[+] (IN)SECUREMagazine

06 | 2018
ISSUE 58

GDPR

Is GDPR-regulated data lurking in unexpected pockets of your organization?

Software-defined perimeter: The pathway to Zero Trust

Leveraging security analytics to investigate and hunt modern threats

HOW TO EXCITE A SOC ANALYST:

1. Zero false positives
2. Accurate detection in minutes
3. Visibility to the full scope story line of every incident

Or all of the above with SecBI's Autonomous Investigation™

www.secbi.com/product/

Oh, and since SecBI is appliance-less, your CFO will get excited too!

SECBI AUTONOMOUS INVESTIGATION™

www.secbi.com info@secbi.com

Table of contents

Contributors

JASON GARBIS, Vice President, Security Software Products at Cyxtera Technologies
MIKE MCKEE, CEO of ObserveIT
COREY NACHREINER, CTO at WatchGuard Technologies
RICK ORLOFF, CSO at Code42
HYDER RABBANI, Chief Operating Officer at CyberSight
JASON STRAIGHT, Senior Vice President and Chief Privacy Officer of Cyber Risk Solutions at UnitedLex
YU XU, CEO at TigerGraph

Visit the magazine website and subscribe at www.insecuremag.com

Mirko Zorz
Editor in Chief
mzorz@helpnetsecurity.com

Zeljka Zorz
Managing Editor
zzorz@helpnetsecurity.com

Berislav Kucan
Director of Operations
bkucan@helpnetsecurity.com

Is GDPR-regulated data lurking in unexpected pockets of your organization?

AUTHOR_ Rick Orloff, CSO at Code42

A recent study has shown that over 60 percent of corporate data is stored on employee endpoints. And yet, as companies work to ensure compliance with the new General Data Protection Regulation (GDPR), they may still be overlooking a few key areas.

The GDPR impacts the processing of all personal data on EU residents and took effect on May 25, 2018. The challenge it presents is that personal data doesn't just live in your customer relationship management (CRM) system, it also exists - in a more unstructured way - on your company's endpoints. To protect company assets and meet GDPR compliance standards, organizations need to have a clear understanding of where personal data resides, including where it is created, used and stored. Failure to adequately secure user endpoints could mean major fines as well as damage to customer relationships and brand reputation.

Protect endpoint data

To secure potentially vulnerable endpoints, companies need to conduct a detailed impact assessment of their data systems. An important initial step in this assessment is defining what constitutes personal data. Because the definition can vary based on context and from country to country, your company should work with its legal counsel to gain clarity. For companies in the US with customers or prospects in the EU, this likely means adopting the stricter European standard.

Next, it's crucial that organizations get a good understanding of where personal data lives in their ecosystems and the areas it traverses, in both structured and unstructured ways. Employees want to work in the most efficient manner possible, which means they don't always follow corporate IT policy when it gets in the way. Doing so isn't necessarily malicious. Imagine the implementation consultant who takes client information home to work on an issue after hours, or the sales rep who brings prospect data on the road in order to craft a customized pitch.

Company leadership certainly does this as well – according to the CTRL-Z report, C-suite executives are the most likely to violate company data security policies. So, while a strict internal data policy is important, you also need the tools in place to account for human behavior and gain visibility into data as it moves in and out of traditional security perimeters.

+ Regardless of where your organization's personal data resides – whether it's on an endpoint or in a cloud application – under GDPR, if you get breached or your data and/or systems get held for ransom, you have to be able to account for it.

The quicker you can identify the scope of an incident, the faster you can begin to remedy the situation. Thankfully, there are software solutions available that can help companies assess their exposure by quickly identifying where files exist and what information is contained within them. By implementing endpoint data protection and visibility solutions, organizations can be well-positioned to investigate incidents and begin the recovery process.

Encryption is not enough

Encryption is another important data protection tool available to companies. But based on the requirements of GDPR, it's still not enough to fully safeguard your company's data assets.

According to industry research, nearly 70 percent of data loss incidents originate on the endpoint. Imagine scenarios in which credentials are taken or an employee acts maliciously with the intent to damage the company. In these cases, encryption wouldn't be enough to stop the possible distribution of vital company data. Any data that users can access is potentially at risk. That's why companies need software solutions that can monitor user endpoints, provide visibility into data movement and interactions, and alert personnel to suspicious activity.

Reporting an incident

Having a complete picture of your data ecosystem – where personal data lives and travels across an organization – is essential to not only safeguarding it, but also successfully reporting in the event of a breach. According to the new GDPR rules, companies must report an incident within 72 hours of detection. However, if you are uncertain where your data lives, there is no way to determine the magnitude of your exposure in such a short time. In the event that data is compromised, knowing exactly what data is exposed and showing sufficient control over it will make interactions with the regulatory authority much smoother.

On the other hand, a breach may not have resulted in any personal data exposure at all. If you do not have a complete inventory of and visibility over your data, you could be filing unnecessary reports and risking consumers losing confidence without any real cause for alarm. Announcing to customers that you are unsure if personal data was exposed is nearly as bad as confirming its loss. After all, who wants to do business with a company that can't be sure where personal data is stored?

Culture change required

Until now, many organizations haven't thought about their entire data ecosystem as an asset that needs to be inventoried and managed in the same way as physical assets or regulated consumer data like protected health information or payment card data. Under GDPR, that perspective will have to change.

> Companies need to expand the scope of what they consider to be personal data. Data should be treated as an asset, and companies need to take that seriously.

Anything less could leave them vulnerable to outside attacks, regulatory infractions and reputational damage.

It's an unfortunate reality that we can't prevent all data breaches or data loss; and since complete prevention is impossible, companies need to be prepared to detect data breaches and respond quickly and effectively. Organizations need policies in place that govern internal data access and ultimately the capability to respond and investigate quickly during a data breach. With continuous data protection, visibility, recovery and oversight, companies can mitigate their risks and feel confident they are meeting GDPR standards while building trust with their consumers.

Security world

Pressures impacting security pros are up, threats are turning up the heat

Trustwave released the 2018 Security Pressures Report based on a global survey of 1,600 full-time IT professionals who are security decision makers or security influencers within their organization.

Findings show that a majority of IT and cybersecurity professionals experienced increased pressures in 2017 when compared to the previous year, driven largely by a steep rise in sophisticated malware, continued deficit of high-level security talent and budget constraints. This report marks the fifth consecutive year pressures have increased year over year.

On the flip side, there were a few bright spots. For instance, pressure to rush IT projects before they are security ready is decreasing and incorporation of managed security services to fill resource and technology gaps has gained traction, signaling a concerted effort to address pressures through better practices.

Overall, 54% of respondents experienced more security pressures in 2017 when compared to 2016. US respondents cite the most increased pressure at 61%, followed by Japan at 55% and Singapore at 54%. However, it is encouraging that 54% of respondents on average are more confident than they were five years ago in their ability to secure their organization, while only 15% are less confident.

Too many IT pros ignore critical security issues

A recent Outpost24 survey of 155 IT professionals revealed that 42 percent ignore critical security issues when they don't know how to fix them (16 percent) or don't have the time to address them (26 percent). The survey, which was carried out at the RSA Conference in April 2018, also asked respondents what area of their IT estate they consider to be the least secure. This revealed 25 percent are most concerned about their cloud infrastructure and applications, 23 percent are most concerned about their IoT devices, 20 percent said their mobile devices, 15 percent said their web applications, while 13 percent were most concerned about their data assets, databases and shares.

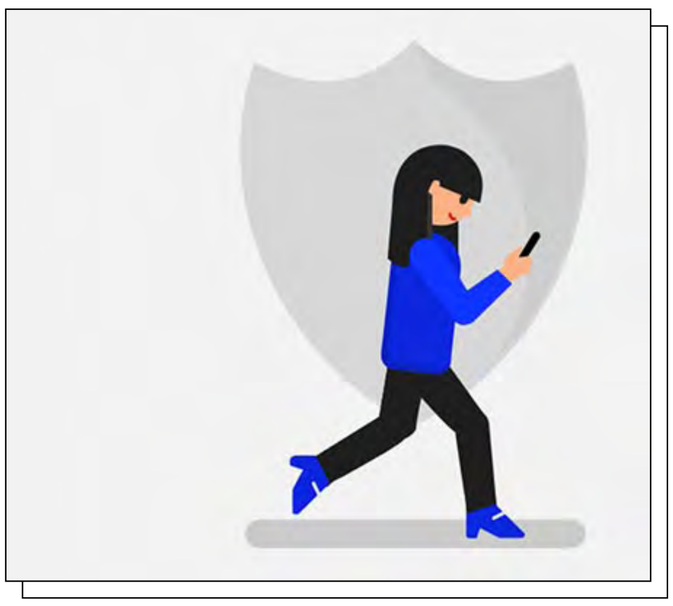
Microsoft will extend GDPR rights to customers worldwide

Microsoft has announced it will extend the rights that are at the heart of GDPR to all of their consumer customers worldwide.

“Known as Data Subject Rights, they include the right to know what data we collect about you, to correct that data, to delete it and even to take it somewhere else,” Julie Brill, Corporate VP and Deputy General Counsel at Microsoft, explained.

Users can access these tools through Microsoft’s privacy dashboard.

Changes to the dashboard that allow Microsoft to comply with GDPR requirements have already been made in January 2018, when the wider availability of the Windows Diagnostic Data Viewer tool was announced.



“GDPR is an important step forward for privacy rights in Europe and around the world, and we’ve been enthusiastic supporters of GDPR since it was first proposed in 2012,” Brill noted.

“We are committed to making sure that our products and services comply with GDPR. That’s why we’ve had more than 1,600 engineers across the company working on GDPR projects. Since its enactment in 2016, we’ve made significant investments to redesign our tools, systems and processes to meet the requirements of GDPR.”

She also noted that changes to the tools can be expected.

“As our customers use our tools and experience other features we’ll also listen to their feedback and suggestions for improvements. Because regulatory interpretations change with experience and changing circumstances over time, we will constantly evaluate our products, services and data uses as understanding of GDPR evolves.”

America’s most cyber insecure cities exposed

From December 2017 – April 2018, Coronet analyzed an enormous set of data comprised of both access and service threats. The data originated from Wi-Fi and cellular networks, devices spanning all operating systems and public network infrastructure. The researchers identified Las Vegas, Memphis and Charlotte as America’s most cyber insecure cities.

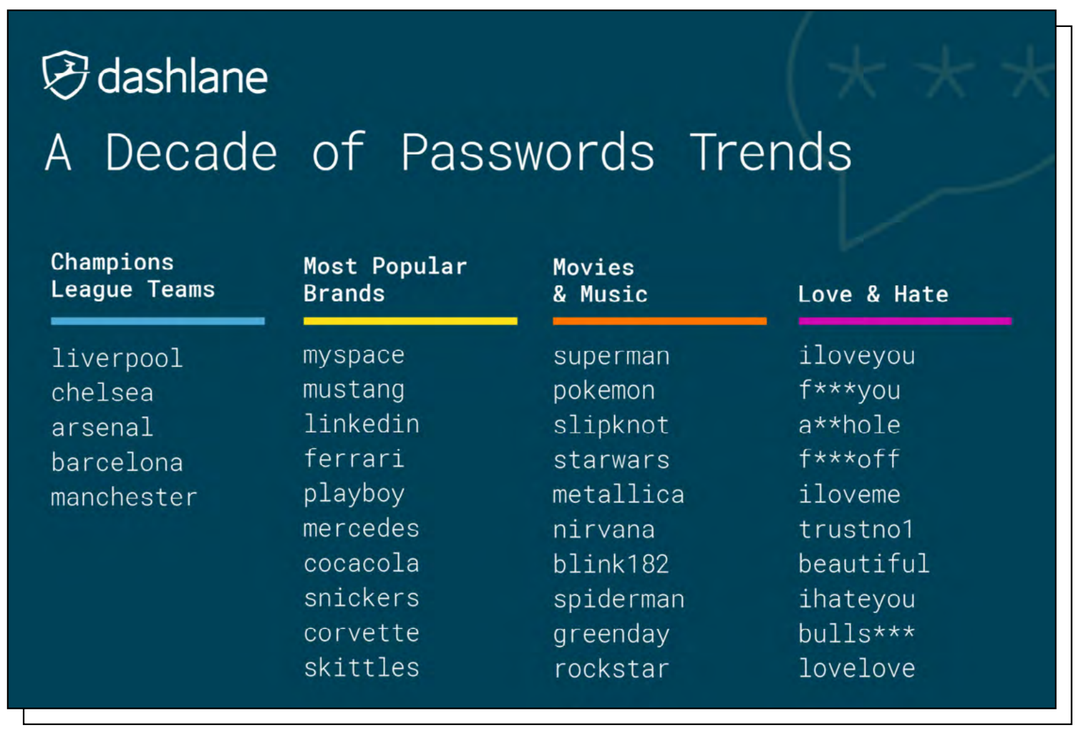
How security pros see the future of cryptocurrencies and cryptomining

Data gathered by Lastline at RSA Conference 2018 reveals that 84 percent of security professionals believe cryptocurrencies are here to stay – either as a mainstream alternative to conventional currencies (45.2 percent) or a fringe option (38.9 percent). Enough believe in this new type of money that 14.5 percent would rather collect their salary in cryptocurrency than in a traditional currency.

Password pattern analysis: Risky, lazy passwords the norm

Dashlane announced the findings of an analysis of over 61 million passwords. The analysis was conducted with research provided by Dr. Gang Wang, an Assistant Professor in the Department of Computer Science at Virginia Tech.

Researchers examined the data for patterns, illuminating simple mistakes that continue to be made by people who use passwords in daily life, which is to say virtually everyone. They found patterns across the keyboard, from not-so-randomly chosen letters and numbers to popular brands and bands, and even passwords created out of apparent frustration.



"It is difficult for humans to memorize unique passwords for the 150+ accounts the average person has," said Dr. Wang. "Inevitably, people reuse or slightly modify them, which is a dangerous practice. This danger has been amplified by the massive data breaches which have given attackers more effective tools for guessing and hacking passwords."

Pervasive password walking

Researchers discovered a high frequency of passwords containing combinations of letters, numbers, and symbols that are adjacent to one another on the keyboard. This practice, known as Password Walking, highlights the apathetic attitude most users have towards passwords, preferring convenience over security.

When users Password Walk, they are creating passwords that are far from secure. Most hackers are keenly aware of the human tendency to rely on convenience and can easily exploit these common passwords.

Most are familiar with versions of Password Walking, such as "qwerty" and "123456", but researchers uncovered several other combinations that are frequently used:

- 1q2w3e4r
- 1qaz2wsx
- 1qazxsw2
- zaq12wsx
- !qaz2wsx
- 1qaz@wsx

These passwords are all comprised of keys on the left-hand side of standard keyboards. This means users can simply use the pinky or ring finger on their left hand to type their entire password. However convenient this may be, saving a few seconds is not worth the loss of one's critical financial and/or personal data due to an account hack.

The prevalence of Password Walking is troubling and should make anyone using such passwords take another look at their password practices. Genuinely random and unique passwords are essential to password security; punching a bunch of adjacent characters will not cut it.

Quantifying cyber exposure: Attackers are racing ahead

Cybercriminals have a median seven-day window of opportunity during which they can exploit a vulnerability to attack their victims, potentially siphoning sensitive data, launching ransomware attacks and causing extensive financial damage before organizations even take the first step to determine their cyber exposure and whether they are at risk.

According to a new Tenable report, it takes a median six days for a cybercriminal to weaponize vulnerabilities once a new public exploit first becomes available. However, security teams can take a median 13 days before launching their initial assessment for a new vulnerability — the first, crucial step in determining overall cyber exposure in modern computing environments. The resulting seven-day lag time means that cybercriminals can attack their victims at will while security teams and their organizations remain in the dark as to the true level of risk to the business.

Digital transformation has radically increased the number and type of new technologies and compute platforms – from Cloud to IoT to Operational Technology – and led to a dramatic growth in the attack surface. Inevitably, this expanding attack surface has given rise to an unrelenting barrage of vulnerabilities.
Many organizations still run their operations programs on fixed cycles – every six weeks, for example – as though they were operating only legacy IT environments, not the dynamic computing platforms of today. Latency is therefore built directly into the cybersecurity process, giving the attacker the advantage from the outset as security and IT teams operate in organizational silos. Many CISOs are left struggling to gain basic visibility into a constantly changing threat landscape and are hampered in their efforts to manage cyber risk proactively based on business criticality.

“This report illustrates the stark reality facing organizations today – cybercriminals and security teams are engaged in a never-ending sprint to seize the first-mover advantage whenever a new vulnerability is discovered. But CISOs are consistently at a disadvantage in large part due to antiquated processes and tools. We must put the CISO in the driver’s seat so organizations can proactively measure and manage cyber risk in the same way as other business risks,” said Tom Parsons, senior director of product management, Tenable. “In a digital economy powered by the cloud, business applications and DevOps cycles, it’s imperative that organizations establish good cyber hygiene, which starts with maintaining live and holistic views into their systems at all times. That’s a critical step toward reducing cyber exposure and eliminating the attackers’ advantage.”

