

## REDEFINING SECURITY VISUALIZATION WITH HOLLYWOOD UI DESIGN



**TOKENIZATION / THREAT INTELLIGENCE**  
**VULNERABILITY DISCLOSURE / DDOS**  
**INTERNET OF THINGS / HUMAN ERROR**

  
**black hat®**

**BEST PRACTICES FOR ENSURING COMPLIANCE  
IN THE AGE OF CLOUD COMPUTING**



Join us for the Fifth Annual

(ISC)<sup>2</sup>



2015

Sept. 28 - Oct. 1 • **Anaheim, CA** • Anaheim Convention Center

# REGISTER TODAY

**MEMBERS SAVE \$355**

**EARN UP TO 62 CPEs!**

## Sessions include:

- » The Anatomy of a Cloud Data Breach
- » Security from the Trenches – Scrying Security
- » Status of the Industry: 2015 Global Information Security Workforce Study
- » Passive Information Leakage: A New Threat to Sensitive Business Information

View the [full list of sessions](#) at (ISC)<sup>2</sup> Security Congress 2015.

## Tracks include:

- » Cloud Security
- » Swiss Army Knife
- » Mobile Devices – Security & Management
- » Governance, Regulation & Compliance
- » Software Assurance & Application Security
- » Malware
- » Threats – Management, Detection, Intelligence & Mitigation
- » Professional Development
- » Forensics
- » Healthcare Security
- » People Centric Security

**REGISTER TODAY**

[congress.isc2.org](http://congress.isc2.org)

Colocated with





# TABLE OF CONTENTS

Page 05 - **Security world**

Page 11 - Redefining security visualization with Hollywood UI design

Page 15 - Best practices for ensuring compliance in the age of  
cloud computing

Page 18 - The evolution of DDoS and how ISPs can respond

Page 22 - NowSecure Lab cloud: Mobile app assessment environment

Page 26 - Why vulnerability disclosure shouldn't be a marketing tool

Page 29 - **Malware world**

Page 33 - Report: Black Hat USA 2015

Page 43 - We don't know what we don't know

Page 45 - Outdated protocols put IoT revolution at risk

Page 50 - The challenges of implementing tokenization in a  
medium-sized enterprise

Page 54 - Automated threat management: No signature required

Page 58 - **Events around the world**

Page 60 - Re-thinking security to detect active data breaches

Page 66 - How to prevent insider threats in your organization

Page 70 - ISO/IEC 27001 scoping and beyond

Page 74 - Combatting human error in cybersecurity

Page 78 - Threat intelligence matters to everyone



# (IN)SECURE Magazine 47

## CONTRIBUTORS LIST



- **Florian Eichelberger**, Information Systems Auditor at Cognosec
- **Gonen Fink**, CEO at LightCyber
- **Brian Honan**, CEO at BH Consulting
- **Eric D. Knapp**, expert in industrial control systems cyber security
- **Rupesh Kumar**, Director of Lepide Software
- **Dave Larson**, CTO at Corero Network Security
- **Ulf Mattsson**, CTO at Protegrity
- **Eddie Mitchell**, Principal Solutions Architect at CSG Invotas
- **Gavin Reid**, Vice President of Threat Intelligence at Lancope
- **Oliver Tavakoli**, is the CTO at Vectra Networks.

Visit the magazine website at [www.insecuremag.com](http://www.insecuremag.com)

### (IN)SECURE Magazine contacts

Feedback and contributions: **Mirko Zorz**, Editor in Chief - [mzorz@net-security.org](mailto:mzorz@net-security.org)

News: **Zeljka Zorz**, Managing Editor - [zzorz@net-security.org](mailto:zzorz@net-security.org)

Marketing: **Berislav Kucan**, Director of Operations - [bkucan@net-security.org](mailto:bkucan@net-security.org)

### Distribution

(IN)SECURE Magazine can be freely distributed in the form of the original, non-modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without the explicit permission from the editor.





Security  
world

### **Hacker had access to sensitive info about Firefox bugs for over a year**

An attacker managed to access security-sensitive information about a considerable number of (at the time) unpatched Firefox vulnerabilities, and there is evidence that at least one of them has been exploited in attacks in the wild.

The breach didn't happen because there is a critical vulnerability in Mozilla's Bugzilla web-based bugtracker, but because the attacker managed to get hold of a privileged users' account password, as the user re-used it on another website that has been breached.

"The earliest confirmed instance of unauthorized access dates to September 2014. There are some indications that the attacker may have had access since September 2013," Mozilla explained in a FAQ.

The attacker accessed 185 nonpublic bugs. Of these, 53 were severe vulnerabilities, and "43 had already been fixed in the released version of Firefox at the time the attacker found out about them."

Of the remaining 10, 2 were fixed less than 7 days after the attacker accessed information about them, 5 were fixed in a period between 7 and 36 days, and the remaining 3 were fixed 131, 157 and 335 days after, respectively.

