congress, Rik addresses the challenges posed by emerging technology and online crime. He is frequently interviewed by the BBC, CNN, CNBC, Channel 4, Sky News and Al-Jazeera English and is quoted by national newspapers and trade publications around the world.

Rik is actively engaged in research into online threats and the underground economy. He also researches the wider implications of new developments in the Information Technology arena and their impact on security, both in the enterprise and for society as a whole, publishing papers, articles, videos and participating in thought-leadership initiatives. With twenty-five years' experience in information security, Rik has been with Trend Micro since 2007. Prior to assuming his current role, he served as Security & Privacy Infrastructure Specialist at EDS where he led the security design work for government projects related to justice and law enforcement and as Senior Product Engineer at McAfee focused on network security, intrusion prevention, encryption and content filtering. Learn more about Rik and the latest security technologies from his team at http://www.trendmicro.com

SECURE YOUR DIGITAL BUSINESS

Applications ***are*** the business in this digital age. Securing the applications that drive your business is essential to providing safe digital experiences to your entire business ecosystem.

The WhiteHat Application Security Platform is a cloud service that allows organizations to bridge the gap between security and development to deliver secure applications at the speed of business.

4 Encryption Technologies You Should Use

by Dan Freeman, Senior Solutions Consultant, HelpSystems

How are you encrypting data in your organization?

The number of users, clients, and organizations who access the internet to share data is growing. In the last year, it's been estimated that over 3.8 billion people use the internet to shop online, check their banking information, continue their education, access test reports from their healthcare providers, apply for jobs, and submit annual tax documents. These activities all require the submission of personal data: usernames, passwords, social security numbers, birth dates, credit card information…. The list of what's shared on the internet is lengthy and complex.

As people submit, transfer, and store sensitive data online, it's imperative for organizations who handle this information to protect it using strong encryption practices. This especially applies to businesses who need to meet state, federal, or industry compliance regulations. Using homegrown encryption methods or, worse, sending communication in the clear (with an FTP server or client) just isn't satisfactory or secure anymore. Cyber crime is evolving. Without proper encryption for your file transfers, it's only a matter of time until vulnerable organizations are hit with a data breach that costs them money or potentially puts them out of business forever.

Finding the right method of encryption for your organization can be overwhelming, but the alternative—compromising your customers' or employees' personal information—isn't acceptable. Don't

let a data breach happen to you. Take the time to find an encryption technology that works in your environment and protects your file servers from vulnerabilities.

To get you started, here are four modern encryption technologies we recommend using:

1. OpenPGP

OpenPGP is an encryption protocol that uses key pairs (a public and private key) to secure your files. If you need to use public and private keys in your organization to give your data a high level of protection, this may be the protocol you want to use. OpenPGP also allows you to verify the authenticity of received data by requiring files to be signed with the digital signature of the message creator.

2. TLS

Transport Layer Security (TLS) is a cryptographic encryption protocol that allows users to encrypt their file transfers over industry standard protocols like AS2, FTPS, and HTTPS (to secure web browser connections). TLS uses x.509 certificates to allow TLS-enabled servers and clients to securely connect to and authenticate each other.

Since these certificates contain information about the entity they represent, TLS provides a high level of protection by requiring specific certificate details (e.g. the entity that signed the certificate, the expiration date, the certificate's public key, and the entity's digital signature).

Helpful Tip: The Payment Card Industry Security Standards Council recently increased the version of TLS organizations should use to remain compliant. If you follow PCI DSS requirements, as of June 2018 you should use TLS 1.1 or higher for your encryption needs. (TLS 1.2 is strongly encouraged.)

3. SSH

Secure Shell (SSH) is a cryptographic network protocol that encrypts file transfers over industry standard file transfer protocols like SFTP and SCP. For organizations who need a bit more flexibility in their authentication methods, SSH uses a combination of asymmetric and symmetric cryptology to provide strong protection. Files that are transferred using SSH can be set up to authenticate using passwords, SSH keys, or a combination of both.

Helpful Tip: Some secure file transfer solutions support SSH with an integrated Key Management System (KMS). This KMS can be used to create and maintain SSH keys, OpenPGP keys, and SSL certificates that are then associated with a TLS client connection. It is highly recommended that you use a solution that offers this benefit, as it reduces the need to create manual keys and certificates in your organization, thus promoting centralized management.

4. AES

The Advanced Encryption Standard (AES) is a symmetric form of encryption cipher that organizations can use to protect their files when stored in transit or at rest. AES-256 encryption is often employed to secure data at rest by encrypting the folders sensitive files are stored in.

Some secure file transfer solutions automate this process by encrypting the data as it's written to files within a designated folder. Files can be decrypted whenever they're accessed by an authorized user, so the user doesn't have to provide a special password or key.

Helpful Tip: Are you FISMA compliant? The Federal Information System Modernization Act of 2014 calls upon the National Institute of Standards and Technology as its security and risk approached framework to ensure proper file and systems protection. AES is the de facto standard and widely accepted encryption method.

No matter which encryption option you choose for your organization, always ensure your data is protected in transit and at rest. With the amount of personal information shared and stored online, data breaches are becoming more and more common. Don't let one happen to you!

About the Author

Dan Freeman is a Senior Solutions Consultant at HelpSystems for the GoAnywhere Managed File Transfer product line. Dan has spent the last 10 years of his career in various security roles ranging from systems engineer to security officer. As a CISSP, Dan has designed networks, systems, and procedures to ensure regulatory compliance using the NIST risk management framework and HIPAA standards. Dan can be reached online at Dan.Freeman@helpsystems.com and at our company website: www.helpsystems.com

REAL-TIME CONTINUOUS DIAGNOSTICS & MONITORING

SHINE A LIGHT ON THE DARKEST CORNERS OF YOUR NETWORK

STIGs & Configurations

Continuous audit of policies & controls.

Threats & Vulnerabilities

Real-time discovery of Threats & Risk.

Asset Discovery

Automatic inventory & tracking of assets.

User & Entity Behavior

Monitoring of risky & unsanctioned activity.

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

Look no further...

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

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

AristotleInsight®
— Identify | Remediate | Document —

AristotleInsight.com | 866.748.5227

Defend against Cloud-based Data Theft with Identity Access Management (IAM)

by Lewie Dunsworth, CISSP, CISO & SVP, Herjavec Group

Phishing attacks will soon become 'so last year' in comparison to cloud-based data theft. Whether you, as a business, have begun to leverage SaaS based cloud applications or have started the arduous task of migrating your entire data center, leveraging IaaS solutions, the cloud has become a greater target for your organizations data and opened a new door for exploitation.

It's no wonder that an internet search for Identity and Access Management (IAM) returns so many results. In a relatively short time, security practitioners have quickly realized how important an identity is in protecting an organization. It's become a central theme to the point where organizations are adopting "identity centric" programs and put pressure on the cyber defense community to develop better solutions that balance usability and security.

Statistics show that the great majority of data breaches and other events of unauthorized access to sensitive information come from human vulnerabilities and the access they possess. Beyond that, the value of information stolen from cloud-based sources tends to be far greater than from other storage locations, partly due to the size and scope of the data bases and because of the dependence and complexity of integrating additional layers of security in cloud-based environments.

As information security practice shifts toward AI, ML, and other means of protection, a strong identity posture starts with understanding what data you are trying to protect, who has access to the data and understand whether that access is being used in a legitimate or illegitimate manner. Once that is understood, baseline identity techniques start with restricting the access of organization employees, based on least privilege, to the sensitive information sought by cyber criminals. Because the cloud is easy to use, and simple to scale, not only do you have the proliferation of company assets being spun up in cloud based environments but now you have to worry about who has access to the data in those environments, ensure that the external API's are locked down and you have the appropriate monitoring in place to identify suspicious/malicious behavior. So, not only do you have to worry about infrastructure and application vulnerabilities in those environments (specifically in IaaS) but there is concern about who is now accessing that information, from where and what they are doing with it. Strong identity practices and programs ensure that you have the appropriate processes in places to define roles appropriately for cloud based systems.