Exposing the threat of shadow devices

Infoblox researchers found that enterprise networks across the US, UK and Germany have thousands of shadow personal devices (laptops, Kindles and mobile phones) and IoT devices (such as digital assistants and smart kitchen appliances) connecting to their network. Over a third of companies in the US, UK and Germany (35 percent) reported more than 5,000 personal devices connecting to the network each day.

Most businesses believe stronger data protection policies will lead to fewer breaches

A new Webroot report looks at how businesses in the US, UK, and Australia are adjusting to new data security measures in order to meet compliance requirements. Specifically, the report measures organisations' readiness to comply with the General Data Protection Regulation (GDPR), and Australia's Notifiable Data Breaches (NDB). The results reveal that 95 percent of IT decision makers surveyed agree that there will be fewer data breaches as a direct result of stronger data protection policies.

Insider threat blind spot enables employee revenge attacks

Based on threat assessments from global organizations in public and private sector industries, Dtex Systems determined there are active insider threats in all assessed organizations.

This is clear proof that none have been able to eliminate the insider threat blind spot. Failure to gain visibility is allowing malicious and negligent employees to engage in undetected high-risk activities on every endpoint, on and off the network.

White House eliminates Cybersecurity Coordinator role

The decision was made by John Bolton, the most recent National Security Advisor of the United States, after both Tom Bossert, the homeland security adviser to the president and cybersecurity czar, resigned in early April and Rob Joyce, special assistant to the President and Cybersecurity Coordinator on the National Security Council, left the post to return to the National Security Agency, where he used to head the agency's Tailored Access Operations (TAO) hacking unit.

IBM employees banned from using portable storage devices

In an attempt to minimize sensitive data loss, IBM will try out a worldwide, company-wide ban on the use of removable portable storage devices such as USB sticks, SD cards, and flash drives. The company's CISO Shamla Naidoo informed IBM employees about the new requirement via an advisory, and noted that the decision to implement it worldwide was made because "the possible financial and reputational damage from misplaced, lost or misused removable portable storage devices must be minimised."

Europe continues to be a cybercrime hub

ThreatMetrix announced new data revealing a 30 percent year-on-year increase in the volume of cyberattacks hitting Europe in the first quarter of 2018. As attacks patterns morph across the region, European digital businesses were hit with 80 million fraud attempts, as they experienced more pronounced spikes of peak attack periods throughout Q1 2018 compared to previous years. There has been an evolution from short, isolated peaks of fraud attacks to more sustained, high-volume attacks across a number of days or even weeks.

Researchers hack BMW cars, discover 14 vulnerabilities

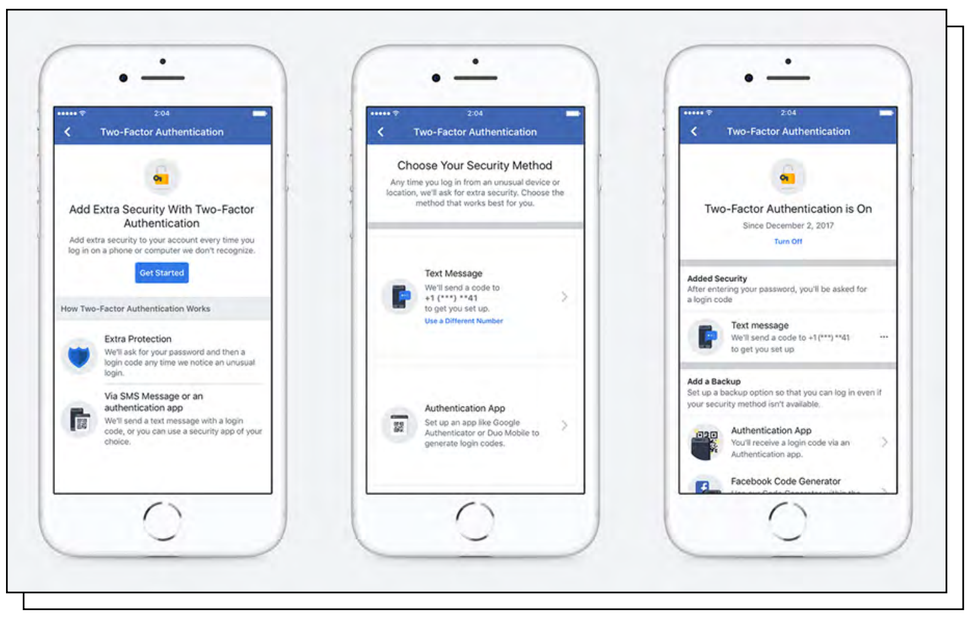
Keen Security Lab researchers have discovered fourteen vulnerabilities affecting a variety of BMW car models. The flaws could be exploited to gain local and remote access to infotainment (a.k.a head unit), the Telematics Control Unit (TCU or TCB) and UDS communication, as well as to gain control of the vehicles' CAN bus.

Fraud data shows 680% spike in fraudulent mobile app transactions

The number of fraudulent transactions originating from a mobile app during the first quarter has increased by 200 per cent since 2015, according to RSA Security. Analysis from the team also indicated that abuse of social media platforms is a growing problem, with social media replacing the dark web as the top hacker marketplace.

Facebook now supports 2FA via authenticator apps

Facebook has good news for users who wish to secure their accounts with two-factor authentication but aren't comfortable sharing their phone number with the social network: there's now an option to use authenticator apps to receive the second authentication factor.



Relying on legacy security technologies leaves you blind to IoT threats

IoT introduces new operating systems, protocols, and wireless frequencies. Companies that rely on legacy security technologies are blind to this IoT threat, says 802 Secure. Organizations need to broaden their view into these invisible devices and networks to identify rogue IoT devices on the network, visibility into shadow IoT networks, and detection of nearby threats.

Rising concerns about managing risk in the medical device industry

Perforce Software released the results of a global survey of medical device professionals. Key findings show increased concerns for mitigating risk and proving compliance during the development process. Proving compliance and passing audits is critical in the medical device industry. Just 46% of the respondents were confident that they could pass an FDA audit.

1 in 10 healthcare organizations paid a ransom within the last year

One in three healthcare organizations have suffered a cyberattack within the last year, while almost one in 10 have paid a ransom or extortion fee, according to Imperva. Healthcare data is extremely valuable on the dark web as it contains sensitive data, both financial and protected health information. As a result, healthcare organizations are increasingly attractive to attackers.

2018 Information Security Leadership Awards Government winners

(ISC)^2 announced the winners of the 15th annual Information Security Leadership Awards (ISLA) Government. The award program recognizes the ongoing commitment of individuals and teams whose initiatives, processes and projects have led to significant improvements in the security posture of a local, state or federal government department, agency or branch in the United Sates.

"We are proud to celebrate the achievements of these esteemed security professionals and their teams," said (ISC)^2 CEO David Shearer, CISSP. "Government executives are challenged with austere budgets, regulatory mandates, and staffing shortfalls – issues threat actors do always not face. These exemplary professionals have demonstrated their dedication and resourcefulness to succeed despite the unique challenges they face to better serve and protect their fellow citizens."

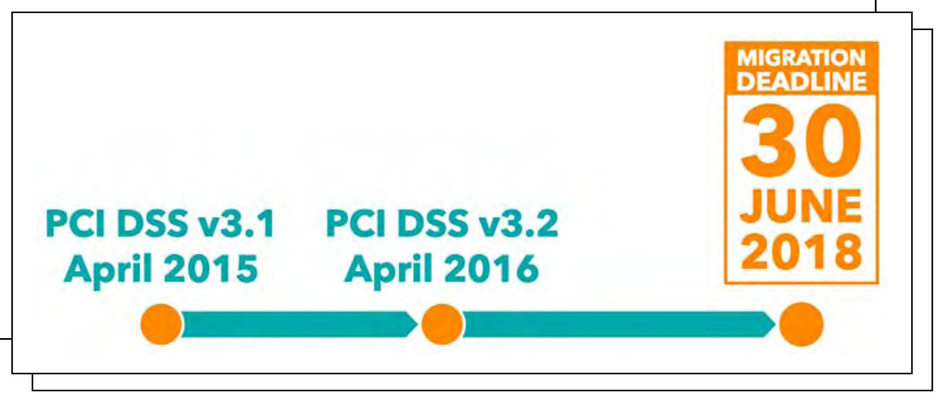
The winners are:

- **Workforce Improvement – Aung Htein, administrator,** Office of Information Systems and Technology, Employment and Training Administration, U.S. Department of Labor.
- **Up-and-Coming Information Security Professional – Mark Bacharach,** CISSP, innovation fellow, Environmental Protection Agency, Office of Environmental Information, Office of Information Security and Privacy.
- **Technology Improvement – Michael Sherwood,** director of technology and innovation, City of Las Vegas.
- **Process/Policy Improvement – Glenn Hernandez,** CISSP, captain, U.S. Coast Guard (retired) and chief information security officer.
- **Most Valuable Industry Partner – Nicholas Andersen,** CISSP, vice president of corporate strategy, Invictus International Consulting.
- **Community Awareness – Matt Goodrich,** JD, FedRAMP director, Technology Transformation Service, U.S. General Services Administration.

A judging committee of senior cybersecurity experts from (ISC)^2's U.S. Government Advisory Council (USGAC) assessed the achievements of security professionals nominated exclusively by their peers and selected this year's award winners. The 2018 ISLA Government judges were Devon Byran, CISSP, Michael Stoner, CISSP and Steven Hernandez, CISSP, CAP, SSCP, CSSLP, HCISPP.

PCI Security Standards Council publishes PCI DSS 3.2.1

PCI DSS version 3.2.1 replaces version 3.2 to account for effective dates and SSL/early TLS migration deadlines that have passed. No new requirements are added in PCI DSS 3.2.1. PCI DSS 3.2 remains valid through 31 December 2018 and will be retired as of 1 January 2019.



Leveraging security analytics to investigate and hunt modern threats

AUTHOR_Mirko Zorz, Editor in Chief, (IN)SECURE Magazine

In this interview, Gary Golomb, co-founder at Awake Security, talks about how machine learning help develop a scalable enterprise cybersecurity plan, what technologies can make a security analyst's job easier, he outlines the essential building blocks of a modern SOC, and much more.

_ ***We've been hearing a lot about machine learning and ways it can empower the infosec industry. What CISOs are wondering is how, in reality, can machine learning help develop a scalable enterprise cybersecurity plan?***

There are things that AI or ML are good for in an enterprise security plan and things they are not good for. Unfortunately, I think a lot of the marketing around machine learning and AI in security has focused on how they can be a solution to the skills crisis. The theory goes something along the lines of:

"With AI or ML, you don't need people anymore, solution will automate , and things will just work."

The reality is a bit different. I often see how this does not work out in practice because of the "Left-Over Principle," where simple tasks are the ones that get automated, leaving only the complex ones for humans.

Just as importantly, a surprising number of AI systems take a fair amount of care and feeding to work, which often includes training periods and identifying what is business justified vs. not. Specifically, a fundamental requirement to use AI is the availability of labeled data that covers the full range of use cases/variations that you intend to identify. Of course, the subtext is that the labels still need human subject matter experts (usually the same people who were previously writing rules, signatures, etc.) to label the data in the first place. And as you might expect, this step is also subject

to the same types of human error as the non-AI methods. And even if you ignore that, the practical problem here is access to enough samples that cover a meaningful range of real world threat cases, and the oddball behaviors that look bad but are business justified.

But to me, there is one other issue that is more insidious and subtle as it applies to AI in the real world. It's what I call discernibility, and this is where we start dissecting issues around the importance of ground-truth "rules." CISOs and security teams would do well to consider the chosen data source to be analyzed by AI and most importantly, the features of that data source. This is critical because there are characteristics of the dataset itself that are crucial for the proper functioning of AI.

+ My recommendation to CISOs is to think about ML in the context of how it can augment their existing teams rather than replace them.

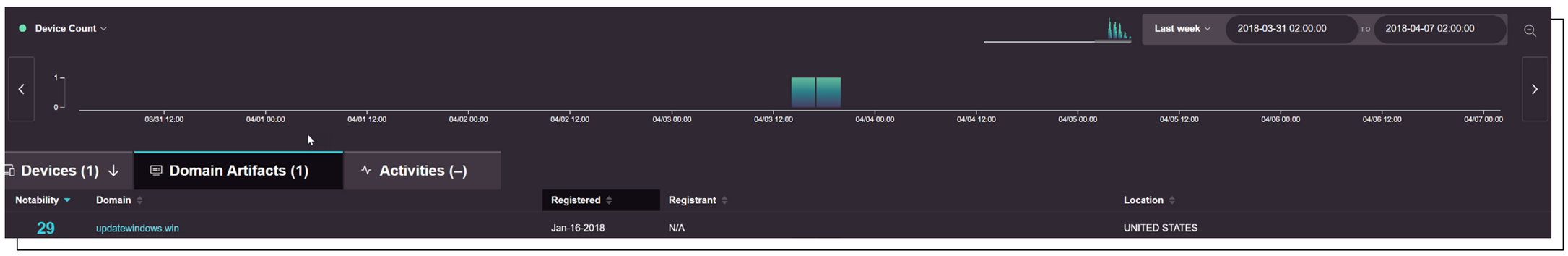
There is a whole branch called augmented intelligence that we should be focused on, but that's a discussion in itself. In the meantime, here are some questions organizations should consider to help determine the best use cases to apply ML or AI:

- How will the data set change over time?
- Is it possible for the data format or structure itself to change?
- More importantly, how can the values within those structures change over time? Can meanings of values change over time?
- How many sources manage possibilities for change or could introduce change in other ways?
- What is the rate of change for each of the characteristics above?
- How closely will the training data match enterprise data over time?

When examined though this lens, you start to see why log-based ML-solutions tend to be useful for only a very limited set of types of threat cases—leading to proliferation of tools for each specific case. Between the network, endpoints, and logs, logs have the least detailed data and by far the least amount of data as a whole.

On the other hand, consider network traffic. The characteristics/features of traffic used in models for AI based detection usually include some combination of protocol and destination domain characteristics, if available. To make this more concrete, let's consider a common type of reference case, malicious redirect chains and even C2 types of examples.

Here we see a common example of that type of activity:



In this case Awake Security's augmented intelligence enables the security team to look for attacker tactics, techniques, and procedures (TTPs). Specifically, this example detected devices communicating with servers advertising themselves as sites affiliated with companies like Microsoft, Google, or Facebook, yet the traffic is actually going to a destination not registered by those companies. As an attacker you can try to look like Google or Facebook, but at the end of the day, you can't look exactly like Google or Facebook. Here we see a long list of suspicious and malicious activities found in a real network just a couple days before the analysis, based on this logic. Not to mention the domain we highlighted that was registered only about 10 days prior!

How long does it take for a security analyst in an average enterprise to collect relevant information about a suspicious event in order to be able to discern the difference between true and false positives? What proven technologies can help speed up this process and make sure the analyst makes the right decision fast?

Over the last 20-30 years the bulk of security investments have focused on prevention and detection tools—these solutions generate alerts, and, in many cases, we collect and correlate them through a SIEM or an MSSP which *hopefully* deliver a smaller set of alerts. At the other end of the spectrum, the security team must "do something" with those alerts.

The challenge is all these tools provide scarce context to people tasked with investigating those threats. So, humans are left to figure out what device (not IP address) is affected, what we already know about the device, what user(s) are associated with the device, what is normal or not normal for that device and user(s), and what is normal for devices and users most like this device or user. And that's just on the inside. The team must then correlate open source intelligence, threat intelligence, details about the specific threat, etc. Closing this Investigation Gap manually, if even possible, can take hours across dozens of data sources and people / departments.

Let's consider an example. Say one of your detection solutions raised a critical alert with evidence of command and control activity coming from 10.1.2.3. As an analyst, one of your first question is likely to be "What is 10.1.2.3?" It might be the device that displays the cafeteria menu, or it might be a computer in the legal department.

In this day and age, it might be the thermostat! How do you grab this context today? You will likely head over to your DHCP server (and if you are like most organizations you typically have more than one and the IP ranges overlap so this will be easier said than done). You then try to find the identity of the computer that was assigned 10.1.2.3 at the time – hoping that the logs for the time of the alert exist. That might give you a MAC address or perhaps a hostname which may still not tell you much. So off to the configuration management database (CMDB) we go. This is where things often get even more hairy – the CMDB could just be an Excel file. You hope to come out with some understanding of the device, where it sits, and perhaps the name of the user the device is assigned to.

Of course, this tells you nothing about the user, so you head off to Active Directory or Outlook, or maybe your HR system. Who is this person? What is their role? What is typical behavior for them? What is not typical? Who else is like this user? The questions go on and on, but a lot of the information you're seeking is not documented anywhere, so now you start to guess.