"It is technically possible that any of these bugs could have been used to attack Firefox users in the vulnerability window. One of the bugs open less than 36 days was used for an attack using a vulnerability that was patched on August 6, 2015," Mozilla noted. "Other than that attack, however, we do not have any data indicating that other bugs were exploited."

Of course, attacks exploiting some of those other bugs could have been so limited that they were never noticed by users or flagged by security researchers.

The good news is that the breach forced Firefox to get a move on fixing those remaining issues, and they did so with Firefox 40.0.3, which was released on August 27. Users who haven't yet updated to this version would do well to do it now.



## An emerging global threat: BEC scams hitting more and more businesses

As more and more victims come forward, and the losses sustained by firms in the US and around the world passed the billion dollar mark, the FBI is once again warning businesses about Business Email Compromise (BEC) scams.

The BEC is a sophisticated scam performed by members of organized crime groups from Africa, Eastern Europe, and the Middle East. They usually target businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.

The scammers impersonate a supplier, a high-level executive with the firm, or a firm's employee by hacking or spoofing their email accounts. From those accounts, they send requests to the firm's employee(s) in charge of making payments to wire a payment to a bank account belonging to the scammers, usually set up with a Chinese bank.

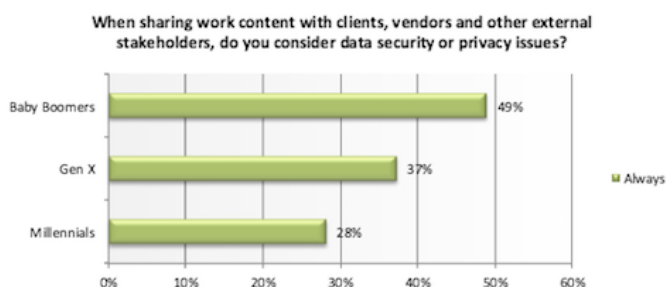
"They know how to perpetuate the scam without raising suspicions," FBI Special Agent Maxwell Marker pointed out. "They have excellent tradecraft, and they do their homework. They use language specific to the com-

pany they are targeting, along with dollar amounts that lend legitimacy to the fraud. The days of these e-mails having horrible grammar and being easily identified are largely behind us."

More often than not, the scammers also manage to infiltrate the company's networks via malware that they have tricked employees into downloading and running. This allows them access to information that they can misuse to make the fraudulent wire transfer requests seem legitimate.

"According to IC3, since the beginning of 2015 there has been a 270 percent increase in identified BEC victims. Victim companies have come from all 50 U.S. states and nearly 80 countries abroad," the FBI shared.

In the meantime, businesses would do well to acquaint themselves with the BEC threat and take measures to avoid becoming victims, such as verifying changes in vendor payment location and confirming requests for transfer of funds, refraining from posting financial and personnel information to social media and company websites, using two-step verification for confirming significant transactions, and more.



## What drives employees to shadow IT?

While 94 percent of knowledge workers recognize the importance of collaboration and 83 percent use technology to collaborate, 59 percent are not satisfied with the tools they are given in their workplace. This is particularly true among millennials and is causing them to knowingly turn to unapproved consumer-grade tools with little concern about the security risks involved, according to Alfresco Software.

- Seventy-one percent of millennials face challenges with company-issued collaboration tools, compared with 45 percent of baby boomers.
- Forty-seven percent of millennials prefer chat and text tools for collaboration, while 36 percent of baby boomers find these least effective.
- Forty-seven percent of millennials favor online meetings to in-person, while only 26 percent of baby boomers would prefer online to in-person meetings.



## Sound-Proof: Two-factor authentication without user interaction

A group of researchers from the Swiss Federal Institute of Technology in Zurich have recently presented at the USENIX security conference their two-factor solution that relies on ambient sound. Dubbed Sound-Proof, the solution does not require interaction between the user and his phone, and works even if the phone is in the user's pocket or purse, and both indoors and outdoors.

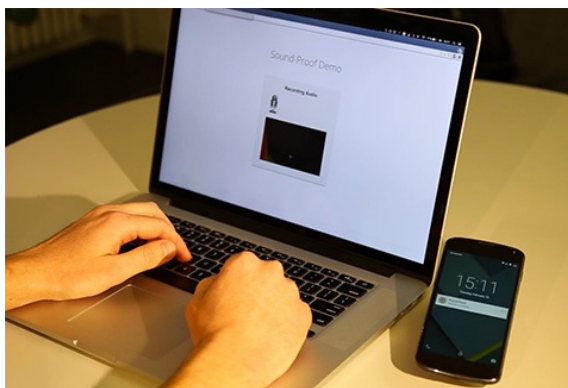
The system works like this: when the user enters his username and password into a website that offers Sound-Proof 2FA, the website switches on the computer's microphone and starts recording. At the same time, it pings the Sound-Proof app which does the same. The two recordings are then turned into digital signatures, sent to a central server, and compared. If they are the same, the authentication

process is completed. If they are not, the app be made to fall back to other types of 2FA or 2SV options.