They also monitor the access and location, deprovision access when it's not needed and govern other changes in the access of your users. The key is visibility and governance An oft-cited example is the well-meaning but dangerous employee behavior of provisioning and running unknown applications in the cloud; while they may be trying to be innovative, create shortcuts or add functionality to the company's operations, they may in fact introduce incompatible programs, new vulnerabilities, and unnecessary access to systems. By creating a culture around access, its importance, least privilege and identity controls, you can create a well-rounded identity program.

Professionals engaged in Identity & Access Management programs have recognized that the one of the fastest growing unmanaged risks to the integrity and confidentiality of sensitive company information is excessive employee access. Beyond the internal storage of such data, such facilities as mobile devices, cloud storage, growth of the Internet of Things, and IT consumerization offer rich targets for increasingly sophisticated cyber-attacks.

Following the instincts of our CEO, Robert Herjavec, the visionary founder of Herjavec Group (HG) (link to herjavecgroup.com), the company took the lead in addressing the challenges posed by developments in the world of Identity. Since its acquisition of Aikya Security Solutions in 2016, HG has built on this base of experience and expertise to become a leading provider of Identity services.

At Herjavec Group we believe in supporting what we view as the 4 pillars of identity (link to https://www.herjavecgroup.com/services/identity-services/):

1. Identity Governance & Administration
2. Privileged Access Management
3. Access Controls
4. Identity Managed Services

Identity programs are highly complex and traditionally difficult to implement at scale. We're here to relieve the burden of integrating this layer of protection into your overall company security posture. The net effect of HG's Identity approach is to lead a client through the identity, access and management journey. It starts with defining a custom strategy based on your specific needs, designing a solution that marries together people, process, technology, and of course the deployment of technical solutions that meet your specific requirements. You've also got to ensure in house or external expertise and scale to manage the environment. The objective is to streamline your processes, improve end-user experience, enhance security and enable compliance.

I'm proud of the holistic and dynamic approach we take to Identity Services. Our "Pillars of Identity" perspective is more than a slogan. We offer a set of services that apply across each pillar:

- **Assessment**
  - o Process Review
  - o Business Requirements
  - o Strategy & Roadmap Planning
- **Design**
  - o Identity Solution Architecture
  - o Access Governance Framework
  - o Single Sign On (SSO) Framework
  - o Role Mining, Modeling & Engineering
  - o Cloud Identity Security
  - o Privileged Access Framework
- **Deployment**
  - o Solution Install & Configuration
  - o Solution Deployment Supporting
  - o Testing & Validation
  - o Production Migration
  - o Integration opportunities to maximize technology
  - o investment – SIEM, DLP, endpoint
- **Managed Identity Services**
  - o 24x7 IAM Platform Monitoring
  - o Basic and enhanced configuration support
  - o Onboarding services to automate and
  - o operationalize provisioning & de-provisioning

If you haven't begun to consider Identity Services as part of your security framework, know this – your business may be scalable and running more efficiently through the cloud but you've opened the door to a new world of exploitation and data theft. Isn't it time you considered Identity?

About the Author

Lewie Dunsworth is Senior Vice President of Professional Services & CISO 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). Learn more about Lewie at https://www.herjavecgroup.com/about-us/executive-team/

5 Steps to Keeping Your Company Compliant in the GDPR Era

By Andrew Clearwater, Director of Privacy and Linda Thielová, Data Privacy Counsel, OneTrust

With the Global Data Protection Regulation (GDPR) effective and inevitably becoming a part of the European legal landscape, a new stage comes for everyone, prompting a question: what now? Here are a few tips to help you keep up-to-date with the development of data privacy requirements.

1. Look out for domestic legislation and EDPB guidelines

The GDPR is still young legislation, so many EU laws containing additional specific privacy requirements still await their effective date. We can also expect the newly established European Data Protection Board ("EDPB") to gradually fill in the blanks and clarify certain issues regarding the interpretation and enforcement of the GDPR.

2. Keep your GDPR compliance framework up-to-date

GDPR compliance should be an ongoing exercise, not a means to an end. Schedule regular privacy check-ups and audits to ensure your organisation's compliance framework remains operational.

3. Make Privacy by Design a constant effort

Privacy by Design gained major traction through GDPR as a concept aiming for more in-depth approach beyond merely addressing privacy as an afterthought. Privacy by default, its important element, seeks to deliver maximum degree of privacy by ensuring that personal data are automatically protected by any system or business practice. These principles can only be achieved by becoming an everyday part of your company's operations.

4. Keep up with Codes of Conduct

GDPR foresees the approval of codes of conduct and accreditation of certifications to help organizations demonstrate compliance with data privacy requirements and best practice. Codes of Conduct may even be binding for certain professional associations and as such may potentially apply to your organization by virtue of membership(s).

5. Get Ready for ePrivacy

The main concern of the not-yet finalised ePrivacy Regulation will be the online tracking and use of cookies. A good practice is to keep an eye on what cookies are being used on your company's websites and be clear about whether these are 1st party or 3rd party, what sort of data is being collected and who is the data controller in each case.

For more tips about privacy regulations and how to tackle the GDPR, visit onetrust.com.

About the Author

Clearwater and Thielová work on the OneTrust privacy team. They provide counsel, leadership, and guidance on data protection. The OneTrust privacy team is also responsible for providing public policy analysis in the areas of privacy, data security, information policy and technology transactions. Clearwater is a Certified Information Privacy Professional (CIPP/US), holds an LLM in Global Law and Technology and is a licensed attorney. Thielová is also a Certified Information Privacy Professional (CIPP/E, CIPM) holds a degree in Law and Legal Science and has a four years' professional experience in privacy.

Andrew Clearwater

Director of Privacy, One-Trust

Linda Thielová

Data Privacy Counsel, OneTrust

This Company Stopped a Phishing Attack in 19 Minutes

by Cofense, Inc.

It was an ordinary day for employees of a national healthcare company. Lots of emails on the usual subjects: meeting invites, questions from colleagues. Nothing really special. But when employees received a message from their CEO, they snapped to attention.

The email asked them to read and agree to a company policy. Simple. Just click on a link, which took them to a login page—from there, they'd enter their credentials and go to the policy page.

But the sender wasn't the CEO. He was a talented fraudster.

The attacker aimed to harvest passwords, gain file system access, and reroute electronic payroll deposits. And he almost succeeded.

Let's take a minute-by-minute look at the phishing attack—and how Cofense combined employee-sourced intel and automated analysis to work with company's security team and mitigate in less than 20 minutes. For security reasons, the company will remain unnamed.

11.48 a.m. The spear phishing campaign launches.

The email showed the attacker "had really done his homework," according to the company's Vice President of Information Security. "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.1 Most BEC scams ask their targets to wire funds. In this case, the attacker used credential phishing to reroute electronic transfers himself.

11:49 a.m. Employees begin reporting the email as suspicious.

The email was quite convincing. Many employees clicked. Fortunately, enough well-trained users looked at the message carefully. The company uses Cofense PhishMeTM for phishing awareness training. It also equips users with the Cofense ReporterTM plug-in to report suspicious emails with a single click.

One of the simulated phishes the company had used in training spoofed the HR department—like the email the real attacker sent, the simulation asked users to click an embedded link to agree to a policy. When they encountered the real deal, alert employees reported it a minute after the attack began.

11:49 a.m. Reported emails go to Cofense TriageTM for machine and human analysis.

The company relies on Cofense Managed Triage for phishing response. Reported emails first undergo automated analysis. Then human analysts at the Cofense Phishing Defense Center (PDC) investigate further to verify whether an email is malicious.