At the same time, you are also trying to find information from the outside, like what do we know about this domain responsible for the command and control (CnC) traffic? When was it registered? Does it look like an algorithmically generated domain name? Am I seeing anyone else who

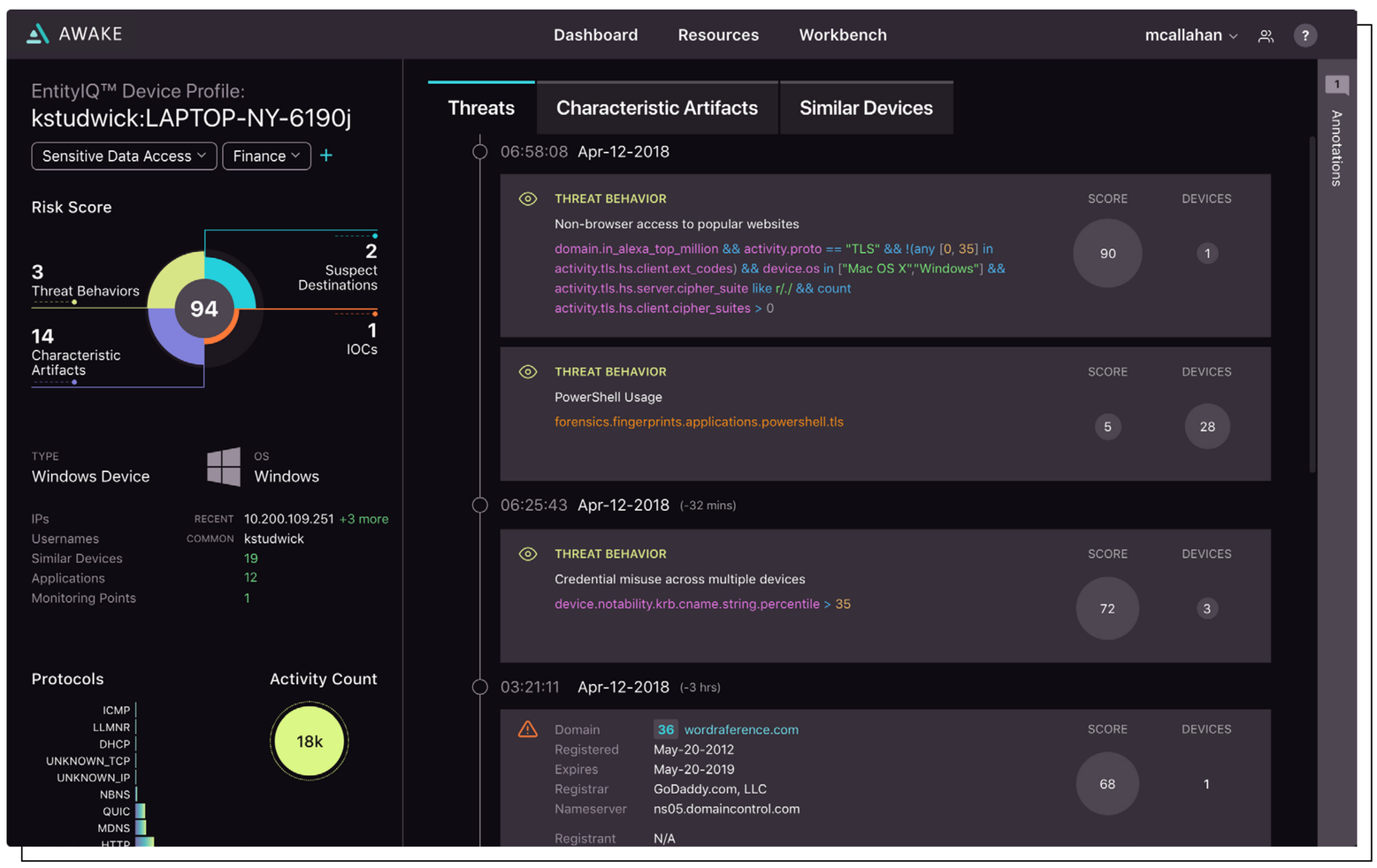
has visited that domain from my organization? How often are people going there? What is open source intelligence (OSINT) telling me about this domain, the hosting provider, etc. Do I have any relevant threat intelligence, etc? I also need to cross reference all this information against what I know about the threat itself—usually with the limited information from my SIEM or the alerting product.

As you can imagine this process is lengthy and involves a bunch of context switching. And unfortunately, in our research we found this example wasn't the exception but the rule.

+ We would routinely find security teams spending hours or more looking across 30 or 40 data sources to piece the information together and hope no mistakes were made along the way.

The solution is technology that precomputes the answers to these questions and gathers the information security teams need at their fingertips, and thus enables rapid, iterative and conclusive alert investigations and hunting. You need technology that can help existing people and process scale by extracting signals from ground truth data sources and then automatically pre-correlating, profiling and tracking assets including devices, users and domains, etc.

As an analyst, this lets you work on these entities rather than primitive and ephemeral data types like IP addresses which slow you down and don't help you make decisions. This technology also needs to capture and share procedural knowledge among the team so it doesn't walk out the door with SOC shift changes or when someone leaves the organization.



What are the essential building blocks of a modern SOC? What advice would you give to an enterprise CISO that wants to make sure his SOC is future-proof as much as possible?

Before I answer this question, it might be best to examine trends that are shaping how the job of defending the organization has evolved.

T1. The sprawl of devices—IoT, BYOD, VDI, etc. have all led to many more devices in the organization than most security teams are even aware of. And of course, without visibility there really is no way to protect those devices or protect the organization from those devices.

T2. This problem is worsened by the fact that attacks are increasingly focused on a population of one—a single user (or a very small subset of users), a single server, etc.

T3. And finally, the attacks themselves have evolved from the traditional malware heavy to what is now called "file-less" malware—which is based on text strings and text files as opposed to compiled executable applications (which are much easier for security software to identify and analyze for maliciousness). This is the abuse of existing system tools used by administrators to further the malicious activities of the threat actor. This evolution means the traditional approach of using malware signatures or "indicators of compromise" is no longer effective at catching a determined adversary.

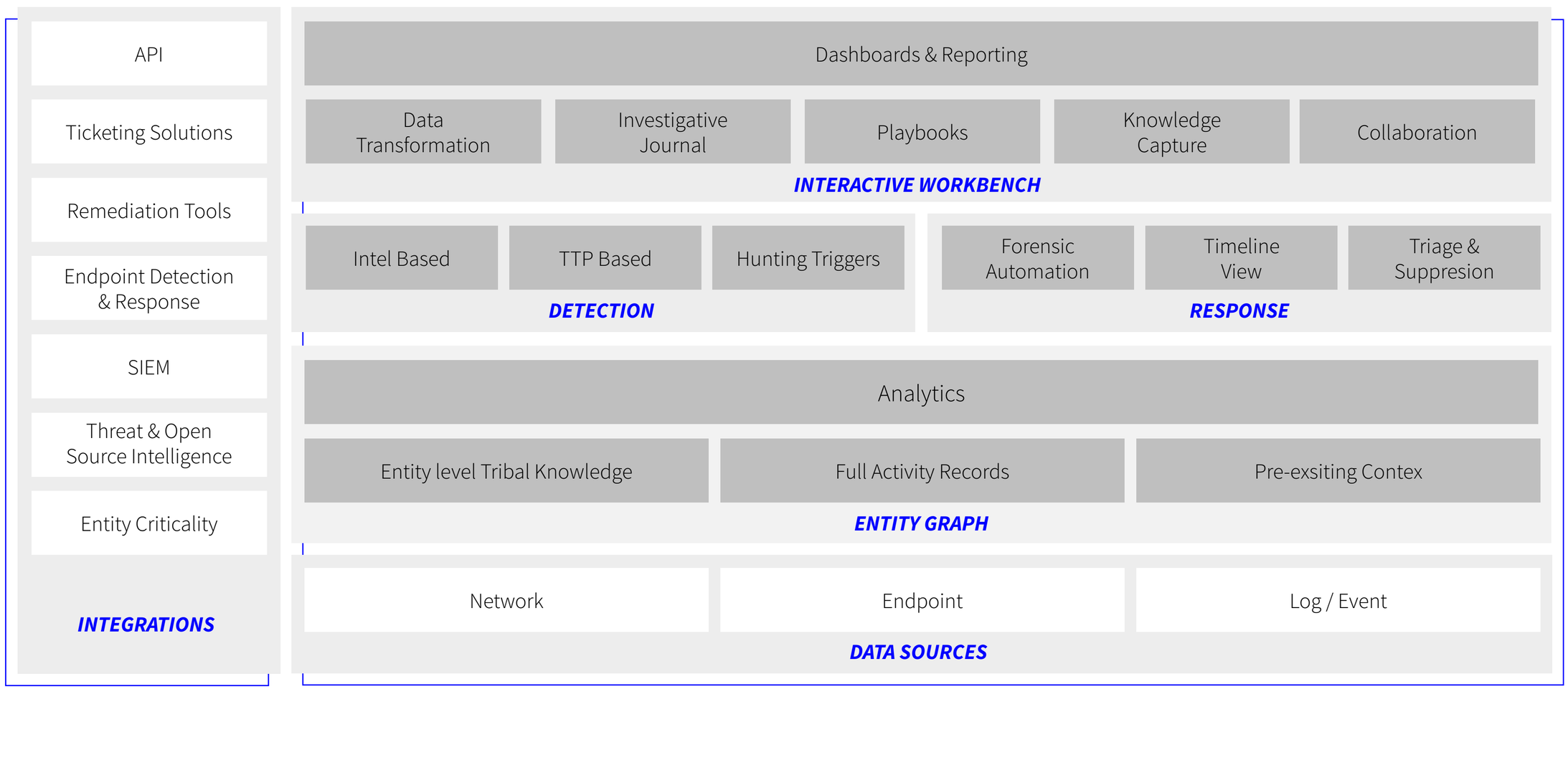
One has to only look at some of the recent large breaches to see the impact of these three trends on even large organizations that have invested in security. The skills crisis and the lack of expertise in security are also massive trends that impact – and are impacted by – all three of the macro trends above. For me, the implications are the clear. The SOC of the future must be able to meet the following key requirements:

R1. Visibility not limited by agents, logs, or meta data that by definition cannot be complete. In addition, visibility by itself isn't enough since we also need to enable the security team with the knowledge to interpret the visibility and factor this information into the organizational threat model.

R2. If the attacker is focused on targeting entities like specific devices or users, then the defenders must be able to view the environment through the same lens – i.e. as a collection of entities—with roles, attributes, behaviors, and relationships. These entities will include the devices, users, external organizations, etc. that exist in the infrastructure.

R3. Defensive and preventative techniques must evolve to automated detection and hunting that can look for anomalous behaviors and attackers TTPs that span the entire attack campaign rather than specific indicators.

With that background, it is now useful to think more concretely about what an effective SOC looks like. It may be best described as shown in the figure below.



As one would expect, information is foundational. The SOC is therefore focused on three primary data sources—the network, endpoints, and log or event data. I would suggest a fourth data source which is human knowledge: tribal and procedural know-how about the environment that leaves the building when the SOC shift is over, or worse, when the person leaves the organization.

The security team needs a lot of information and, as alluded to above, can only process such a high volume using technology that can extract signal and represent the data as a collection of internal (devices, users etc.) and external entities (domains, etc.). Moreover, the technology must be able to pre-correlate those entities with their attributes, behaviors, relationships, and activity records as well as existing context such as directory services, HR systems, vulnerability, and threat data. Advances in data science can then be used to run analytics on the entities to find anomalous behaviors, what makes them unique and different in the environment, how entities are like other entities, etc.

This in turn allows the security team to satisfy requirement R3 above—moving beyond just IOCs (still necessary to handle the noise) to a model of defense based on understanding normal and abnormal, good and bad behaviors, etc.

The aggregation of information in this form also gives this capability to analysts of all skill levels and allows them to use it in real-time. In comparison today, if you are lucky enough to have experts on staff, they can certainly achieve the same result but with a lot of time, and dare I say frustration, along the way. Clearly that is not a long term workable model. Along similar lines, the SOC of the future also encourages and helps with the capture and sharing of knowledge, collaboration both internally and with outside peers, and the use of tried and tested playbooks for detection and response.

Finally, all of this must neatly integrate with existing tools and processes within the organization to make them more effective – e.g. allowing the organization to get more value out of SIEM, threat intelligence feeds, asset tracking, and remediation tools, among others.

Many vendors use the term “advanced analytics”. What exactly does it mean in the context of a complex enterprise security architecture, and how can advanced analytics help with keeping a large network more responsive to attacks, and therefore more secure?

Unfortunately, there has certainly been a flood of tools marketed as analytics solutions.

Many of them however fail because they neglect to capture the real-world entities we talk about above in their data model. Instead, they force security teams to piece together information about entities at query time from low-level data like IP addresses. The problems with this approach are many:

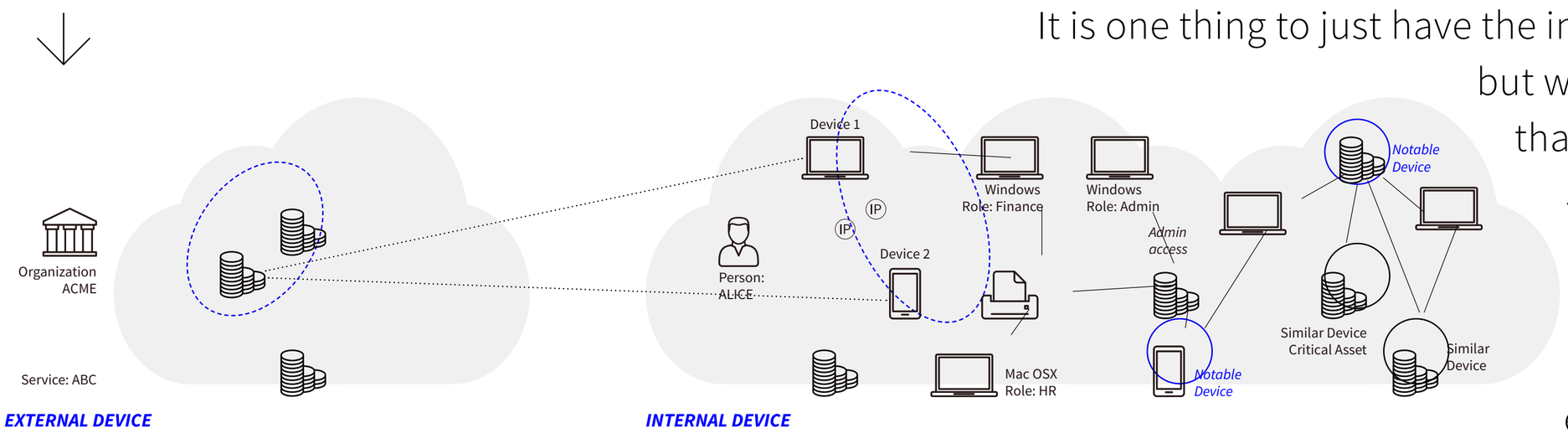
- It’s hard to formulate the right queries
- The process must be repeated again and again
- The queries themselves can be very slow to run, impairing productivity, since they often need self-joins on huge tables—this has led to the notion of “coffee-break queries”.

From the start at Awake Security, we were convinced that the right approach was having the system itself find and track the entities that match the analyst’s mental model, even before a query is conceived. Then, the analyst can query the system directly about the entity of interest and get results instantaneously even if that means aggregating information gathered from days, weeks or months of observation. Most importantly the analyst does not need to piece data together manually. Think of this as similar to instantly looking up the balance on your bank account, versus having to compute it each time by tallying the

transactions that have been performed on it since you opened the account.

We call this capability the Awake Security Knowledge Graph data model.

To build the Security Knowledge Graph, we had to decide what kinds of entities the system should model to make the analyst's life easiest, while also improving the likelihood of a rapid, conclusive investigation. Clearly information such as an internal IP address is typically not helpful on its own, since it mixes events and attributes of multiple devices using the address at different times. Therefore, we chose a "device"—that is, a communicating endpoint, which might be a server, client, IoT or BYO device—as a foundational entity type. A device may have different IP addresses over time. But that's just one entity. To understand the full set of entities we needed to model in the system, we combined feedback from 200+ security teams with our own deep in-house investigative expertise. In the end, we produced a model that can be summarized in the following diagram:



Or in words, analysts need to compile information about the person who uses a device (who may have multiple usernames and credentials), internal organizational entities that person is a member of, and external organizational entities they interact with. The person in question may interact with a given piece of data. The Awake model captures the relationships between these real-world entities.

The results of the Security Knowledge Graph approach exceeded even our own expectations. In our early deployments, analysts have been able to investigate alerts ten times faster than they could with other tools, and get more conclusive results. Importantly, the benefits are not restricted to just investigations either but also to behavioral detection and proactive threat hunting. Specifically, the impact of this entity data model on the hunting process is even more dramatic, both in terms of time and the quality of the hunt. For instance, finding all devices that are running Windows 7 with a particular patch version is trivial, as the data model would have summarized the OS running on the devices by collecting large numbers of indicators present in network data—and this works purely through passive network observation, without needing agents or log data. However, you could take the complexity of the query up a notch: it's also easy to find, in seconds, all such devices that have also connected to a given external domain or to all domains with a particular registrant email. You get the picture…

It is one thing to just have the information above, but we also recognized that the utility of the Security Knowledge Graph would also depend on the speed and ease with which analysts could extract answers out of it. And so, to enable our security analytics to execute queries like this and even more complex ones in seconds, we introduced the notion of pre-correlation: correlating events at ingestion time with their associated entities. Most solutions on the market cannot effectively do this due to the sheer scale of data volume and hence they lack the interactivity needed for an effective hunting process.

When was the last time your anti-virus software alerted you?

AUTHOR_Hyder Rabbani, Chief Operating Officer at CyberSight

I started my tech journey with PCs in the mid 1980s, with CP/M, MS-DOS and applications like WordStar, dBase II and the must-have for all tech geeks at the time: Norton Utilities, which eventually came to include Norton AntiVirus in the early 1990s.

Since that time, it's been standard practice for business and home users to buy and install anti-virus software on PCs for fear of viruses, Trojans, adware and other nasty software. Most IT budgets include a standard line-item for "AV" without a second thought.

On a recent trip to Singapore I had several interesting conversations with CIOs, CTOs, CSOs and CISOs of multiple large companies representing the healthcare, telecom, broadcast and semiconductor industries.

I wanted to learn what these executives are dealing with, particularly for endpoint security and the threat landscape, and how they are addressing problems. We discussed deploying advanced security measures, powerful firewalls and monitoring systems.

I asked each IT executive what their organization uses for cybersecurity software. Everyone named at least one anti-virus (AV) title. I asked why they were still using AV. The executive's responses weren't what I expected – instead of naming threats like viruses, malware, spyware, or similar software, they responded instead that their AV was "for compliance, because our financial auditors require AV software" or that AV "is a standard requirement for all PCs."

I went further and asked them when was the last time their AV software alerted them to a problem. In every case, the answer was either "a long time ago" or "I don't recall the last time." I thought about my own devices at work and home. I have AV software

installed on every device, and I, too, could not recall the last alert from my software.

These conversations got me thinking: what if we are investing in AV software to detect and manage threats that no longer pose the risks they did in the past? Is this money and effort being wasted?

What could be causing the steep decline in traditional threats that AV products detect and stop?

In the old days viruses and malware were generally a nuisance perpetrated to cause interruption by hackers who were seeking fame or stealing data or going after monetary gains. New threat databases usually solved the problem and numerous companies were born to deal primarily with the threat of viruses. However, things have changed.

Today, one of the most nefarious threats is ransomware, which not only penetrates the computing environment but also encrypts data files, rendering them inaccessible. Ransomware has become sophisticated. It can be polymorphic, multi-threaded and capable of silently deploying “Easter eggs” that can quietly collect data and detonate at a later date and time.

The press regularly reports on crippling ransomware attacks targeting hospital systems, police departments, transportation, financial institutions and ordinary users.

There are multiple reasons for this shift, but perhaps the biggest is that cybercriminals have realized ransomware is far more lucrative than old-school viruses. Simple, large-scale deployments can be done at low or no-cost via email, social engineering or phishing. Many ransomware strains detect online backup services and compromise them, rendering backups useless, and decryption tools are often limited in their scope and ability to reverse malicious file encryption. As a result, many attacked organizations simply pay the ransom demanded, especially when critical business operations, like hospital patient admittance and recording or emergency services dispatch, are affected. Also, the ransoms are primarily paid in cryptocurrencies that are anonymous and untraceable and authorities are generally unable to find and prosecute cyber criminals, particularly if they are in foreign locations.

Furthermore, unlike traditional viruses, ransomware doesn't require development by experienced hackers; it can be outsourced to "ransomware-as-a-service" (RaaS) providers that offer complete turn-key solutions, even going so far as setting up payment collection and forwarding. With RaaS, there are no upfront or out-of-pocket costs. Instead, RaaS providers offer creative "revenue share" deals. They collect ransom payments, deduct their share and pass the rest to the customer.

By comparison, traditional viruses are unsophisticated and unprofitable. As they say, follow the money. The money is now in ransomware.

It could be argued that ransomware IS the new virus.

+ Opportunities for bad actors to benefit from malicious software have never been easier. Given the evolved threat conditions, we need to rethink our security posture.

There are many great AV products in the market that claim anti-ransomware capabilities. We need to critically examine these tools and their performance, and ask the following questions:

1_Do they detect zero-day and unknown ransomware?
   a. If yes, how?
   b. What is the efficacy rate?
   c. What is the file loss rate (by ransomware strain)?
   d. How fast was the ransomware detected (milliseconds)?

2_Does the ransomware detection include multi-layered defense for polymorphic, multi-threaded and auto-run or boot up protection?

3_Does the AV require continuous updates of patterns or databases to detect new strains?

4_Are there rollback capabilities in the AV upon detection of ransomware encryption?

5_How does the AV compare to other ransomware-focused solutions?

In my business and home computing environments, I am rethinking my AV solutions and looking at how best to deploy solutions to better protect against the threats that are most prevalent today, like ransomware.

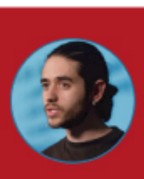
The first HITB Security Conference in China

October 29th - November 2nd @ Kempinski Beijing

Featuring some of our most popular past HITB speakers

The Grugq

Vice President of Threat Intelligence, Comae Technologies

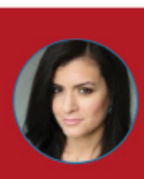


Hugo Teso

Head of Aviation Cyber Security Services, F-Secure Corporation

Sophia D'Antoine

Security Researcher, Trail of Bits

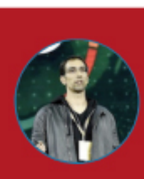


Najwa Aaraj

Senior Vice President – Special Projects, DarkMatter LLC

Fyodor Yarochkin

Threat Researcher at Trend Micro



Benjamin Kunz

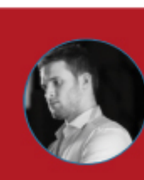
Founder, Vulnerability Lab

Emmanuel Gadaix

Founder, TSTF

Evan Booth

Challenge Designer, Counter Hack Challenges



Matteo Beccaro

Co-Founder/CTO, Opposing Force s.r.l.

Rodrigo Rubira Branco

Senior Principal Security Researcher, Intel Corp

Stefano Zanero

Associate Professor, Politecnico di Milano

Nikias Bassen

VP of Platform Researcher, ZIMPERIUM

Don Bailey

Founder, Lab Mouse Security

Jun Li

Senior Security Researcher, UnicornTeam, Qihoo360

Adam Laurie

Director, Aperture Labs

Marco Balduzzi

Senior Research Scientist, Trend Micro

Saumil Shah

Founder/CEO, Net-Square

James Forshaw

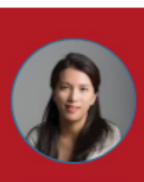
Security Researcher, Google Project Zero

Jaya Baloo

Chief Information Security Officer, KPN

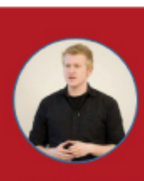
Haroon Meer

Founder, Thinkst



Lin Huang

Wireless Security Researcher, Qihoo360 Unicorn Team



Halvar Flake

Google

Andrea Barisani

Head of Hardware Security - F-Secure, Founder - Inverse Path

Fred Raynal

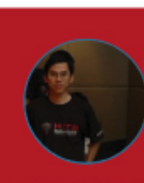
CEO, QUARKSLAB

Zuk Avraham

Founder, CEO at ZecOps / Founder, Chairman @ZIMPERIUM

Michele Spagnuolo

Information Security Engineer, Google



Thanh Nguyen

Founder, VNSECURITY

REGISTRATION OPENS JUNE 2018

https://conference.hitb.org/hitbsecconf2018pek/

2 & 3-day Hands-on Technical Trainings
Triple Track Conference with HITB Labs
CommSec Village / Exhibition
HITB CommSec Track
HITB Capture the Flag

Scan me

Software-defined perimeter: The pathway to Zero Trust

AUTHOR_ Jason Garbis, Vice President, Security Software Products at Cyxtera Technologies

Our networks and data are under attack. We live in an age of cyber warfare where no one should be trusted, yet we still use the same tools to secure our networks that were used by our parents two decades ago – tools that implicitly trust networks and the users that access them.

This makes the task of securing our networks nearly impossible, as the enterprise – and enterprise IT – changes rapidly. It's no longer static, but dynamic. It's no longer on-premises - it's hybrid. IT has never been more diverse and distributed: it's running in more locations, on more platforms and with more diversity of models than ever before.

Data stored in physical servers has been replaced by virtual ones, housed in data centers owned and controlled by third parties. The desktop PC still exists, yet it's surrounded by tiny mobile devices capable of accessing terabytes of data. Teams in multiple time zones can collaborate as if sitting mere inches away

from one another. Even the workforce is no longer confined to a desk within an office. Employees are free to connect from anywhere.

While these flexible working practices have delivered increased collaboration and productivity, they operate on a misplaced sense of trust, granting over-entitled access to entire corporate networks. Cyber criminals, disgruntled employees, third party contractors and employee mistakes are huge risk in a trusted approach to network security.

Trust no more

To address cyber warfare in our hyperconnected, diverse world, we need to abandon the notion of trust.

Zero Trust, an approach originally coined by Forrester, is a network security strategy that puts micro-perimeters around specific network services so that granular, user-centric access rules can be enforced. The fundamental concept – centered on the principle that neither internal nor external networks can be trusted – challenges organizations to change their thinking and secure their networks in a fundamentally different way.

There are three main concepts of Zero Trust according to Forrester:

First, when you eliminate the concept of trust from the network, it becomes natural to ensure that all resources are securely accessed — no matter who creates the traffic or from where it originates. You'll ensure all resources are accessed securely, regardless of location or hosting model including cloud, on-premises or collocated resources.

Next, by adopting a least privilege strategy that enforces access control, you eliminate the human temptation to access restricted resources.

A least privilege strategy should provide precise, fine-grained control of user access to resources, adjust user access dynamically based on context, and ensure the SDP system is inaccessible to unauthorized users.

Finally, Zero Trust allows you to continuously inspect user traffic for signs of suspicious activity and log and analyze all network traffic.

This detects unauthorized access attempts, reduces noise for improved security analyst efficiency and provides compliance reporting needed in today's highly regulated landscape.

The most effective way to accomplish Zero Trust

Where do you start? There are five steps you can take to quickly move to a Zero Trust model.

1_Inventory all protected workloads: What workloads exist and where are they located? What other assets are needed to function? Are there specific regulatory controls that these workloads must adhere to?

2_Review access of protected workloads: Who has access (individuals, job functions, etc.) and what access do those people have? Do they need that access? Are there additional safeguards in place or regulatory controls these workloads must adhere to?

3_Secure access to protected workloads: Are workloads accessed securely, and only in a secure manner? This seems straightforward, but this is often a huge problem.

4_Adopt a least privilege strategy: Do all users have the access they need for their job function, and ONLY the access their need for their job function? Eliminate "over-privileged" users.

5_Inspect and log all network traffic. Are you aggregating your device and systems logs in a central repository? Can your security tools inspect and act upon any abnormal events found in traffic and log data? Is this raw data enriched with user identity and context?

These steps seem straightforward but are next to impossible to accomplish without modern security solutions and tools.

Yesterday's technologies have not kept pace

Arguably the best place to start is by evaluating and modernizing your existing security solutions. Start by reviewing the technologies that have not kept up with rapidly evolving IT infrastructure.

Twenty years ago, organizations had centralized IT with a physical perimeter. The enterprise built hardened perimeters with firewalls, VPNs and NACs to protect their internal networks. However, these obsolete tools are complex and expensive to operate. Fundamentally, these tools were created and designed in a safer and more open world and based on implicit trust.

Perimeter-based security solutions such as VPNs, next-gen firewalls and NACs are ineffective against malicious insiders and targeted attacks. These antiquated tools are also complex and expensive to operate and their putting your organization at risk.

So what type of network security architecture can help them meet the goals of Zero Trust?

A software-defined perimeter: The pathway to Zero Trust

Today's IT reality requires flexible and adaptive security, one centered on a user's identity instead of the various networks that they consume.

This approach is called a software-defined perimeter.

A software-defined perimeter dynamically creates one-to-one network connections between users and the data they access. It addresses the perimeter-less enterprise and is built on three core principles.

First, it's identity-centric. Designed around the user, it addresses the perimeter-less enterprise. Users are authenticated BEFORE they can connect to a network.

Second, it enforces a "Zero-Trust model" so that anyone attempting to access a resource must authenticate first. All unauthorized resources are invisible. This applies the principle of least privilege to the network and completely reduces the attack surface. By default, users are not allowed to connect to anything – the opposite of traditional corporate networks, where once a user is given an IP address, they typically have access to everything on the network. Instead, Zero Trust ensures that once proper access criteria are met, a dynamic one-to-one connection is generated from the user's machine to the specific resource needed. Everything else is completely invisible.

Finally, it's architected for hybrid environments – built for the cloud, and like the cloud. It has no centralized network chokepoint. It's completely distributed and as scalable as the internet itself. A software-defined perimeter is engineered to operate natively in cloud networks. It's not simply a modified perimeter-based device that's been place into a virtual machine. Plus, it's completely compatible with existing corporate networks, integrating and augmenting your existing security tools and network devices, modernizing your existing investments.

A software-defined perimeter is the most effective way to accomplish Zero Trust. It controls over-privileged remote or third-party user access, helps to securely migrate critical workloads to the cloud, and remove constraints on cloud DevOps.

Malware world

VPNFilter malware compromises over 500,000 networking devices around the world

Cisco Talos researchers have flagged a huge botnet of small and home office routers and NAS devices, capable of collecting communications and data and launching cyber attacks.

About the VPNFilter malware

The malware that makes it all possible has been dubbed VPNFilter. It's persistent, modular, and delivered in several stages.

The stage 1 malware's main task is to persist through reboots and to discover the IP address of the current stage 2 deployment server.

The stage 2 malware is downloaded from those servers (one of which has been seized by the FBI) and is capable of collecting files, exfiltrating data, managing the device and executing code on it.

Some versions also have the capability to overwrite a critical portion of the device's firmware and reboot the device, effectively rendering it unusable. Although, as the researchers pointed out, it's more than likely that the threat actor running the botnet can deploy this self-destruct command to most devices that they control.

The stage 3 modules are effectively plugins for the stage 2 malware. One can sniff and collect traffic that passes through the device (including website credentials), another allows the malware to communicate with the C&C server via Tor. The researchers believe there are other plugins, but so far they've only been able to discover and analyze those two.

The data collection capability could be used to assess the potential value of the network that the device serves.

"If the network was deemed as having information of potential interest to the threat actor, they may choose to continue collecting content that passes through the device or to propagate into the connected network for data collection," the researchers noted.

"At the time of this posting, we have not been able to acquire a third-stage plugin that would

enable further exploitation of the network served by the device. However, we have seen indications that it does exist, and we assess that it is highly likely that such an advanced actor would naturally include that capability in malware that is this modular."