PDC research shows that crimeware as a percentage of reported emails can range from practically nothing to over 90% monthly. From one month to the next, it's not unusual for a company to see dramatic swings.

12:00 p.m. The investigation escalates.

As users reported more emails and more evidence emerged, the PDC escalated the initial investigation. The threat analyst conferred with his manager on duty. Cofense Triage groups malicious emails into common clusters. Further, the PDC team applies human intelligence to confirm a phishing campaign.

The approach combines the best of both worlds. Automation greatly accelerates email analysis at scale, while human vetting makes use of insights machines can't deliver.

12:07 p.m. Cofense completes the investigation and alerts the company.

Upon wrapping up the investigation, the PDC called the company's VP of Information Security. Cofense Triage automation and human expertise enables the company to respond to the threat in real time. The possibility of a breach is detected in minutes, not months.

Not bad, when you consider that IBM Security and the Ponemon Institute report the average business detects a breach in 196 days2—and that most breaches begin as phishing emails.

12:07 p.m. The healthcare company responds.

After consulting with Cofense, the company blocked the phishing site and began to mitigate the attack. Incident responders retracted the bad email from inboxes, monitored behavior from affected Office365 accounts, and disrupted any lateral movement.

"We removed the email quickly," said the VP of Information Security, "though in the space of a few minutes a lot of people clicked. Once we contained the threat, we started on repair and recovery work, seeing who clicked and mitigating problems linked to their accounts."

"All of this was the result of a single well-crafted phishing email."

The VP of Information Security adds, "If we hadn't been prepared, the damage would have been worse. We were able to retract the email in under 20 minutes."

Good thing this company had built a complete, collective phishing defense, protecting against phishing attacks from the inbox to the SOC. By striking a balance between automation and human intuition, the company was ready when trouble loomed—and equipped to prevent a disaster.

By Cofense CTO and Co-Founder Aaron Higbee

Aaron Higbee,
Chief Technology Officer and Co-Founder

Aaron is the Co-Founder and CTO of Cofense (formerly PhishMe), Inc. directing all aspects of development and research that drives the feature set of this market leading solution. The Cofense method for awareness training was incubated from consulting services provided by Intrepidus Group, a company that Aaron Co-Founded with Rohyt Belani in 2007.

Aaron remains on the board of directors for Intrepidus Group to ensure it focuses on forging new service lines and attracting motivated researchers and consultants.

Before Cofense and Intrepidus Group, Aaron served as Principal Consultant for McAfee's Foundstone division where he was a lead instructor and known for his ability to mentor and develop junior consultants into expert penetration testers. Prior to his seven years of consulting experience, Aaron worked for large Internet Service Providers handling security and abuse incidents, subpoena compliance, and datacenter security. Aaron's biggest achievement is building industry recognized Intrepidus Group and incubating Cofense out of it.He enjoys the diverse personalities in the information security community and is known for building creative environments needed to promote rich personal and professional development. His creative touch is evident in the unique way he recruits and retains talent and his style further extends itself into his leadership role at Cofense. Aaron is a speaker at regional conferences and associations as well as large conferences such as BlackHat, DefCon, Shmoocon, etc. His expert opinion is a valuable resource for many media outlets interested in security.

WE STOP THE PHISHING ATTACKS YOUR OTHER TECH MISSES.

PHISHME *IS NOW* COFENSE

Cofense combines best-in-class incident response with employee-sourced attack intel. Stop attacks in progress and stay ahead of breaches. With Cofense, you'll experience **the power of the collective.**

Learn more at **COFENSE.COM**

How AI and Automation Can Solve Your Security Hiring Problem

by Aarij Khan, VP Marketing, Securonix

Cyber attacks are increasing in volume and complexity, and affecting more people and costing more money. Last year 1,579 breaches were reported (source: ITRC), costing an average of $3.62 million per breach (source: Ponemon Institute).

Security teams simply can't keep up. Organizations struggle to manage the deluge of security alerts. Existing CSIRT and SOC teams are stretched. Meanwhile thousands of security job openings go unfilled. According to ESG, two-thirds of security professionals claim they are too busy to keep up with skill training and development. Enterprises are left to tackle security with entry-level analysts and hope for the best.

One answer to this problem is to incorporate AI and automation, with innovations like Securonix ResponseBot. ResponseBot is a new capability within Securonix Security Analytics, and uses machine learning to learn the responses of highly experienced security experts. Once the behavior is learned, ResponseBot can automatically execute response actions for specific cybersecurity alerts. Automation executes routine tasks, such as quarantine, forensic data collection, etc., reducing the overall level of manual effort required.

"We constantly hear that cybersecurity experts are in extremely high demand and organizations do not have enough trained personnel to address the flood of security incidents they face," says Tanuj Gulati, CTO and co-founder of Securonix. "Securonix's ResponseBot arms junior security analysts with the information and expertise of a highly advanced SOC analyst, enabling them to address complex cybersecurity alerts right away."

Leveraging machine learning with security analytics can relieve the stress on cybersecurity analysts and help reduce incident response time by up to 95 percent. Junior analysts can increase efficiency by following AI-based guidelines, essentially operating like more experienced staff. Senior analysts are then freed up to tackle the truly challenging cybersecurity issues, resulting in a 300-500 percent improvement in threat detection and remediation times.

About the Author

Aarij brings a deep understanding of the security market and buyer combined with over 15 years of marketing leadership at high growth, innovative security vendors. Previously, Aarij led marketing efforts at RiskIQ where he was responsible for product marketing, analyst and public relations strategy, channel marketing, field marketing, and growth. He also led product and solution marketing at Tenable Network Security, ThreatMetrix and had spent over 4 years at ArcSight/HP where he was instrumental in the rapid adoption of ArcSight SIEM products.

SECUTECH
www.eSecuTech.com

NO MINIMUM ORDER!
FREE EVALUATION REQUESTS AVAILABLE!
FREE DELIVERY FOR ONLINE ORDERS PROMOTION

UniMate® Family

- UniMate® USB/USB Mini
- UniMate® STD
- UniMate® Flex

FIPS 140-2 (Level 2) Certified

PKI Two Factor Authentication Smart Card Token for PC (USB) and for mobile (3.5mm TRRS audio)

UniOTP® Family

- UniOTP® 300/500:

OATH Compliant One Time Password (OTP) Token, both Event (button press) and Time (60s) options available.

OEM Customization

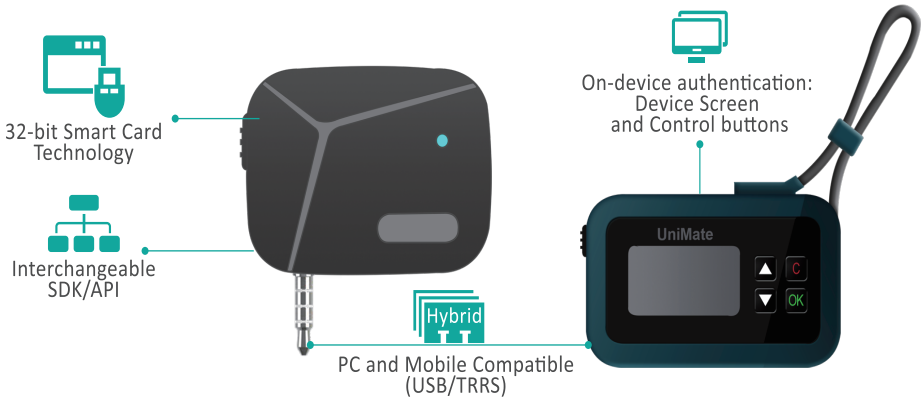
	*Logo Customization*
	*Case Options*
	*Color Options*
	*Device Naming Service*
	*CSP Naming Service*
	*Encryption algorithm customization*