About the VPNFilter botnet and likely botmaster(s)

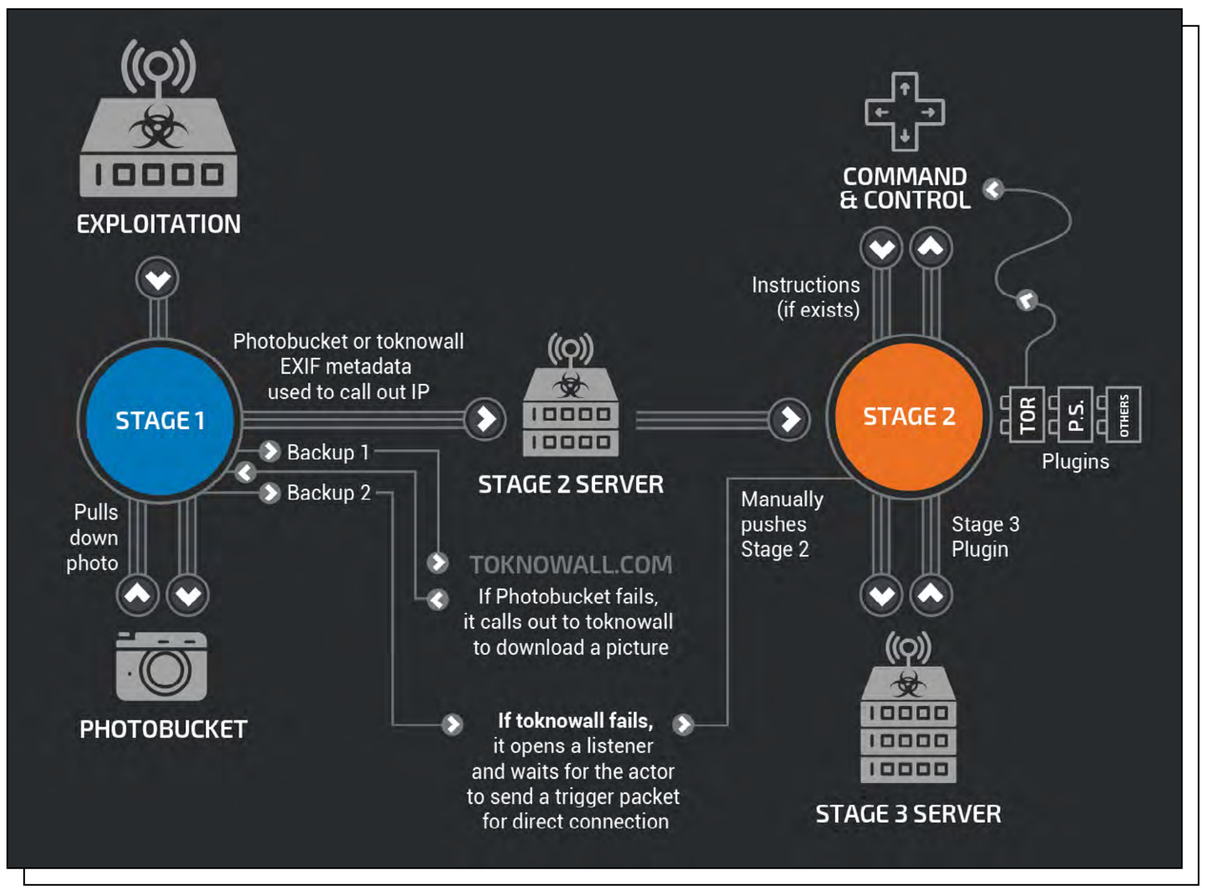
The botnet has been slowly growing since at least 2016 and currently consists of at least 500,000 infected devices in some 54 countries around the world.

"The known devices affected by VPNFilter are Linksys, MikroTik, NETGEAR and TP-Link networking equipment in the small and home office (SOHO) space, as well at QNAP network-attached storage (NAS) devices. No other vendors, including Cisco, have been observed as infected by VPNFilter, but our research continues," they shared.

"The type of devices targeted by this actor are difficult to defend. They are frequently on the perimeter of the network, with no intrusion protection system (IPS) in place, and typically do not have an available host-based protection system such as an anti-virus (AV) package. We are unsure of the particular exploit used in any given case, but most devices targeted, particularly in older versions, have known public exploits or default credentials that make compromise relatively straightforward."

They noted that their research is far from complete, but they went public with it because they fear the botnet will soon be used for attacks against targets in the Ukraine.

"The code of this malware overlaps with versions of the BlackEnergy malware — which was responsible for multiple large-scale attacks that targeted devices in Ukraine. While this isn't definitive by any means, we have also observed VPNFilter, a potentially destructive malware, actively infecting Ukrainian hosts at an alarming rate, utilizing a command and control (C2) infrastructure dedicated to that country. Weighing these factors together, we felt it was best to publish our findings so far prior to completing our research."



The similarity to BlackEnergy and the recent focus on Ukrainian hosts seem to point to a Russian-backed actor operating the botnet, although it's impossible to know for sure.

"This is a very sophisticated, multi-stage malware that allows attackers to spy on all network traffic and deploy destructive commands to industrial devices in critical infrastructure networks," commented Phil Neray, VP of Industrial Cybersecurity at CyberX. "Russian threat actors have previously used similar tactics in cyberattacks on the Ukrainian

electrical grid. While the recent burst of activity also targets the Ukraine, the malware exploits vulnerabilities in devices that are widely used around the world — which means the same attack infrastructure could easily be used to target critical infrastructure networks in the US, the UK, Germany and any other countries seen as enemies of the attackers."

What to do?

Cisco Talos has created and deployed more than 100 Snort signatures for the publicly known vulnerabilities affecting the devices targeted by VPNFilter, and has started blacklisting the domains associated with the threat.

The company has also notified the manufacturers of those devices about the threat and shared their research with international law enforcement and the Cyber Threat Alliance.

Owners of the affected devices should reboot them to remove the non-persistent malware elements and then reset them to factory defaults, which should get rid of the persistent, stage 1 malware.

They could then get in touch with the manufacturer and get instructions on how to make sure the devices are updated to the most recent firmware/software versions. Changing any default credentials is also a good idea, and so is turning off remote management of the device.

Since there's no easy way to determine whether a device has been compromised by the VPNFilter malware or not, Cisco researchers advise all owners of the targeted SOHO and NAS devices to go through those steps.

Fortnite is coming to Android, but malicious fake apps are already there

Android users eager to play the increasingly popular Fortnite survival game on their mobile devices are being targeted left and right with malicious apps masquerading as the game or apps related to it. Scammers are not waiting for summer to take advantage of the hype, and have already started pushing fake Fortnite apps, both on Google Play and third-party Android markets, and through dedicated websites.

Cryptominers displace ransomware as the number one threat

During the first three months of 2018, cryptominers surged to the top of detected malware incidents, displacing ransomware as the number one threat, Comodo's Global Malware Report Q1 2018 has found. Another surprising finding: Altcoin Monero became the leading target for cryptominers' malware, replacing Bitcoin.

Organizations across the UK are still struggling with ransomware

Webroot surveyed over 400 IT decision makers at UK businesses and found that 45 per cent of those surveyed had suffered a ransomware attack, with nearly a quarter (23 per cent) actually paying the ransom. Despite this finding, 88 percent of organizations feel better equipped to deal with an attack following WannaCry, suggesting a sense of false confidence.

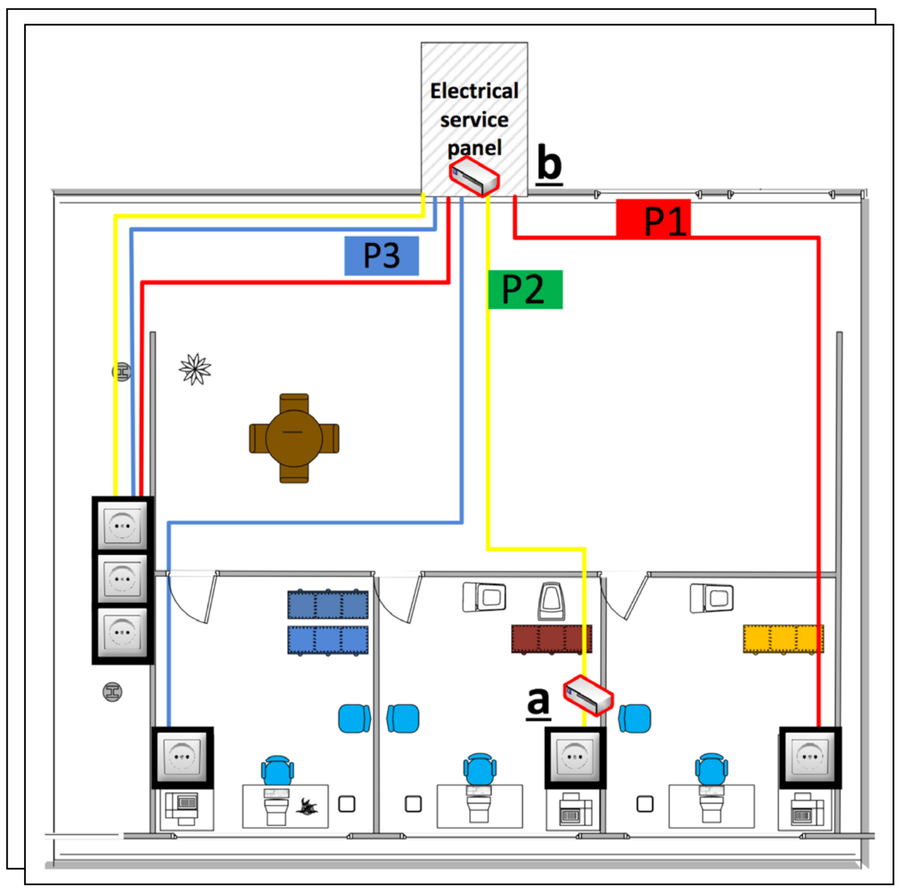
Researchers use power lines to exfiltrate data from air-gapped computers

Researchers from the Ben-Gurion University of the Negev have come up with another way to exfiltrate data from air-gapped computers: this time, it's via malware that can control the power consumption of the system.

"Data is modulated, encoded, and transmitted on top of the current flow fluctuations, and then it is conducted and propagated through the power lines," they pointed out. They call this malware PowerHammer.

Data exfiltration via power lines

They have devised two versions of the attack: line level power-hammering (the attacker taps in-home power lines directly attached to the electrical outlet) and phase level power-hammering (the attacker taps the power lines in the main electrical service panel).



"The receiver is a non-invasive probe connected to a small computer (for the signal processing). The probe is attached to the power line feeding the computer or the main electric panel. It measures the current in the power line, process the modulated signals, decodes the data and sends it to the attacker (e.g., with Wi-Fi transceiver)," the researchers explained.

Special malware present on the target computer harvests the wanted data (e.g., passwords, encryption keys, etc.), encodes the data, transmits it via signals injected to the power lines and delivers it to the probes.

The signals are generated by changing the workload on the CPU cores that are not utilized by working processes, so the computer would not slow down or show any indication of data exfiltration.

According to their testing, binary data can be extracted through the power lines at bit rates of 1000 bits per second for the first attack and 10 bits per second for the second.

Countermeasures

There are several things defenders can do to spot and protect computers from these types of attacks: they can monitor the currency flow on the power lines, install power line filters, engage in signal jamming, and implement host-based intrusion detection and prevention systems to continuously trace the activities of running processes.

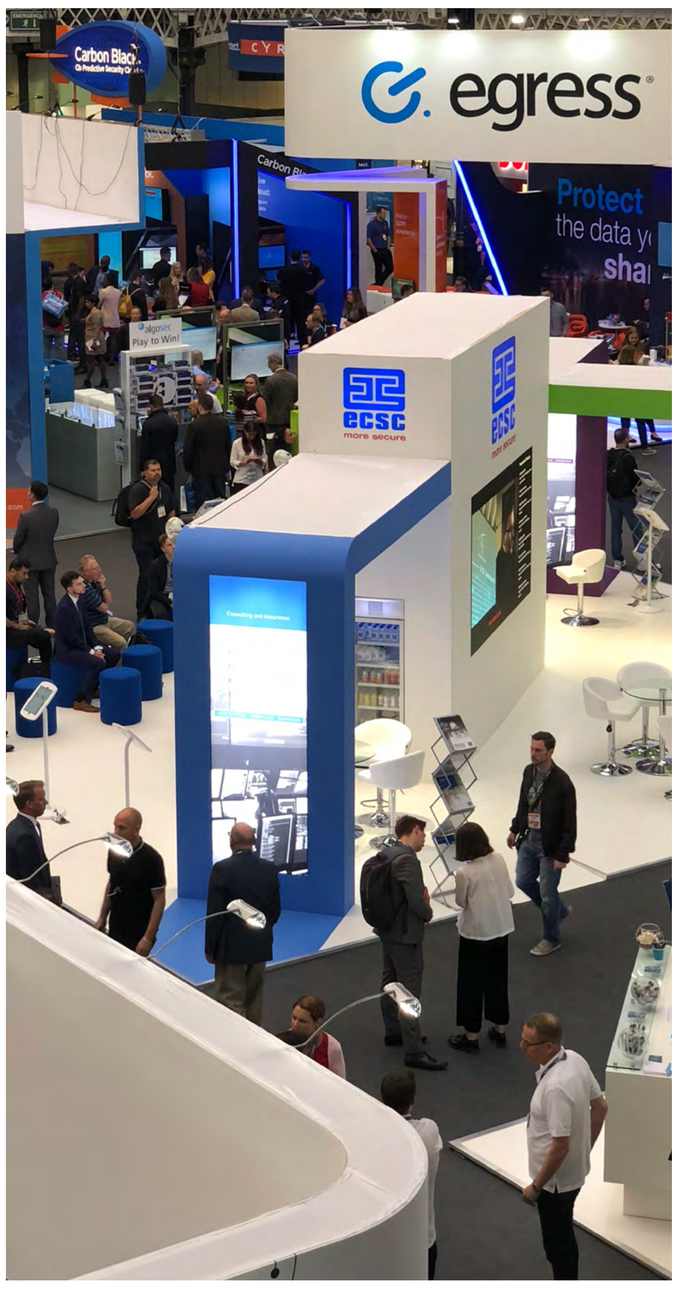
Each of these approaches has its weaknesses, though: unreliable results, can be thwarted by additional malware, too many false alarms, works for one type of attack and not the other, and so on.

REPORT:

Infosecurity Europe 2018

Infosecurity Europe 2018 in London featured over 400 exhibitors showcasing the latest security solutions, as well as a comprehensive conference program. Industry leaders addressed the challenges of building strong cybersecurity strategies and tactics to protect an organization's critical information assets.

A host of senior cybersecurity professionals discussed and debated the latest trends and hot topics in information security. Featured organizations included Domino's Pizza, GSK Technology, KPN Telecom, Marks & Spencer, Pinsent Masons, Ramsay Healthcare UK, Sainsbury's, Trainline, Vodafone and Williams Grand Prix Engineering.



Infosecurity gallery


infosecurity
EUROPE
NETWORKING
BAR
sponsored by
infosecurity
Infosecurity Europe Mobile App
Download and login to get going
@infosecurity
#infosec18
infosecurity
NETWORKING
BAR
better together
when they work
better together.


GUIDANCE SOFTWARE is now
opentext™
LOGPOINT
LogRhythm
The Security Intelligence Company
Threat Lifecycle Management Workflow
Time to detect
Time to respond
Discover
Qualify
Investigate
Neutralise
Recover
Security. Made Smarter.
LOGPOINT


Qualys.
Continuous Security
Use Case:
Vendor Risk Assessment
Assess cyber security controls of vendors & 3-parties
Gather Evidence
Review answers
Toilets
Cloakroom
Lift
Exit


GUIDANCE SOFTWARE is now
opentext™
LOGPOINT
LogRhythm
The Security Intelligence Company
Threat Lifecycle Management Workflow
Time to detect
Time to respond
Discover
Qualify
Investigate
Neutralise
Recover
Security. Made Smarter.
LOGPOINT


sumologic
Security Analytics as a Service
Continuous Intelligence Drives
Digital Business
ELASTIC, SCALABLE SERVICE
NATIVE CLOUD INTEGRATIONS
INDUSTRY-LEADING SECURITY & ATTESTATIONS
ADVANCED MACHINE LEARNING ANALYTICS
sumologic
Security Analytics as a Service
Continuous Intelligence Drives
Digital Business


ExtraHop
TRUSTED ACCESS
SECURONIX
Security Analytics. Delivered.
THE MOST VISIONARY SIEM PLATFORM
UEBA 6.0 | Security Data Lake | SIEM 2.0
algosec
Play to Win!
Share and collaborate securely
egress
Maintain GDPR compliance
Secure data in Microsoft Office 365
Prizes to be w
Okta Is Th dentity Cloud
Soliton
E220 Teramind Inc
Microsoft
Microsoft
microsoft.com/infosecurity

Most businesses still struggling with mobile working and security

95 percent of surveyed organisations in the UK recognise problems with mobile and remote working, and worryingly, 18% suggest their mobile workers don't care about security, according to Apricorn.

All surveyed IT decision makers noted that they had employees who work remotely at least some of the time, with an average of over a third (37%) of staff members who do so. With an increase in the numbers working remotely, this means more data moving beyond the confines of the corporate network, and organisations need to ensure that any data, be it at rest, or on the move, remains secure.

While many are taking steps, such as implementing security policies for mobile working and BYOD, to ensure their data is protected, just under half of respondents (44%) still agree that their organisation expects their mobile workers to expose them to the risk of a breach.

Roughly a third (32%) say that their organisation has already experienced a data loss or breach as a direct result of mobile working and to add to this, 30 percent of respondents from organisations where the GDPR applies are concerned that mobile working is an area that will most likely cause them to be non-compliant.

Fifty-three percent cited that one of their biggest problems with remote working is due to the complexity and management of the technology that employees use. Over half (54%) say that while their mobile workers are willing to comply with security measures, employees lack the necessary skills or technologies required to keep data safe.