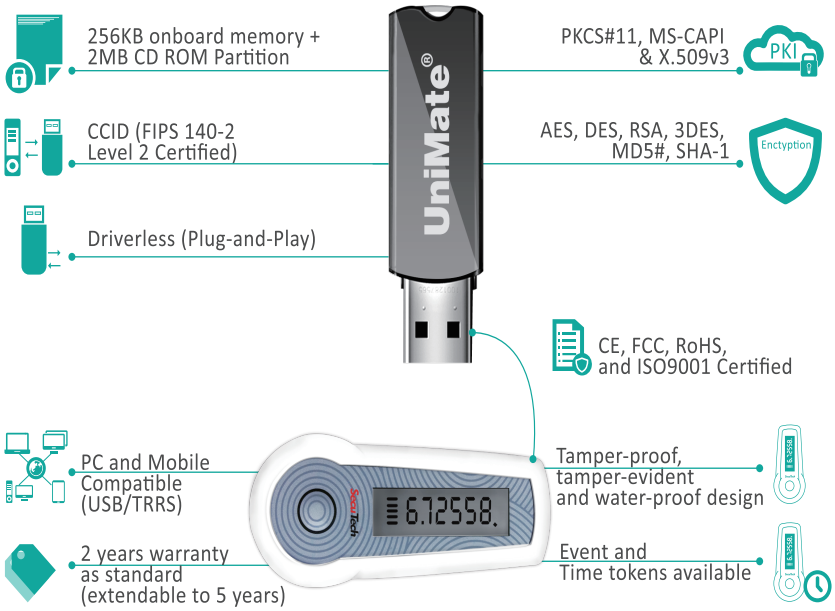
CHINA CITIC BANK CFCA
BOSCH CHINA HUARONG
BROADCOM SonoSite

From high profile banks to local administrators:

A COMPLETE SUITE OF TWO-FACTOR AUTHENTICATION (TFA) SOLUTIONS

in one place (PC to mobile)





SecuTech® is a global leader in providing hardware based software protection & licensing options, as well as strong authentication for Windows, iOS, Linux and Mobile based systems, with a wide array of flexibility that tailor to varying business needs. Our technology and technical expertise is provided to thousands of customers including: Boeing, Bosch, JVC Kenwood, Siemens, among other various banks and government agencies. Do you want to take advantage of our expertise?

Proactive Security Is the Key to Mitigating Future Threats

by Branko Primetica, The President and Chief Strategy Officer of eGlobalTech (eGT)

In today's increasingly dangerous digital environment, reactive security is not enough to effectively protect an organization from cyber threats. Reactive security includes things like securing your systems through an Assessment and Authorization process, installing firewalls, and implementing antivirus software. However, digital modernization, the expansion of cloud computing, and the Internet of Things (IoT) are resulting in a rapidly growing attack surface. In addition, humans are becoming more sophisticated when it comes to developing ways to attack networks, with Advanced Evasion Techniques becoming more common.

Proactive security, on the other hand, includes all the reactive security measures but expands them to encompass items such as actively seeking out vulnerabilities and hunting for threats to mitigate issues before they become reality. The simple objective is to enhance visibility to thwart suspicious activity and contain attacks.

Practical initial steps for transitioning to a more proactive security posture include:

1. Consolidate Your IT Security Programs. Federated organizations, at times, have multiple IT security programs. By consolidating into a single program (to the maximum extent possible), adoption of common standards and enterprise-wide detection and monitoring of intrusions becomes more possible.

2. Perform Regular Comprehensive Assessments. This includes performing assessments of IT Controls and Risks to help identify where the highest risk impact lies and where control gaps exist. These analyses will also help to drive investment in controls to close those gaps efficiently and cost-effectively.

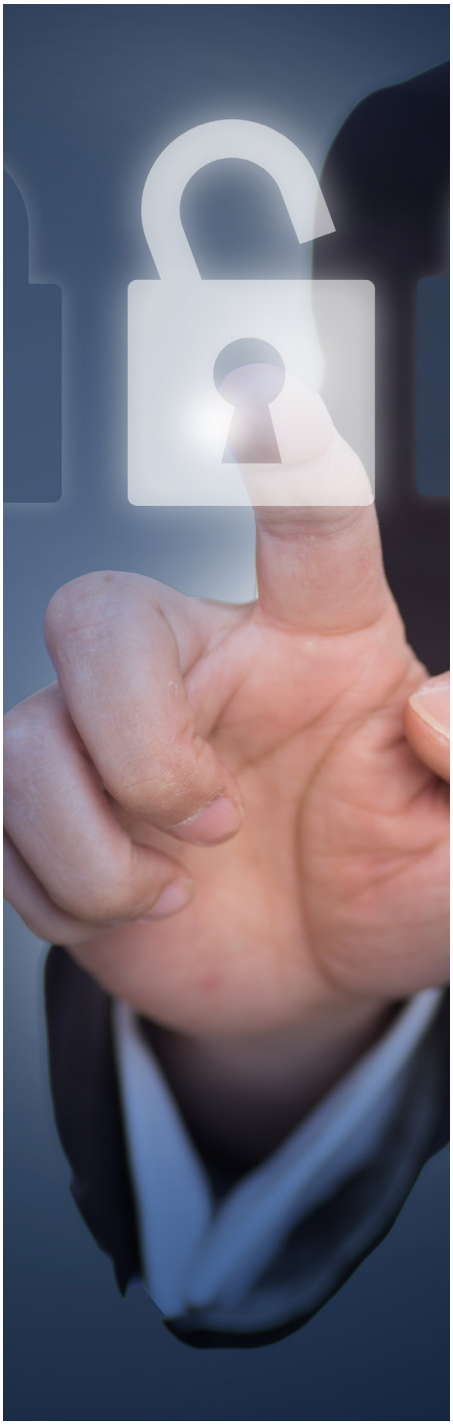
3. Raise Cybersecurity Awareness. The human factor of proactive security cannot be ignored. Employees must be taught how to identify threats and malware, and what they must do in response.

4. Establish a Program to Identify and Respond to Threats. Establishing an enterprise monitoring and response operation to hunt for and respond to threats and breaches across a network is a cornerstone of a proactive security program. This operation can achieve the visibility required to slow down and stop suspicious activity in its early stages.

5. Continuous Penetration Testing. Many organizations test their systems once or twice a year. However, their network and infrastructure evolve constantly. This means they have little to no visibility into new vulnerabilities and attacks until it's too late.

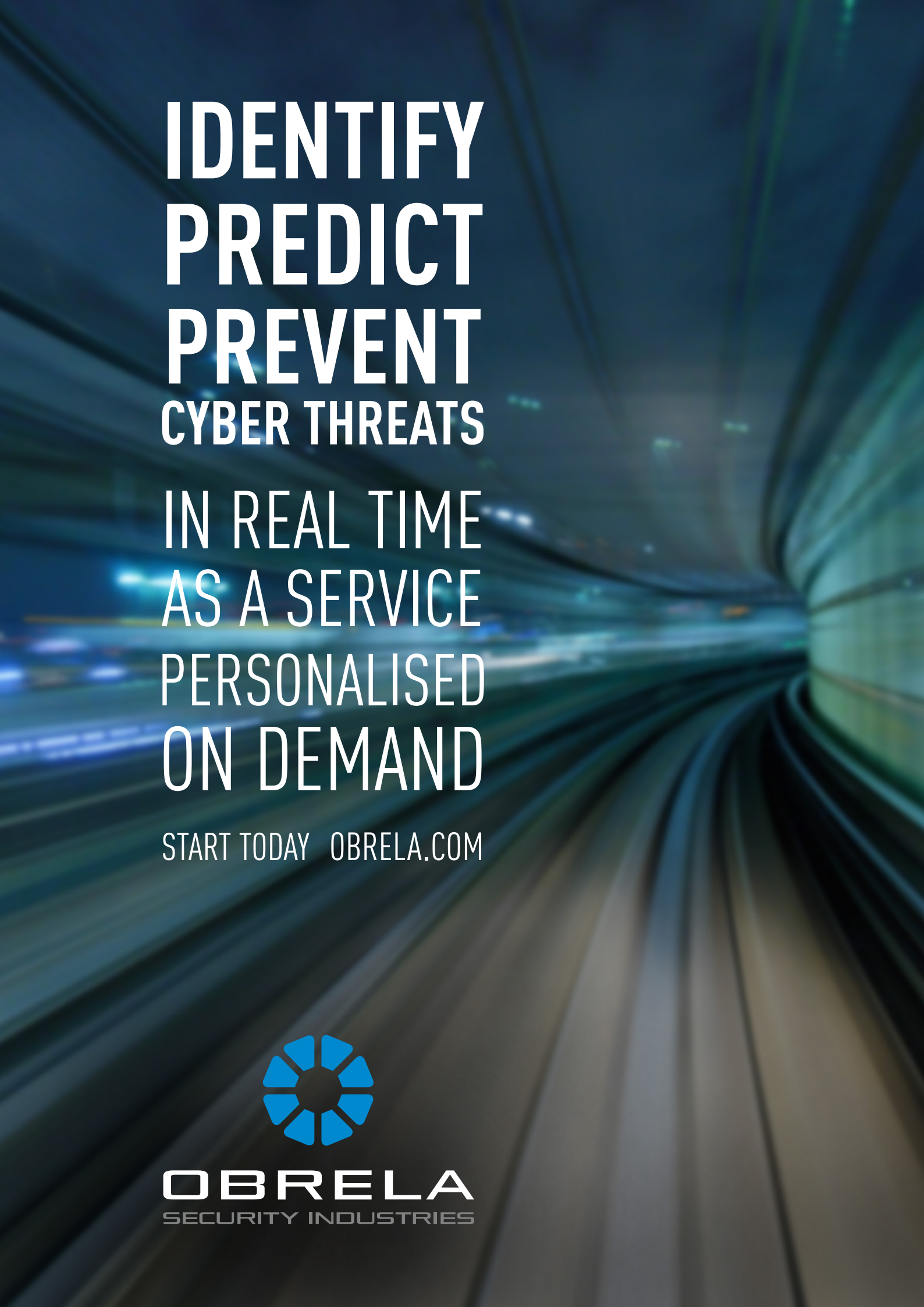
Once the basics are taken care of, organizations should move on to conducting Red Team-Blue Team exercises and carrying out simulated phishing campaigns.

A proactive security posture is based upon maintaining up-to-date situational awareness at all times. By following the steps described above, organizations can start to develop and maintain a comprehensive view of their security landscape, mitigate risk before a cyber threat becomes reality, and identify what needs to be done to improve overall enterprise security.



About the Author

Branko Primetica serves as the President and Chief Strategy Officer of eGlobalTech (eGT), a leading cybersecurity and IT solutions firm primarily supporting the U.S. Federal Government. Find out more at www.eglobaltech.com.


IDENTIFY
PREDICT
PREVENT
CYBER THREATS
IN REAL TIME
AS A SERVICE
PERSONALISED
ON DEMAND
START TODAY OBRELA.COM
OBRELA
SECURITY INDUSTRIES

THREAT INTELLIGENCE: 5 APPLICATIONS OF CONNECTED DOMAINS

by Jonathan Zhang, Founder and CEO, Threat Intelligence Platform

Many organizations are turning towards threat intelligence to reduce the occurrence of cyber attacks. Sure enough, the practice can help security specialists prevent scams and hacks in various ways. One of them, quite inevident at first sight yet effective in practice, lies in taking a closer look at connected domains.

But first thing first. How do domains connect exactly? Roughly speaking, it can happen through infrastructure in the form of shared hosting, IP addresses, and name servers, as well as common registrant details — names, physical location, emails addresses — and confusingly similar names.

There is a lot to learn from these connections as they may be at the basis of vulnerabilities in your or somebody else's cyber defense. In this article, let's look at five situations in which you probably want to check for connected domains names and the reasons why.

1. Phished Well-Known Organizations

Hackers, like all criminals, have a knack for forgery. And reputable organizations are the perfect means to conduct social engineering attacks since they are trusted by customers, employees, and people

at large. When an email is received from such an entity asking to confirm or update personal or confidential details, the temptation to comply without doubting the origins of the sender is high.

But what does all this have to do with connected domains? Well, fraudsters typically register confusingly similar names to make their phishing attacks even more credible and less noticeable. So when you hear that a famous brand is being impersonated through phishy emails, you can protect your staff with threat intelligence by creating a list of all domains that are too close to be legit and block those by putting corresponding mail servers and IP addresses on a blacklist.

2. Dangerous Neighboring Hosts

Sharing hosting resources including IP addresses is like sharing a flat or office. Whatever your housemates or coworkers do can disrupt your well-being and ability to live or work normally. Similarly, neighboring hosts' bad practices such as spammy behaviors and fraudulent activities are likely to impact your online reputation and SEO. Worse, internet service providers may even decide to over-block your website warning visitors against it because others have misused and abused shared infrastructure.

Checking connected domains here is necessary to ensure you do not end up associated with cybercriminals or illicit content providers by mistake, and therefore protect your integrity and reliability in the eyes of your customers, suppliers, and the press.

3. Variations of Your Domain Names

It's not just about protecting yourself from external parties. Security professionals also need to make sure that the name of their organization is not used for malicious ends. A thorough check of all domains connected to yours, notably for variations of your domain and subdomain names, will help you evaluate whether the risk of impersonation is high. If this is the case, you can take timely precautionary measures and alert customers and everybody else.

4. Malicious Domains Detected

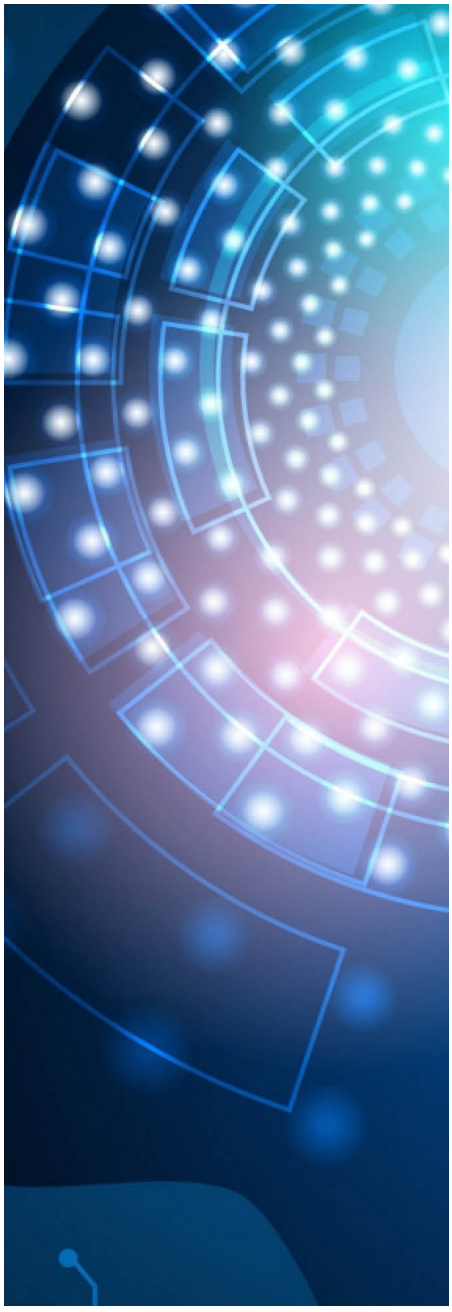
In an effort to maximize gains, cybercriminals typically use different websites simultaneously to execute cyber attacks at scale. While this sounds intimidating, your security team can actually leverage that approach to uncover networks of fraudulent names.