To pay hackers' ransom demands or to invest in more security?

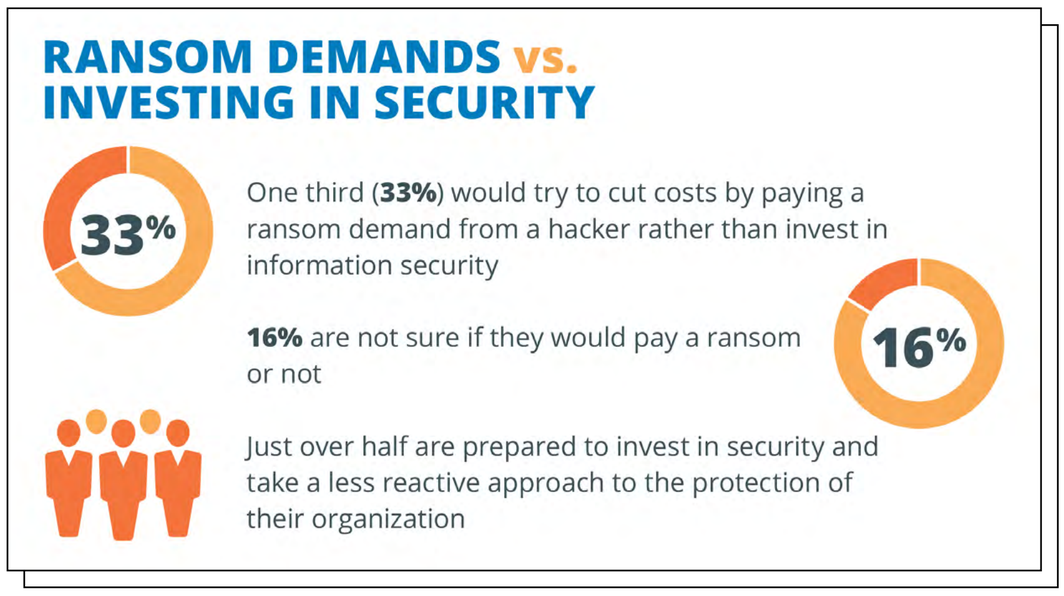
One third of business decision makers report that their organization would try to cut costs by paying a ransom demand rather than invest in information security.

The findings from NTT Security's latest Risk:Value report, show that a further 16 percent are not sure if they would pay or not, leaving just half of respondents prepared to invest in security and take a less reactive approach to the protection of their organization.

Examining business attitudes to risk and the value of information security, te company's annual Risk:Value report surveyed 1,800 C-level executives and other decision makers from non-IT functions in 12 countries across Europe, the US and APAC and from across multiple industry sectors.

The findings are particularly concerning, given the growth in ransomware. According to NTT Security's Global Threat Intelligence Report (GTIR) published in April, ransomware attacks surged by 350 percent in 2017, accounting for 7 percent of all malware attacks worldwide, while in EMEA, ransomware represented 29 percent of all attacks in the region.

Levels of confidence about being vulnerable to attack also seem to be unrealistic. Around half of respondents (47 percent) claim that their organization has not been affected by a data breach,



although of these 14 percent expect to suffer one, while a third do not expect to suffer from a breach at all. More worrying is the 12 percent globally who are not sure, an average driven up by the one in five (22 percent) in the UK who do not know if they have suffered a breach or not.

When it comes to the impact of a breach, respondents are most concerned about what a data breach will do to their image, with more than half concerned about loss of customer confidence (56 percent) and damage to reputation (52 percent).

The financial losses from a breach come second after image, according to the report. The estimated loss in terms of revenue is 10.29 percent on average, up from 2017's 9.95 percent, although executives in Europe are more optimistic, expecting lower revenue losses than those in the US or APAC. The estimated cost of recovery has increased to $1.5m, up from $1.3m in 2017 and $900k in 2015, while encouragingly respondents anticipate it would take 57 days to recover, down from 74 days in 2017.

Would you delete your account if a social media provider misused your data?

With the Facebook scandal involving Cambridge Analytica still fresh in people's minds, two-thirds of professionals admit they would delete their account if a social media provider misused their personal data. This is according to a snapshot poll of 220 cybersecurity and IT professionals conducted by Centrify at Infosecurity Europe.

Quizzed about attitudes to data breaches that involve identities (passwords, usernames, etc.) 59 percent of respondents say they have already deleted a social media account, while another 7 percent plan to if their data is misused. However, a significant third of respondents (32 percent) say they have no plans to delete Facebook or any other social media account.

Following major breaches at high profile organisations, including Uber, Equifax and TalkTalk in recent years, the poll also reveals that more than half (55 percent) of poll respondents would stop using a company following a data breach. However, 45 percent admit they would carry on using a company despite the risks.

Asked about their biggest concerns when it comes to privacy of personal data, just one in ten point to social media providers tracking or harvesting their personal information, while a third (34 percent) worry most about data breaches at companies that have access to their data, and a quarter admit credit card fraud is their biggest fear.

"It's really interesting to see how high profile stories involving big brands and social media providers are affecting our attitude to these companies and how they use – and indeed misuse – our personal information," comments Andy Heather, VP and Managing Director EMEA.

Discover all IT assets across your global hybrid infrastructure

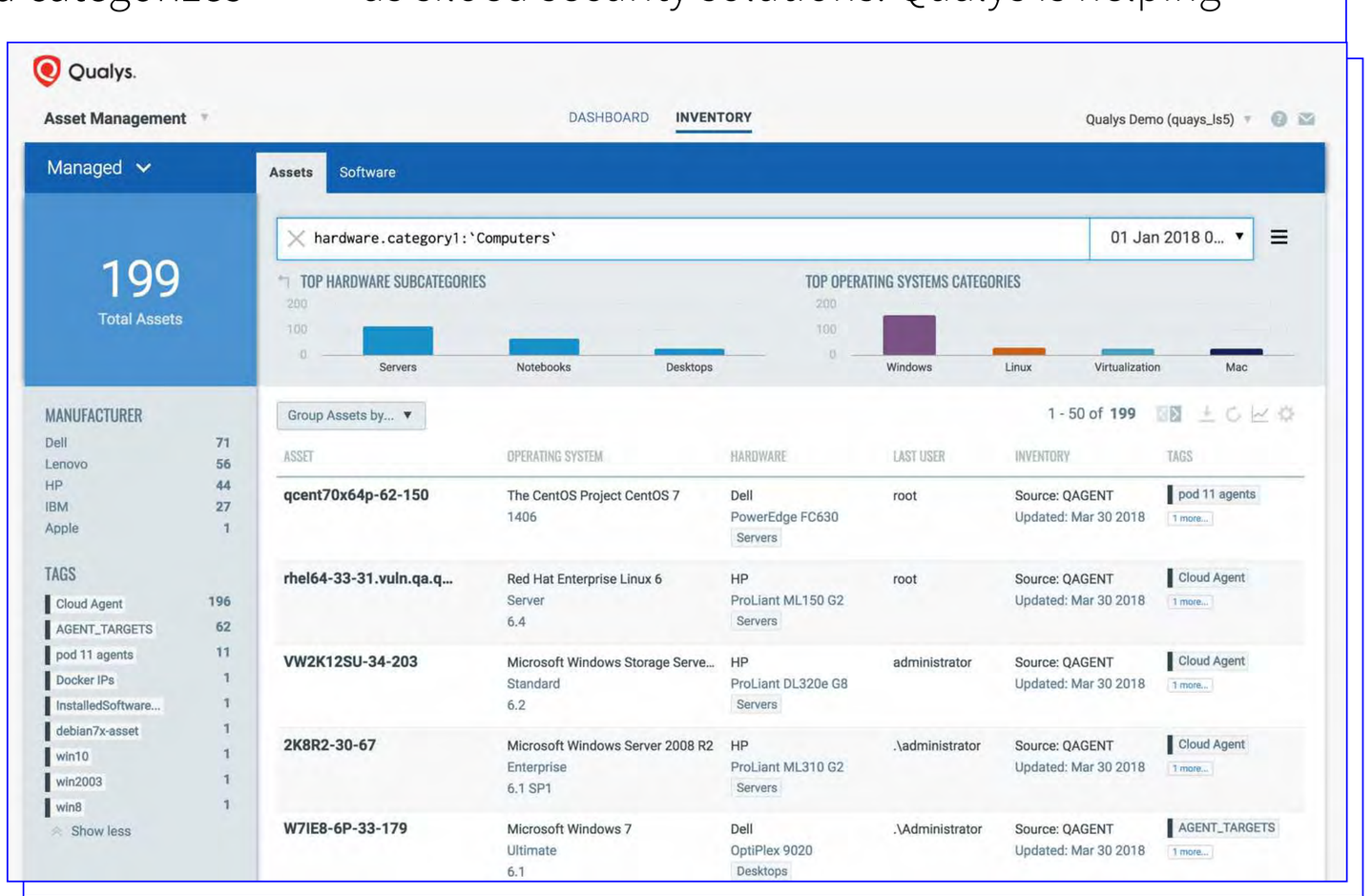
Qualys announced Asset Inventory (AI), a new cloud app with capabilities that provide customers a single source of truth for IT assets spread across hybrid environments including on-premises, endpoints, clouds and mobile, with synchronization capabilities to Configuration Management Databases (CMDBs) to keep asset data up-to-date.

Qualys' AI Cloud App leverages Qualys sensors including network scanners and Cloud Agents to discover all assets across global hybrid infrastructure, then normalizes and categorizes the information gathered for each hardware and software asset. By indexing and enriching asset inventory with metadata, the AI Cloud App delivers customers accurate CMDB data and out-of-the-box analytic capabilities.

This single, standardized source of truth allows teams to see assets from different perspectives, and leverage standard data for specific tasks, giving them unprecedented understanding of their asset landscape and ability to better manage them.

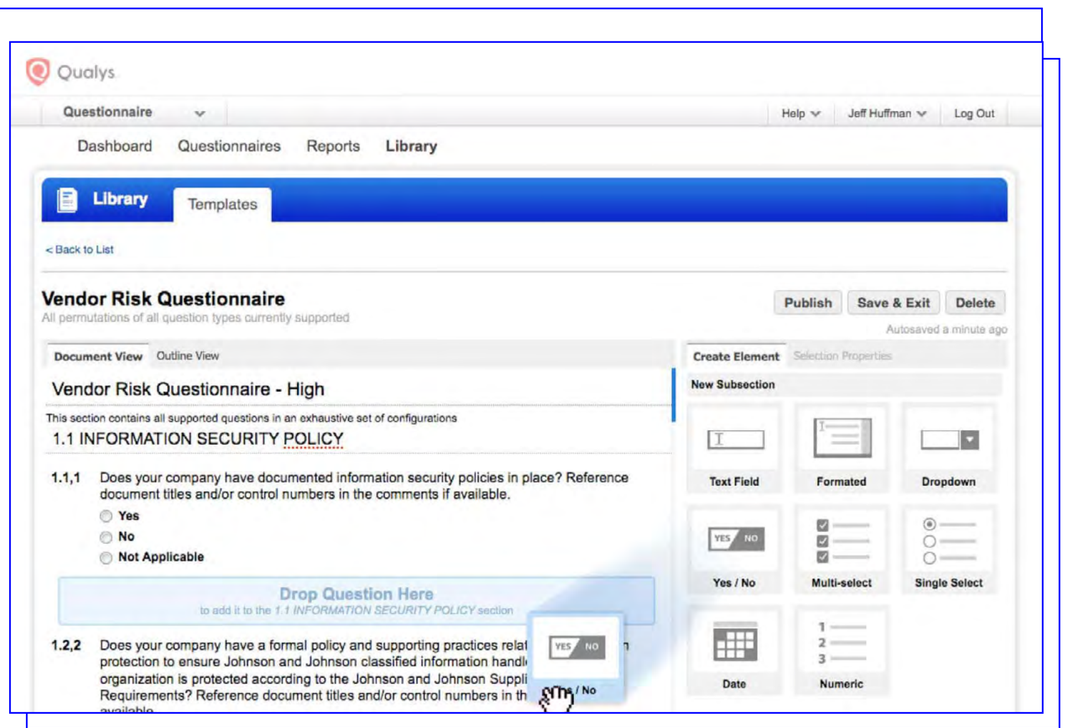
"Digital business is driving rapid changes in the way technology assets are deployed, used and managed, and also in the very definition of 'technology asset,' according to Gartner. "Sourcing and vendor management leaders must rapidly mature their IT Asset Management discipline in order to deliver on the promise of digital business."

The digital transformation and the ever-evolving cybersecurity threat landscape introduce new technology at increasing variety, scale and speed. Simultaneously, teams are trying to manage resources and budget constraints as well as siloed security solutions. Qualys is helping



customers tackle these challenges by delivering a unified solution and a single source of truth that allows better interchange between the CIO and CISO to improve IT, and enables better collaboration and strategic planning across IT and Infosec.

Qualys streamlines supply chain GDPR compliance assessment with cloud app



Qualys announced new functionality in its Security Assessment Questionnaire (SAQ) cloud app that allows customers to better achieve visibility of data across their own network and supply chain for compliance with the GDPR.

New GDPR-specific SAQ templates and a purpose-built dashboard allow customers to reduce the cost and effort of risk assessment to determine the status of their own business and procedural readiness for GDPR, as well as that of vendors in their supply chain.

SAQ will also offer customers a single dashboard from which to launch GDPR campaigns, manage new GDPR templates, and manage risky third-party vendors. This new tool will simplify the execution and management of GDPR vendor risk assessments by saving time and effort.

With a single pane of glass for all GDPR-related assessments, customers can launch new GDPR assessments using the SAQ templates within a matter of minutes and a few clicks. Information on the status and aging of all assessments, vendor risk data along with risk scoring will be available on this dashboard.

Each of the seven new questionnaire templates spells out GDPR requirements in granular detail and helps teams assess their business readiness for GDPR compliance:

- **GDPR Business Readiness Self-Assessment** Designed to identify key areas where operational changes will be required, and to assist the organization in prioritizing efforts for GDPR compliance.
- **GDPR Data Inventory and Mapping**: Helps in assessing the process to identify, locate, classify and map the flow of GDPR-protected data.
- **GDPR Accountability and Responsibility Assessment**: Helps in assessing the process of accountability and responsibility in terms of data governance as per GDPR requirements.
- **GDPR Data Privacy Assessment in Operations:** Focuses on assessing appropriate technical and organizational measures to protect EU residents' personal data from loss or unauthorized access or disclosure.
- **GDPR Third-Party Vendor Assessment:** Helps to identify and assess the requirements of third-party vendors with which you share personal data of EU residents.
- **GDPR Data Incident and Breach Notification Assessment:** Helps in the assessment of GDPR's data breach notification and communication requirements.
- **GDPR Data Protection and Privacy Impact Assessment:** Helps organizations in the assessment of the privacy risks and data protection safeguards of new projects.

Life after May 25th: How large organization should navigate the new security reality

AUTHOR_ Mike McKee, CEO of ObserveIT

It's hard to believe that May 25th has come and gone, leaving a new era of regulation with little precedent on how it may unfold.

Companies across the global are working to find their footing, but in particular for large organizations the stakes are high and the impact substantial. With Gartner estimating that, by 2020, 40 percent of organizations will be in violation of GDPR, organizations need to stop discussing the regulation and start acting on it. To understand GDPR best practices for your organization, lets first discuss the security requirements associated with the regulation.

The Rulebook

While the level of complexity varies across organizations, all companies should begin their compliance journey by considering the following GDPR security requirements:

- **Article 5, "Principles relating to personal data processing"** requires organizations to assume processes and technology that establishes data confidentiality – including the prevention of unauthorized processing.
- **Article 24, "Responsibility of the controller"** requires companies to monitor and demonstrate compliance with processes and technology that provide total visibility, detection, and prediction of user-based risks.
- **Article 25, "Data protection by design and by default"** gives direction on the implementation of the appropriate technical and organizational measures for ensuring that only necessary personal data is processed.
- **Article 32, "Security of processing"** ensures organizations are taking proper steps to anonymize and encrypt personal information when collecting data. It also ensures that organizations apply CIA (Confidentiality, Integrity, and Availability) concepts to data processing, creating standards

for accountability around data retrieval and processing.

- **Articles 33/34, "Notification of a personal data breach to the supervisory authority"** requires organizations to notify data owners and controllers of a data breach that may involve user data. A procedure must be in place to enable swift notification channels in the event of a data breach.
- **Article 35, "Data protection impact assessment"** compels organizations to evaluate technologies for effective data processing strategies, taking into account the impact to user data privacy.
- **Article 39, "Tasks of the Data Protection Officer (DPO)"** makes organizations appoint one point-person to both monitor and implement GDPR on the whole. This means through technology and processes, and also through staff trainings to increase internal awareness.