For instance, once they have identified a malicious domain, they can use threat intelligence to start looking for answers to questions such as: Are domain registration details including names and addresses, regardless of whether these are fake or not, uncoincidentally close? Is the same cheap hosting provider and infrastructure being used over and over? Even hackers have limited imagination and resources.

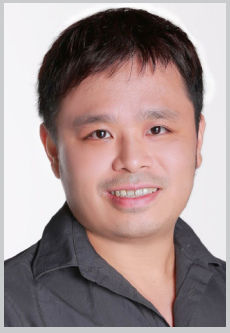
5. Suppliers and Vendors

Last but not least, your cybersecurity team can run a threat intelligence analysis to keep track of the name variations and registrant information of close business partners. This matters because if your staff is already unlikely to question the legitimacy of famous organizations, imagine what data might be in danger when fraudsters impersonate trusted long-term suppliers and vendors.

Bottom line: Monitoring connected domains and the infrastructure behind them is a good example of how threat intelligence enables organizations to protect their online reputation, customers, and employees.



About the Author



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

Breaches, Defenses, Countermeasures, Attack Methodologies

Preparing for a Future with Quantum Computers

by Jane Melia, Vice President of Strategic Business Development, QuintessenceLabs

Quantum computing is progressing fast. Google and IBM are making notable developments in the space, as are other firms. On the government side, bills recently proposed in the U.S. House and Senate are looking to put more than $1 billion into furthering quantum technology. The age of quantum computing is textbook transformative, and it's worth getting excited about. But with that excitement comes a reminder that for cybersecurity, the sheer speed and power of quantum will render today's public-key encryption standards obsolete.

But it's not all doom and gloom. Quantum is also being leveraged to create stronger cybersecurity solutions that address the needs of companies today and safeguard for a future with quantum computers. After all, protecting our most valuable resource -- information -- has never been more critical.

A Look at Quantum – What's All the Fuss About?

There is a growing awareness that conventio nal cybersecurity won't be able to stand up to the processing capabilities of quantum computers. The current strategies for sharing encryption keys rely on methods commonly known as "asymmetric encryption," involving factoring a large multiplication back into its prime constituents; a problem that

is beyond the reach of classic computers in a reasonable time frame. Quantum computers will be able to crack this math easily, hampering one of the foundations of our current security structures. Alongside is symmetric encryption, commonly used to protect data at rest, but which will also be at risk if the keys are not of a significant length and don't have high enough entropy (randomness).

It's not just large IT enterprises are concerned about their proprietary information -- financial institutions, government agencies and other organizations who value security are all looking for ways to prepare for the future challenges of quantum before the technology breaks into the mainstream.

"Safety First" – Prepping for Quantum

Perhaps the brightest side to this new world is that there are ways to "prepare" for quantum-powered cyber attacks today, with existing encryption approaches and methods – even some that use quantum-based tech. You'll hear them called "quantum resistant," "quantum resilient" or "quantum-safe," but they all have the same goal of getting your infrastructure suitably protected against what may come.

An important first step to quantum resilience involves the generation of encryption keys from the ground up using quantum random number generation. Simply put, strong encryption, whatever its type, depends on using strong random numbers to generate keys. Some pseudo-random number (or algorithmic) generators have resulted in vulnerabilities and breaches even before the threat of quantum computers.

High-entropy random numbers protect you from this risk enabling encryption to be delivered at its full strength. The best way to get high entropy is through a quantum random number generator (QRNG). It's not a quantum computer, but does use quantum physics to generate keys, for example quantum tunneling, wherein the activity of electrons travelling ("tunnel") unpredictably through a semiconductor barrier, is measured and turned into streams of numbers. Given that this is a quantum physical phenomenon, not every electron passes the barrier, resulting in full-entropy random numbers from which form the strongest possible keys.

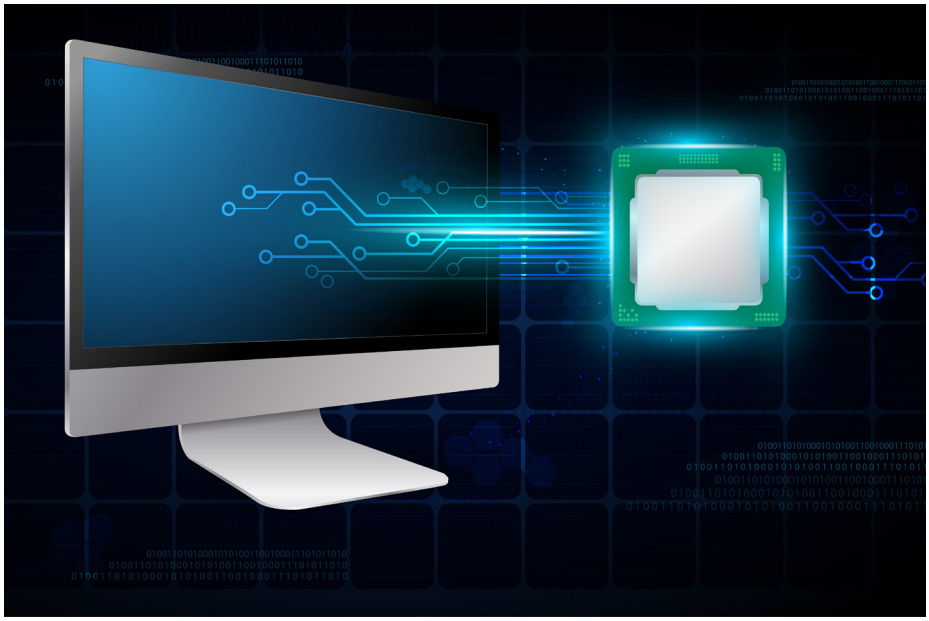
Secondly, symmetric encryption will retain its strength as long as the keys are at least doubled in length and generated from a high-entropy source like a QRNG. Making these changes to your encryption keys and deploying a quantum random number generator are good steps to protecting data at rest from quantum attacks. The resilience of symmetric encryption can be further leveraged to build up quantum resistance within an organization; for example, by wrapping data as it is transferred between replication nodes. This approach can successfully secure data exchanges between two internal nodes using TLS, which is a common mutually-authenticated secure transfer protocol (along with RSA/ECC/AES encryption), that will otherwise be vulnerable to quantum attacks. In practice, a high-entropy symmetric key can wrap the TLS transfer payload, providing another layer of quantum-resilient protection.

As an aside, replication is a priority practice to implement for all important data. Ensure your key management infrastructure enables replication of keys between nodes. Losing keys or not being able to decrypt them can be disastrous!

What's Next

The third step is to keep an eye on the development of new quantum resistant tools and techniques, including quantum resistant encryption algorithms and quantum key distribution for exchanging keys.

Today's reliance on asymmetric protocols for key exchange such as RSA and ECC has brought us far. However, they use mathematical formulas that are demonstrably weak against quantum computers, so alternatives are being sought. NIST started a post-quantum algorithm standardization process in 2017, with recommendations expected to be published in 2022 or later.



Quantum key distribution (QKD) takes a different approach to exchanging cryptographic keys securing this exchange using physics, so parties can share keys in a way that's invulnerable to the typical cyber threats of today and ones we can anticipate in the

future. It is based on a fundamental characteristic of quantum mechanics: the act of measuring a quantum system disturbs the system, so an "eavesdropper" trying to intercept a quantum exchange will inevitably leave traces, allowing the legitimate exchanging parties to get rid of the corrupted information. Quantum computers will not be able to compromise keys shared using QKD, making it the ultimate quantum-safe solution.

QKD is still a developing technology with challenges to overcome, but commercial implementations are beginning to roll out to some degree, and further development will transform QKD's capabilities beyond point-to-point fiber connections to free space.

Fighting Quantum with Quantum

There's no doubt that quantum computers are coming, but as quantum-based cybersecurity demonstrates its capability to improve security, it's only a matter of time before we see its greater adoption, allaying at least in part those concerns about our quantum future. The solutions above – high-entropy keys; symmetric key wrapping; new advanced algorithms, and the onset of QKD – serve as great examples of how industries are preparing. Our quantum resilient future will likely contain hybrid solutions blending quantum resistant algorithms and QKD for key exchange, and even now symmetric encryption using longer and stronger keys for data storage and wrapping and quantum random number generators can start to shore up security for the quantum threat.

About the Author

Jane Melia is the Vice President of Strategic Business Development at QuintessenceLabs, where she leads all market and product strategy activities. Prior to joining QuintessenceLabs, Jane held leadership roles in several Silicon Valley start-ups, including solar firm SolFocus, where she headed the Technical and Product Marketing team for 5 years. Jane's 20 years' experience in technology industries includes 8 years at HP, including as Senior Business Consultant in the Strategic Planning and Modelling group. Jane holds a degree in Engineering from Imperial College, London, and Ph.D. in Fluid Mechanics from Cambridge University. Jane can be reached via Twitter (@Jane_QLabs), and QuintessenceLabs can be found at www.quintessencelabs.com

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

by Stan Engelbrecht, Director of Cybersecurity Practice, D3 Security

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

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

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

Smarter

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

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

Faster

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

Wiser

Security teams accumulate tribal knowledge over time about the history and patterns of incidents, plus the intricacies of their IT and security infrastructure. Senior analysts can build up this wisdom over time, but without a way of documenting the lessons they have learned, their wisdom is lost when they leave the organization—or simply go on vacation.

With the right SOAR platform, senior colleagues can codify their knowledge into playbooks, guided workflows, and reports, and share their experience with the team, including in the critical onboarding phase for new analysts. Junior analysts can also access historical data from every previous incident to see how comparable cases have been handled in the past. This empowers the entire team with the wisdom of their most experienced analysts—past or present.

Happier

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

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

About the Author

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

Industry Newsflash: CYSIV, the new "cyber risk management as a service" company, formed by TrendMicro and HITRUST

by Tom Hunter, Vice President for Business Development & Strategy, Cyber Defense Media Group

Two cyber security titans have entered the newly-conceived "cyber risk management as a service" market. TrendMicro and HITRUST have formed Cysiv, a company with a unique new way to help select U.S. enterprises defend themselves from cyberattacks.

The concept of "cyber risk management as a service" is a completely new formulation, never before brought together as an integrated means of responding to cyber threats and attacks. The intersection of the three elements reflects a creative approach melding powerful responses to "cyber" and "risk management" with the "as a service" delivery platform.

Only participants with the strengths and experience of TrendMicro and HITRUST could have perceived this gap in the market and come together to offer such an integrated and seamless solution. That is why Cysiv has burst onto the cyber security scene with a paradigm shift for potential client organizations.

TrendMicro is a global leader in cybersecurity solutions, and HITRUST is a leading security and privacy standards development, accreditation and information risk management organization. Statements from the leading executives of the two companies illustrate how their individual capabilities will complement each other in supporting the operations of Cysiv.

"The AI-powered security operations and analytics platform that's at the heart of this new service is part of our on-going efforts to enable the SOC with greater visibility, and to add more actionable intelligence and automation to enterprise security," said Eva Chen, co-founder and chief executive officer of Trend Micro. "We're excited by its immediate value to Cysiv customers, and more broadly by its longer-term potential for Trend Micro customers and partners."

"Insights from both our risk management and information sharing service, clearly demonstrate that organizations of all sizes are struggling to effectively implement and operate their cyber defenses in today's escalating threat environment," said Daniel Nutkis, chief executive officer of HITRUST. "This new venture leverages the tremendous experience we've gained in conducting assessments, in managing a threat sharing platform and ultimately helping customers manage their cyber risks."

Cysiv has begun operations and offers a unique combination of expertise, cyber intelligence, and technology, all deliverable as a service, to U. S. companies needing to access cyber risk management services on an integrated basis.

For further details on Cysiv, including its leadership team and services, please visit www.cysiv.com

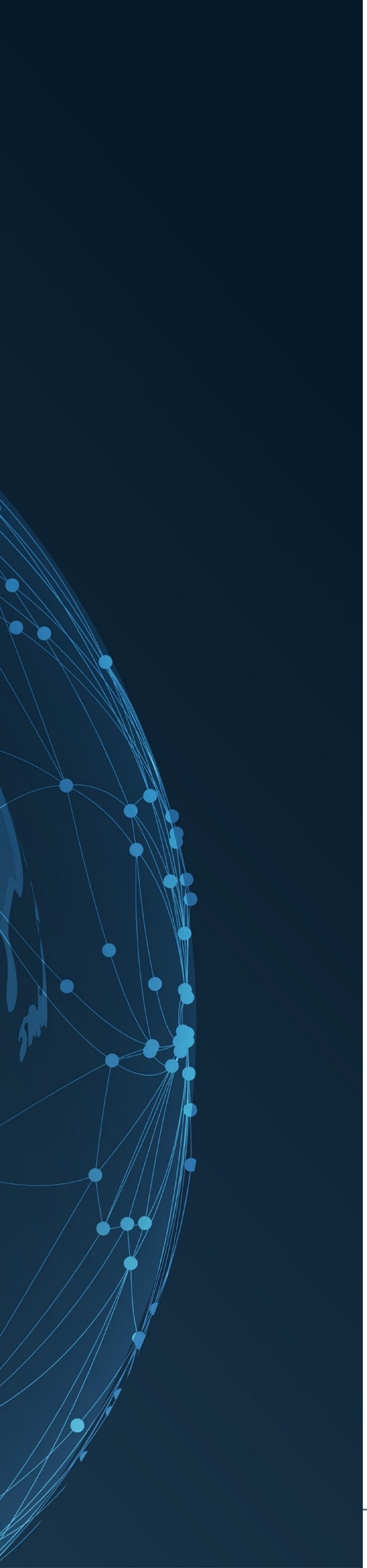
About the Author

Tom is our Vice President for Business Development & Strategy. He is currently based in our London office and has been with Cyber Defense Media Group for two years. Prior to joining Cyber Defense Media Group, Tom held key roles at Rothschild Investment Bank focused on M&A and finance raising, a global commodities firm as a Senior Trader and various high impact freelance business consulting roles. He graduated in law (honours) from the University of Aberdeen and Advanced Project Management at the University of Oxford. He is originally from the North of Scotland and his hobbies include martial arts and travelling. Visit Tom online at http://www.cyberdefensemagazine.com

2018 Cyber Defense Global Awards

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION



Welcome to the Cyber Defense Global Awards for 2018. It's been six months in the making – our annual review of the hottest, most innovative, best, market leaders, next-generation and cutting edge INFOSEC companies offering incredible products and services. While we're in our sixth year of delivering awards to innovators in the USA, which we will continue to do during the RSAC conference in San Francisco, CA in early 2019, you're looking at our Global Awards where we scoured the globe of the nearly 3,000 InfoSec players from the USA to Israel to Japan to Germany to China and back here to the United Kingdom. Some were started in little villages in Greece and others in big cities like Tel Aviv or Tokyo or Beijing. Some of them you have never heard about until today and that makes us very proud. Some are startups, and some are early stage. Some of them are bigger and well-known players. One thing you will see that they all have in common – their products, services, solutions and technologies stand out from the crowd. Their mission is the same as ours – to help you get one step ahead of the next breach. They are on a mission to help you document regulatory compliance such as GDPR. They have been leveraging new techniques including machine learning, artificial intelligence, cloud-based security, new forms of encryption and so much more. After reaching out to thousands of these companies around the globe, we narrowed our list down to a much smaller group of finalists and only 100 companies around the Globe who will all share in the spotlight – winners of our prestigious award. These companies have gone through much scrutiny by our judges and we share this outcome with you, here for your review and consideration. Please join us in congratulating these winners – many of whom you will see at IP EXPO EUROPE as you make your way around the show floor. Let them know you found them, here in Cyber Defense Magazine.