Pain points of implementation: Key considerations to understand

Given the nature of the regulation, execution and enforcement will vary from country to country. Regardless of location, organizations around the world will need to accept this set of mandatory guidelines, many of which pose more challenges than solutions when it comes to implementation.

Enforcement will be the largest obstacle long-term as regulators struggle to figure out how to measure GDPR compliance. Although there are many clear limits in the guidelines, including the 72-hour requirement to notify users of an incident involving their data, there are pitfalls in the logistics around the guidelines. The main issue comes with how – how exactly should organizations respond, and what are the appropriate responses for when a data breach incident happens, and in-scope user data is impacted? For full enforcement to be effective, the question of how must first be addressed by both organizations and regulators.

For large organizations in particular, one of the biggest obstacles is that GDPR will expose how woefully unknowledgeable most organizations are about what data they have collected, where it resides and how it is being used. With major organizations juggling so many moving pieces, enforcing company-wide standards around data management can be difficult, especially when employee ignorance and oversight can make such protocols pointless. Additionally, in order to address these shortcomings, large organizations are taking drastic and costly steps –according to a 2017 PWC survey, 88 percent of companies reported spending more than $1 million on GDPR preparations and 40 percent reported spending more than $10 million.

The GDPR guidelines raise the question of how organizations will best understand which users and data flows are in scope of the regulations? Segmenting users into specific compliance groups might help, but organizations will still need to integrate additional technologies and processes. The best use of this technology will be to monitor for in-scope and out-of-scope data flows on endpoint systems where users directly interact with data.

Best practices: The implementation checklist

1_To ensure compliance, the first step is to **implement a Privacy Impact Assessment (PIA),** which allows organizations to act purposefully when educating data subjects about data processes and retention times. The PIA ensures that organizations are documenting the purpose for data processing, exactly what data is being processed, as well as for how long that data is retained.

2_**Ensure an organization's privacy policy or privacy statement cover both internal employees and data subjects,** including customers and partners. It is crucial to make this privacy statement simple, easy to understand and transparent about:

- What information is collected?
- Who is collecting it?
- How long is it retained?
- Where is it being shared?
- How can data subjects either correct (rectify) or control the use and distribution of the collected information?

Having such a document will make communication across offices and departments simpler and more concrete, ensuring all involved understand the company's objectives.

3_**Create an orderly process for notifying users** when their data has been breached. A comprehensive breach notification should include the following:

- Volume and type of data breached, and data subjects affected
- Any existing measures taken
- What are the likely consequences
- What are the planned mitigations

The larger the corporate food chain, the more vital this process is. Companies need to understand who needs to know, when they need to know it, and where the bottlenecks are located.

4_**Appoint a data protection officer (DPO)** who is responsible for overseeing and advising compliance efforts, training staff, and processing personal data requests. The DPO should work closely with business process owners, allowing them to make proper, risk-based decisions regarding large scale data.

The European Commission explains officers are only necessary for companies where their core activities involve processing of sensitive data on a large scale. Community doctors and small law firms will, therefore, not need a DPO but large organizations will likely need to appoint someone to the position.

5_**Organizations need to establish or reassess efforts to meet required policies** and large organizations should be conducting periodic risk assessments and mitigating any issues that arise. This is critical to ensure that proper data handling and data protection procedures are in place, working as expected and covering all expected data flows. Without having a process that continually and consistently ensures all data privacy controls are in place, GDPR functions as a one-time event not as part of your overall data privacy strategy. Given the scale of large organizations, this can create additional risk relating to the data they are collecting.

Critical activities for successful assessments include documenting what data is being masked or anonymized, what data should be encrypted, whether data is being shared with approved parties, retained within allowed time periods, and properly deleted upon request or after the retention period has expired.

6_**Educate internal parties about the risk and legalities relating to GDPR.** Failure to do so can be some of the biggest risks for both an organization and their data. Particularly when organizations have several offices and numerous employees, it is crucial to make everyone at all levels understands the ins and outs of the new guidelines.

Organizations need to act accordingly in order to save themselves from the financial and brand reputation consequences of non-compliance. Organizations around the world are working through the logistics of GDPR, but ignorance will not be an excuse now that the law has gone into effect. By following the proper protocol, organizations large and small can thrive in the new standard of security.

Introducing

Two new free services!

CertView

qualys.com/certview-free

Full inventory of your Internet-facing certificates

See your SSL/TLS configuration grades with recommended fixes

Identify the certificate issuer

Track certificate expiration

Instantly upgrade to include internal certs

CloudView

qualys.com/cloudview-free

Total visibility into your public cloud workloads & infrastructure

See all of your cloud assets from a single-pane interface

Monitor your clouds' users, instances, networks, storage, databases and their relationships

Instantly upgrade to run security assessments on your cloud assets

Qualys®

Combating fraud and money laundering with graph analytics

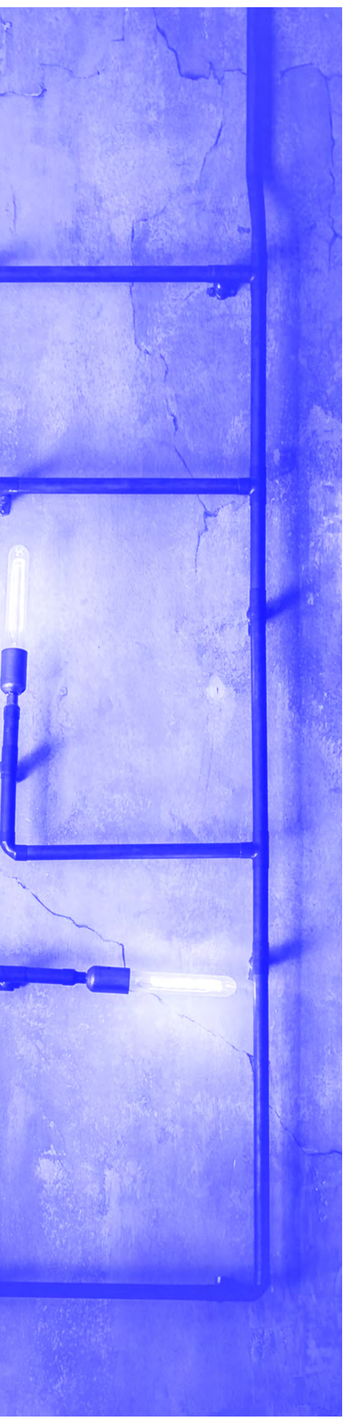
AUTHOR_ Yu Xu, CEO at TigerGraph

Dirty money and money laundering have been around since the dawn of currency. The United Nations estimate that, on a global level, as much as $2 trillion is laundered annually. Today's criminals are sophisticated and are constantly adapting tactics to bypass traditional anti-fraud solutions. Even in cases where enterprises have enough data to reveal illicit activity, more often than not they are unable to conduct analysis to uncover it.

As the fight against money laundering continues, AML (anti money laundering) compliance has become big business. Global spending in AML alone surpasses $8 trillion, according to WealthInsight. Considering how any organization facilitating financial transactions falls within the scope of AML legislation, this figure will continue to grow.

Combating crime is never easy, especially when organizations face pressure to reduce cost and minimize the time it takes them to achieve AML compliance to avoid regulatory fees. Legacy monitoring systems have proven burdensome and expensive to tune, validate and maintain. Often involving manual processes, they are generally incapable of analyzing massive volumes of customer, institution and transaction data. Yet it is this type of data analysis that is so critical to AML success.

New ideas have emerged to tackle the AML challenge. These include semi-supervised learning methods, deep learning-based approaches, and network/graph-based solutions. Such approaches must be able to work in real time and handle large data volumes – especially because new data is generated 24/7. That's why a holistic data strategy is best for combating financial crime, particularly with Machine Learning (ML) and AI to help link and analyze data connections.



Graph analytics for AML

Graph analytics is an ideal technology to support AML. Graphs overcome the challenge of uncovering the relationships in massive, complex and interconnect data.

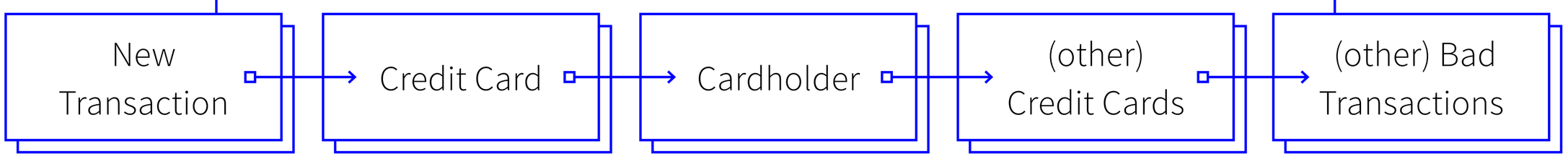
The graph model is designed from the ground up to treat relationships as first-class citizens. This provides a structure that natively embraces and maps data relationships, even in high volumes of data, and provides maximum insight into data connections and relationships.

For example, “Degree Centrality” provides the number of links going in or out of each entity. This metric gives a count of how many direct connections each entity has to other entities within the network. This is particularly helpful for finding the most connected accounts or entities that are likely acting as a hub and connecting to a wider network. Another is “Betweenness,” which gives the number of times an entity falls on the shortest path between other entities. This metric shows entities that act as a bridge between other entities. Betweenness can be the starting point to detect any money laundering or suspicious activities.

Today’s organizations need real-time graph analytic capabilities that can explore, discover and predict very complex relationships.

This represents Real-Time Deep Link Analytics, achieved utilizing three to 10+ hops of traversal across a big graph, along with fast graph traversal speed and data updates.

Let’s take a look at how Real-Time Deep Link Analytics combats financial crime by identifying high-risk transactions. We’ll start with an incoming credit card transaction and demonstrate how this transaction is related to other entities:



This query uses four hops to find connections only one card away from the incoming transaction. Today’s fraudsters try to disguise their activity by having circuitous connections between themselves and

known bad activity or bad actors. Any individual connecting the path can appear innocent, but if multiple paths from A to B can be found, the likelihood of fraud increases.

More hops are needed to find connections two or more transactions away. This traversal pattern applies to many other use cases, where you can simply replace the transaction with a web click event, a phone call record or a money transfer. With Real-Time Deep Link Analytics, multiple, hidden connections are uncovered, and fraud is minimized.

By linking data together, Real-Time Deep Link Analytics can support rules-based ML methods in real time to automate AML processes and reduce false positives. Using a graph engine to incorporate data science techniques such as automated data flow analysis, social network analysis, and ML in their AML process, enterprises can improve money laundering detection rates with better data, faster. They can also move away from cumbersome transactional processes and towards a more strategic and efficient AML approach.

Example: E-payment company

For one example of graph analytics powering AML, we can look at the #1 e-payment company in the world. Currently this organization has more than 100 million daily active users and uses graph analytics to modernize its investigation methods.

Previously, the company's AML practice was a very manual effort, as investigators were involved with everything from examining data to identifying suspicious money movement behavior. Operating expenses were high, and the process was highly error-prone.

By implementing a graph analytics platform, the company was able to automate development of intelligent AML queries, using a real-time response feed leveraging ML. Results included a high economic return using a more effective AML process, reducing false positives and translating into higher detection rates.

Example: Credit card company

Similarly, a top five payment provider sought to improve its AML capabilities. Key pain points included high cost and inability to comply with federal AML regulations. The organization relied on a manual investigative process performed by an ML team comprised of hundreds of investigators, resulting in a slow, costly and inefficient process with more than 90 percent false positives.

The company is currently leveraging a graph engine to modernize its investigative process. It has moved from having its ML team cobble processes together towards combining the power of graph analytics with ML to provide insight into connections between individuals, accounts, companies and locations.

By uniting more dimensions of its data and integrating additional points such as external information about customers, it is able to automatically monitor for potential money laundering in real time, freeing up investigators to make more strategic use of their now-richer data. The result is a holistic and insightful look at its colossal amounts of data, producing fewer false positive alerts.

As we continue into an era of data explosion, it is more and more important for organizations to make the most of analyzing their colossal amounts of data in real time for AML. Graph analytics offers overwhelming potential for organizations in terms of cost reduction, in faster time to AML compliance and most importantly, in their ability to stop money laundering fraudsters in their tracks.

Events

Black Hat USA 2018

August 4-9, 2018
Mandalay Bay, Las Vegas, USA
https://www.blackhat.com/us-18/

Now in its 21st year, Black Hat USA is the world's leading information security event, providing attendees with the very latest in research, development and trends. Black Hat USA 2018 opens with four days of technical Trainings (August 4 – 7) followed by the two-day main conference (August 8 – 9) featuring Briefings, Arsenal, Business Hall, and more.

HITB GSEC Singapore

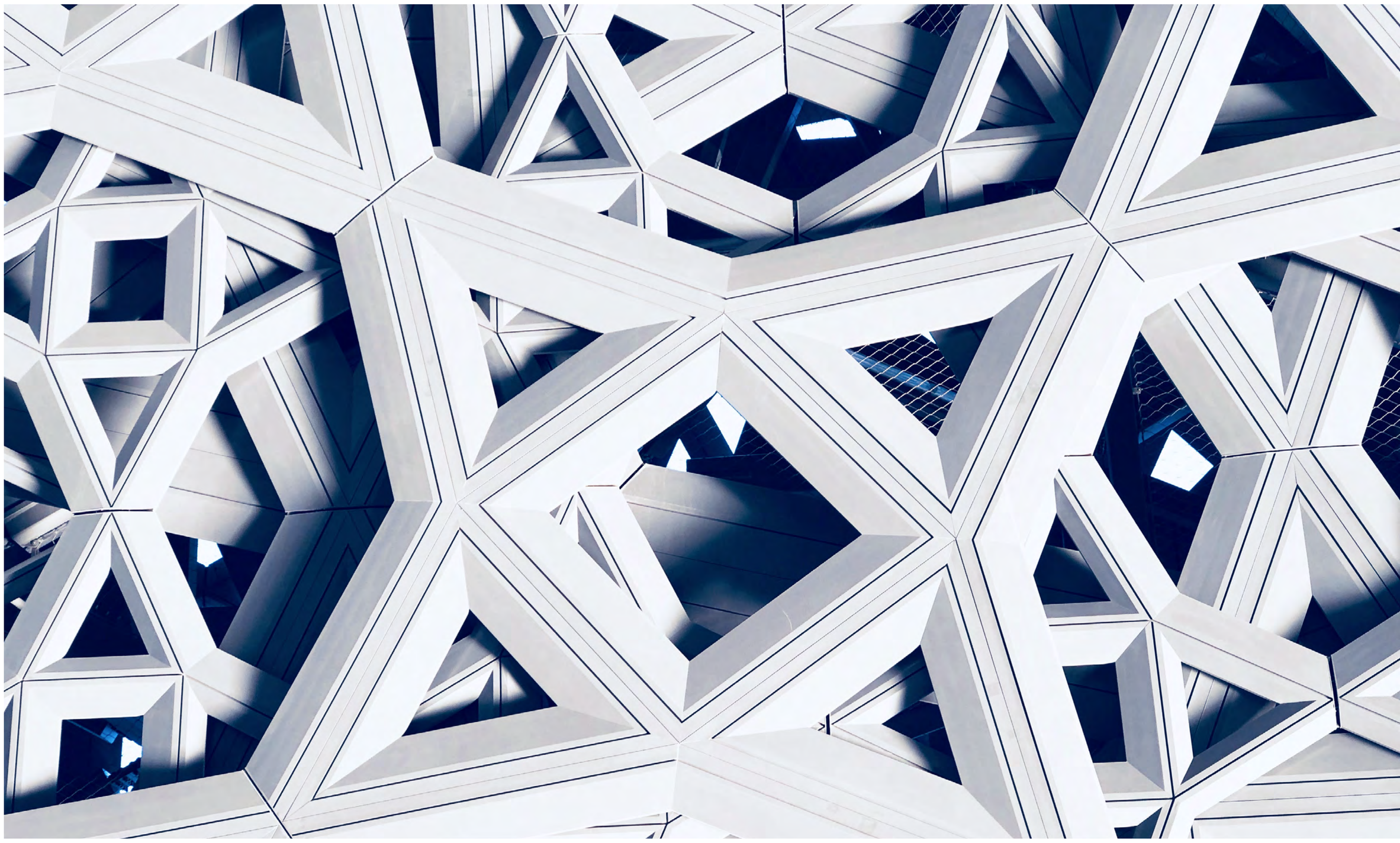
August 27-31, 2018
InterContinental Singapore
https://gsec.hitb.org/sg2018/

The conference that puts the power of speaker selection in your hands returns to Singapore for the fourth year! HITB GSEC 2018 Singapore takes place August 27th 'till the 31st at Intercontinental and again features a single, audience-voted track of talks and an additional free-to-attend track of 30 minute talks that runs alongside it.