All the best,

Gary Miliefsky
Publisher

Adaptiva

Cutting Edge Endpoint Security

AlienVault

Leader Threat Intelligence

AlienVault

Editor's Choice Unified Threat Management (UTM)

ANOMALI®

Anomali

Best Product Threat Intelligence

APCON
Solutions for Networks

APCON Inc.

Most Innovative Network Packet Broker

atarlabs

ATARLABS

Cutting Edge Security Orchestration, Automation and Response

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNERS

Attivo NETWORKS

Attivo Networks®

Most Innovative Deception Based Security

®buguroo

buguroo

Best Product Fraud Prevention

cavirin

Cavirin

Best Product Cloud Security

Cloud Security Alliance

Leader Cybersecurity Training

Cofense

Next Gen Anti-phishing

Contrast Security

Editor's Choice Cybersecurity Company of the Year

Cynash, Inc.

Editor's Choice ICS/SCADA Security

D3 Security

Most Innovative Incident Response

D3 Security

Hot Company Security Investigation Platform

DEMISTO

Demisto

Hot Company Incident Response

eclectic iq

EclecticIQ

Editor's Choice Threat Intelligence

EdgeWave™

EdgeWave

Best Product Anti-phishing

EdgeWave

Best Product Email Security and Management

First Nation Group

Chief Risk Officer of the Year, Chris Maier

ForeScout

Leader Internet of Things (IoT) Security

ForeScout

Best Product Network Access Control (NAC)

Fortanix

Next Gen Encryption

GTB Technologies

Leader Data Loss Prevention and Data Protection

GO ANYWHERE®
A HelpSystems Solution

HelpSystems
Best Product Managed File Transfer

HERJAVEC GROUP

Herjavec Group
Most Innovative Identity and Access Management

HERJAVEC GROUP

Herjavec Group
Leader Managed Security Services

HID Global

Most Innovative Cybersecurity Discovery

iboss

Leader Cloud Security

Illumio

Next Gen Micro-segmentation Product of the Year

Illumio

Editor's Choice Security Company of the Year

Illusive Networks

Cutting Edge Advanced Persistent Threat (APT) Detection and Response

Inky

Editor's Choice Anti-phishing

Intezer

Cutting Edge Malware Analysis

IP Technology Labs

Next Gen IoT Trunking Gateways

Ixia, a Keysight Business

Hot Company Cloud Security

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNERS

ixia
A Keysight Business

Ixia, a Keysight Business

Leader Enterprise Security

jumio

Jumio

Best Product Biometrics

jumio

Jumio

Next Gen InfoSec Startup of the Year

Kingston Technology

Most Innovative Encryption

Kingston Technology

Editor's Choice Bring Your Own Device (BYOD)

Kingston Technology

Hot Company Data Loss Prevention

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNERS

Kingston Technology
Most Innovative Data Loss Prevention

Kingston Technology
Best Product Security Hardware

Kingston Technology
Next Gen Security Hardware

KnowBe4
Human error. Conquered.

KnowBe4

Leader Security Training

Logsign
Your teammate in cyber security

Logsign Inc

Hot Company Security Information Event Management (SIEM)

NEHEMIAH SECURITY

Nehemiah Security

Cutting Edge Risk Management

Netlok

Most Innovative Multi, Single and Two Factor Authentication

Neustar

Cutting Edge Cloud Security

Neustar

Most Innovative Web Application Security

NightDragon Security

Leader Security Advisory and Investment

Panaseer Limited

Cutting Edge Cyber Security Intelligence Platform

Nuspire Networks

Hot Company Managed Detection and Response (MDR)

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNERS

OBRELA
SECURITY INDUSTRIES

Obrela Security Industries

Editor's Choice Managed Detection and Response (MDR)

observe it

ObserveIT

Cutting Edge Insider Threat Detection

observe it

ObserveIT

Best Product Insider Threat Prevention

OneTrust
Privacy Management Software

OneTrust
Privacy Management Expert of the Year, Kabir Barday

OneTrust
Privacy Management Software

OneTrust
Best Product Privacy Management Software

OVERSEAS INFRASTRUCTURE ALLIANCE
building infrastructure worldwide

Overseas Infrastructure Alliance
Chief Information Officer of the Year, Sourabh Tiwari

PC Pitstop

Editor's Choice Anti-Malware

portnox™

Portnox

Editor's Choice Network Access Control (NAC)

Proficio

Most Innovative Managed Detection and Response

PROFICIO

Proficio

Hot Company Managed Security Services Provider

PROFICIO

Proficio

Most Innovative Security Company of the Year

GEOACL LLC

Editor's Choice Authentication Solution for Rainbow Password

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNERS

Recorded Future

Recorded Future

Most Innovative Threat Intelligence

Resecurity®

Resecurity, Inc.

Best Product Digital Footprint Security

Resecurity®

Resecurity, Inc.

Hot Company Forensics

RiskLens

Most Innovative Risk Management

SecPod Technologies

Cutting Edge Vulnerability Assessment, Remediation, Patch and Configuration Management Endpoint Security

Secure Channels Inc.

Editor's Choice Encryption

Securonix

Best Product Cybersecurity Analytics

Sergeant Laboratories

Most Innovative Cybersecurity Analytics for AristotleInsight

Shanghai Moule Network Technology Co. Ltd

Editor's Choice Vulnerability Discovery and Intelligent Defense

Siemplify

Cutting Edge Incident Response

SKD Labs

Editor's Choice Independent Information Security Test Labs

SlashNext

Cutting Edge Anti-phishing

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNERS

SUCCEED TECHNOLOGIES
We'll get you there...

Succeed Technologies Pvt Ltd

Editor's Choice Security Training

THREATQUOTIENT™

ThreatQuotient

Most Innovative Advanced Persistent Threat (APT) Detection and Response

THREATQUOTIENT™

ThreatQuotient

Next Gen Security Investigation Platform

ThreatQuotient

Hot Company Threat Intelligence

Thycotic

Cutting Edge Privileged Account Security

Titania

Leader Vulnerability Assessment, Remediation and Management

Ttec

Chief Information Security Officer of the Year, Paul (Kip) James

Unbound Tech

Next Gen Cryptography

Untangle

Leader Firewalls

Untangle

Hot Company Network Security & Management

Untangle

Best Product Unified Threat Management (UTM)

Veridium

Next Gen Product Biometrics

WatchGuard Technologies

Leader Multi-Factor Authentication

WatchGuard Technologies

Leader Unified Threat Management (UTM)

WhiteHat Security

Leader Application Security

WhiteSource

Leader Open Source Security

XM Cyber

Cutting-Edge Breach and Attack Simulation

XTN Cognitive Security

Best Product Mobile Endpoint Security

XTN Cognitive Security

Hot Company Application Security

XTN Cognitive Security

Next Gen Fraud Prevention

Zimperium

Leader Wireless, Mobile, and Portable Device Security

Hacker.House

Most Innovative Cybersecurity Training

Congratulations to this year's Cyber Defense 2018 Global Awards

Winners!

www.cyberdefenseawards.com


Go ahead...
Open E-mails with Confidence.
Inky.com

TREND MICRO™ | Machine Learning Masters

Go Beyond Next-Gen

trendmicro.com