HITBSecConf2018 Dubai

November 25-28, 2018
Grand Hyatt, Dubai
https://conference.hitb.org/hitbsecconf2018dxb/

After an 8-year hiatus, HITB Security Conference returns to the Middle East! Taking place November 25th till the 28th at the Grand Hyatt Dubai, the event features 8 hands-on technical training courses, a 2-day multi track conference with a Capture the Flag, technology exhibition and more!



Are SMBs driving the adoption of security automation by enterprises?

AUTHOR_ Corey Nachreiner, CTO at WatchGuard Technologies

If you tracked the lifecycle of new security technologies, you'd likely see that most start as enterprise solutions and eventually trickle down to small and medium-sized businesses (SMBs).

You could probably guess why new security technology flows in this direction. For starters, enterprises typically have more financial and human resources, and can afford to develop and roll out untested security solutions. New security solutions are also often immature, and thus more complex, but enterprises typically have dedicated security professionals that can decipher and monitor these emerging solutions. And finally, the industry still tends to suffer from the fallacy that sophisticated attackers primarily target bigger companies, so enterprise customers usually get first crack at advance security services.

Over time these technologies mature and develop, and eventually transition into SMB solutions.

However, right now the reverse is happening to security automation.

+ Enterprises are just now adopting more automated detection and prevention solution that have been common in SMBs for years.

Let's examine this issue in more detail and explain why automation seems to be moving in reverse.

You can probably recall a number of recent security technologies that fit the enterprise-to-SMB evolutionary profile. One that immediately comes to mind is advance malware detection. For decades, the security industry realized reactive, pattern or signature-based security solutions were losing efficacy. This was (and still is) because threat actors continued to evolve their attacks and refreshed their malware variants so regularly that signature-based solutions simply couldn't keep up with the deluge of new threats introduced daily. The industry had to come up with more proactive ways to catch new threats. Thus, behavioral malware detection was born, which became popular about five to ten years ago.

However, the original advanced malware detection solutions were complex and expensive. They required both expensive hardware virtualization appliances to detonate malware and a mix of network and endpoint technology to capture suspicious files to inspect. Early on, these solutions easily cost six figures to purchase and required trained security experts to understand and monitor the technology. When this tech emerged, there was no chance an SMB could use it. But much has changed in the last five years. Today, organizations can offload expensive processing tasks to public clouds. Expensive virtualization servers are no longer needed to detonate malware, which has made the technology both cheaper and easier to use. As a result, today SMBs can find advanced malware protection services as a checkmark feature in most unified threat management (UTM) solutions or next-generation firewalls (NGFW).

Many, if not most security technologies seem to follow this evolutionary example; starting as innovative but expensive and immature enterprise technology, and eventually developing into a more user-friendly, commoditized product that SMBs can afford. However, we're starting to see a new trickle-up trend developing in information security technology. Some of the attributes that make security consumable for SMBs are becoming just as attractive to bigger enterprises.

+ Besides price, the largest barrier to SMBs using newer security technology comes down to ease-of-use.

One key differentiator is the ability of enterprises to employ dedicated security professionals versus an SMB that's often just lucky to have an IT guy that knows security. SMBs don't have incident handlers that can monitor security dashboards all day and interpret security events. Not only do they need solutions than can consolidate many security controls into one pane-of-glass, but they also need these services to automate prevention, detection and remediation. Simply put, if the security solution requires a human to monitor threat intelligence and to make prevention or remediation decisions, the solution will likely not work for SMBs. For a long time, enterprises turned their noses up at consolidation and even automation. Why

consolidate security in one solution when they could pick and choose what they thought were the best-in-class services? Furthermore, since they're big enough to divide their security into dedicated teams for network, endpoint and application protection, it seemed to make sense to have individual controls for each of those teams. They also didn't always trust security solutions to make decisions for their business. Rather than automate detection and prevention with things like intrusion prevention solutions, they'd elect to stick with intrusion detection paired with their SOC and let incident handlers make the decision to block things or not.

However, the latest emerging security technologies suggest that enterprises have started rounding a corner and are adopting technologies that consolidate and automate security—something the SMB has been doing for years. On the consolidation side, security information and event management (SIEM) and orchestration technologies are now taking all the logs and management of many individual security systems and putting them under one pane-of-glass.

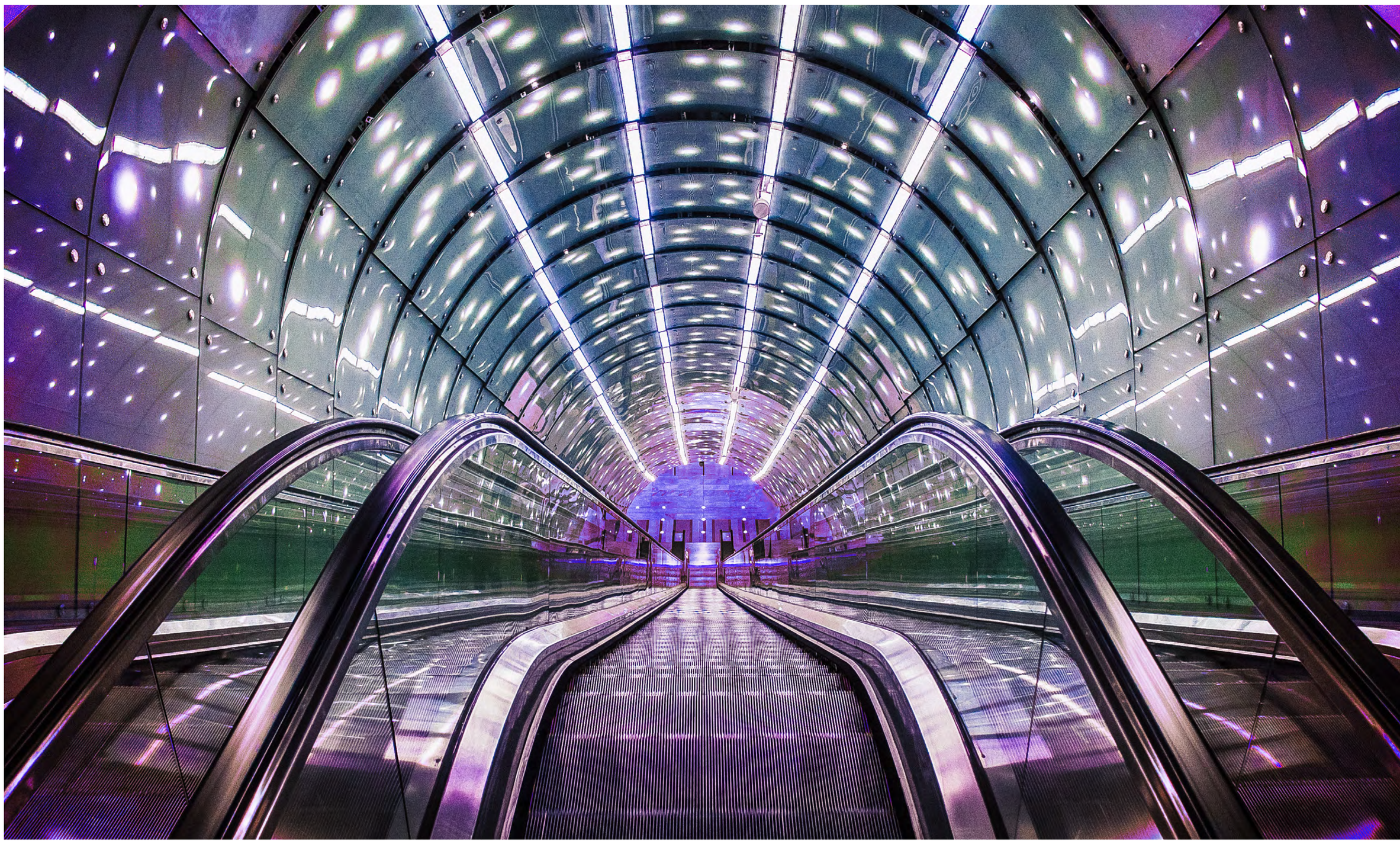
Meanwhile, on the automation side of things, enterprise incident handlers are failing under the huge deluge of security incidents they see from endpoint detection and response (EDR) and threat intelligence solutions. Even if they have security professionals to man these solutions, those handlers find themselves buried under an overflow of real and false incidents. As a result, they're turning to security automation solutions that correlate events using machine learning or other intelligence technologies.

+ Guess what enterprises? You're using technologies SMBs have relied on for a while now.

The whole point of consolidating security services into multifunction solutions like UTM and NGFW was to ease management. Furthermore, when all the technologies log information in one place, these solutions can automatically start to correlate and remediate events. Let me give you a specific example.

Some UTMs have threat detection and response solutions to help identify breaches in your network. Similar to EDR, these solutions can identify and remediate infected computers in your organization by correlating host and network-based security indicators. However, unlike the enterprise EDR solutions, SMBs can't rely on incident handlers to decide what incidents to remediate. Instead, SMB solutions must automate the event correlation and figure out if an incident really is a threat on its own. To do this, many solutions rely on machine learning to score the various indicators together or help polarize the score by automatically sending files to cloud sandboxes to monitor their behaviors. In the end, existing UTM threat detection and response services are already doing some of the things security automation systems are trying to do for enterprises.

SMBs have long known they could learn about information security from enterprises. While they can't always afford or manage the latest security technology, they can watch as it proves out in the enterprise market and adopt the more mature and effective solutions that come out the other end. However, it's time enterprises also realize they can learn from SMBs. They may have bigger budgets and more dedicated security staff, but even they can't keep up with the acceleration of threats coming from today's ecosystem. Consolidation and automation have helped SMBs survive the modern threat landscape so far, and it looks like both are trickling up to the large enterprise.



GDPR compliance: Identifying an organization's unique profile

AUTHOR_ Jason Straight, Senior Vice President and Chief Privacy Officer of Cyber Risk Solutions at UnitedLex

After a two-year transition period, the General Data Protection Regulation (GDPR) became enforceable on 25 May 2018. Presumably, many large companies have been working on a compliance program for months now. As the deadline approaches, many organizations are finding that ensuring compliance is a more complex endeavor than they had initially expected. GDPR replaces the 1995 Data Protection Directive (Directive 95/46/EC), and the new regulation imposes a substantial increase in requirements, reflecting major technological changes over the last two decades and mounting concerns about the vulnerability of personal data.

While it's worth noting that fines for non-compliance among enterprises can reach up to 4% of an organization's annual worldwide turnover – an estimated $480 million for the average Dow Jones-listed company – it's also important not to allow fear and uncertainty to cloud the planning and decision-making surrounding GDPR. Internal disputes about

which controls are most practical, where to direct resources, and who will be held accountable for the design and management of the compliance program will only add to the complexity.

Incorporate diverse perspectives from key stakeholders

> Cooperation among business unit leadership is vital to the success of any effort to design and implement an effective compliance initiative.

In particular, legal, IT security, privacy and information governance functions must all be closely aligned as the process moves from the planning, scoping and design phases to implementation and ongoing management of the program. Compliance will need to encompass IT systems, staffing, policies and contracts, but organizations should avoid the trap of relying on IT expertise exclusively. It is imperative that creators of successful GDPR compliance programs incorporate viewpoints from key stakeholders across the organization.

Match solution design to your unique risk profile

Apart from fostering cooperation and collaboration among stakeholders and business units, how should companies be responding? A measured approach is probably best for most organizations. Understanding where your company's biggest GDPR risks lie is critical. Start by looking at situations where your company is collecting and/or processing personal data for consumers based in the EU. If your company's core business involves processing such information, your risk will be far greater than the risk for organizations engaged primarily in B2B transactions and not marketing products directly to consumers. If you establish protocols for recording processing activities as required by GDPR, you will be able to identify security and process gaps that will require remediation. Vendor-driven templates and methodologies, often accompanied by large teams of consultants, are likely overkill and may be poorly matched to the unique needs of individual organizations.

Few companies need massive, expensive, world-class solutions. Instead, develop a logical approach that is customized to your organization's unique risk profile. It is entirely possible (and eminently practical) for most organizations to distill GDPR compliance to a set of core, actionable components while leveraging existing data protection capabilities and management processes.

Prioritize core requirements

Let's take a look at new requirements and restrictions that should be priorities in most compliance programs. Under the new regulation, companies must:

- Identify and clearly **document any activities related to the processing of personal information** of EU data subjects. This must include establishing a lawful purpose for each processing activity.
- Ensure that you **provide adequate notice to data subjects at every point personal data is collected**, advising them of what data is being gathered and stating exactly how it is being processed.

- Be prepared to **respond to data subject access requests (DSARs)** and other assertions of rights by EU residents. GDPR imposes a 30-day time limit to respond to a request.
- **Develop a process for conducting privacy impact assessments** – a formal analysis of data protection and impacts on individual privacy rights – with the introduction of any new business process or system.
- **Safeguard personal data transferred outside the EU** via adequacy, consent, binding corporate rules or other contractual provisions.
- **Scrutinize access controls, encryption, pseudonymization and technical security measures** for protecting personal information under the company's control.
- **Notify an EU data protection authority within 72 hours** of a security incident that compromises personal information of an EU citizen.
- **Appoint a data protection officer** responsible for regular and systematic monitoring of data protection efforts, as well as for internal education and training and compliance audits. This person will also be responsible for communications between the company and GDPR Supervisory Authorities, as well as communications with data subjects. This requirement applies to any organizations that possess particularly sensitive data or that process and/or store large volumes of EU personal data, regardless of whether the subjects are employees or individuals outside the organization.

Understand the steps to developing a defensible plan

First of all, review the new regulations and make sure that your team of stakeholders is aligned on key definitions and interpretations.

Next, create a detailed map of your organization's data. You will need to have a thorough understanding of how all EU personal data flows through your systems, where it is stored and who has control over it. We recommend you document processing activities by using automated survey tools, but also by utilizing input from internal stakeholders. It's essential to account for any third-party vendors in this mapping exercise.

As you proceed, your team should rigorously review data retention policies for structured data sources like CRM systems, personnel records, marketing databases, etc. Many organizations keep far more personal data than is justified by the business value of doing so. Companies will also want to identify and document processing

activities using automated survey tools and formal input from stakeholders to identify EU personal data and map locations of protected data types.

As part of this process, be sure to identify any unstructured data sources like email. With regard to email, companies will want to take steps to make individual users aware of the risks associated with retaining and sharing the personal data of EU subjects, and the potential consequences for companies and individuals alike when that information is not rigorously protected. Many companies will want to consider encryption, pseudonymization and/or email monitoring to bolster security protocols.

After mapping, it's time to develop a comprehensive written plan.

+ We urge organizations to view GDPR compliance planning as an opportunity to thoroughly revisit the full range of their existing security controls with respect to personal data and identify gaps and weaknesses.

This includes scrutiny of functions like access controls, patching and vulnerability management. The plan must also account for incident detection and response capabilities. Also, don't forget to review vendor and other business contracts for GDPR compliance, and promptly negotiate new terms, including any necessary data processing agreements.

Note that new GDPR reporting requirements include a provision requiring organizations to provide regulators notification of a breach within 72 hours. If you don't already have a detailed plan for incident response, you will need to develop a defined process that spells out exactly how internal stakeholders will be notified and by whom, who will contact the regulator and how, and when and what to tell customers. Again, the details of these and other protocols are difficult to standardize across diverse organizations and will depend to a large extent on your company's unique risk profile.

To get a more comprehensive understanding of potential risks, many companies will find it useful to conduct a Privacy Impact Assessment (PIA). This is a formal process to evaluate an organization's ability to meet legal, regulatory and policy requirements for privacy, identify and assess potential risks related to personal data, and propose specific measures to manage those risks. Hiring a Certified Privacy Professional to review existing documentation and recommend new or additional policies may also expedite the planning process.

Compliance also requires that you create a process for responding to requests from EU data subjects to access, modify or delete their personal information. For many organizations, it might make sense to fulfill this obligation through use of a qualified third party rather than imposing an additional burden on internal staff.

Finally, a critical and often neglected component of an effective compliance program is employee education and training.

+ You must ensure employees have a clear understanding of the company's obligations and risks with respect to GDPR regulations.

Conduct executive briefings throughout the planning process. Develop and implement a privacy training program that is tailored to your information and security systems, your risk profile and your company culture. And make sure everyone participates.

August 27th - 31st @ Intercontinental Singapore

https://gsec.hitb.org/sg2018/

HITBGSEC2018 - SINGAPORE

Vote for the talks you want to see and speakers you want to meet

Voting is now open! You decide who speaks!

https://gsec.hitb.org/vote/

HITBSecConf2018 - BEIJING

Organized in collaboration with JD Security

The First HITB Security Conference in China

REGISTRATION OPENS JUNE 2018

https://conference.hitb.org/hitbsecconf2018pek/

October 29th - November 2nd @ Kempinski Beijing

2 & 3-day Hands-on Technical Trainings
Triple Track Conference with HITB Labs
CommSec Village / Exhibition
HITB CommSec Track
HITB Capture the Flag