The researchers built an app for Android and iOS, and the solutions works with any HTML5-compliant browser that implements the WebRTC API (Chrome, Firefox and Opera for now, and IE very soon).

"Since audio recording and comparison is transparent to the user, he has no means to detect an ongoing attack. To mitigate this, at each login attempt the phone may vibrate, light up, or display a message to notify the user that a login attempt is taking place," they noted.

Sound-Proof can also be used for continuous authentication, although privacy implications have to be taken into consideration in that case.



## Addressing IoT risks with a trust framework

The Online Trust Alliance (OTA) released its Internet of Things Trust Framework, which presents guidelines for IoT manufacturers, developers and retailers to follow when designing, creating, adapting and marketing connected devices in two key categories: home automation and consumer health and fitness wearables.

"The rapid growth of the Internet of Things has accelerated the release of connected products, yet important capability gaps in privacy and security design remain as these devices become more and more a part of everyday life," said Craig Spiegle, Executive Director and President of OTA. "For example with a fitness tracker does the user know who may

be collecting and sharing their data? When you purchase a smart home what is the long-term support strategy of patching devices after the warranty has expired? How do manufacturers protect against intrusions into smart TV's and theft of data collected from device cameras and microphones? What is the collective impact on the smart grid or our first responders should large numbers of these devices be compromised at once?"

Without addressing sustainability, devices that may have been secure off the shelf will become more susceptible to hacking over time. This could lead to hackers remotely opening garage doors and turning on baby monitors that are no longer patched to infiltrating fitness wearables to spy on health vitals, or creating mayhem by sabotaging connected appliances.



## Researchers get \$100k for detecting emerging class of C++ bugs

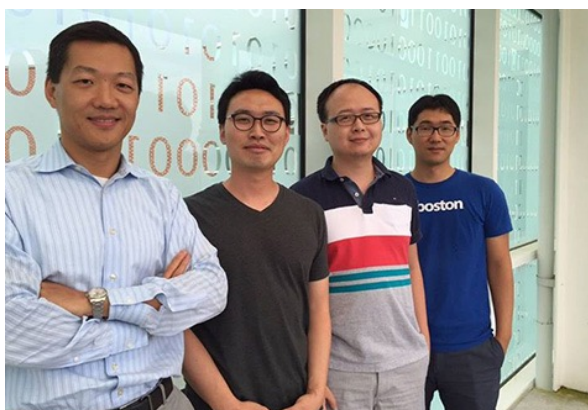
Facebook has awarded \$100,000 to a team of researchers from Georgia Tech for their discovery of a new method for identifying "bad-casting" vulnerabilities that affect programs written in C++.

"Type casting, which converts one type of an object to another, plays an essential role in enabling polymorphism in C++ because it allows a program to utilize certain general or specific implementations in the class hierarchies. However, if not correctly used, it may return unsafe and incorrectly casted values, leading to so-called bad-casting or type-con-

fusion vulnerabilities," the researchers explained in their paper.

"Since a bad-casted pointer violates a programmer's intended pointer semantics and enables an attacker to corrupt memory, bad-casting has critical security implications similar to those of other memory corruption vulnerabilities."

They have created CAVER, a runtime bad-casting detection tool, and have successfully used it to test software such as Chrome and Firefox. The result? They found eleven previously unknown security vulnerabilities, which have already been fixed.



Georgia Tech researchers.

## How to sabotage DDoS-for-hire services?

A simple move like making PayPal seize the accounts through which the people offering booter (or stresser) services get paid can make business much more difficult for them and, in some cases, can result in some of them going out of business. Another thing that could help decimate these services is if CloudFlare would stop providing them with protection against DDoS attacks.

"All 15 booters in our study use CloudFlare's DDoS protection services to cloak the ISP hosting their frontend servers and to protect them from abuse complaints and DDoS attacks," a group of researchers that analyzed the booter market pointed out.

Among the other things that they discovered are that:

- A large amount of DDoS attacks are being launched by relatively unsophisticated attackers that have purchased subscriptions to low-cost DDoS-for-hire services
- Customers of booter services prefer paying via PayPal and are not that fond of Bitcoin
- Some operators of booter services prefer renting high-bandwidth Virtual Private Servers for attacks rather than to rely on botnets
- According to geolocation information provided by PayPal, over 44% of the customer and merchant PayPal accounts associated with booters are likely owned by US-based individuals
- Booter services offer different kinds of attacks, but amplified volume-based attacks is the preferred one.



## **81% of healthcare organizations have been compromised**

Eighty-one percent of health care executives say that their organizations have been compromised by at least one malware, botnet, or other cyber-attack during the past two years, and only half feel that they are adequately prepared in preventing attacks, according to KPMG.

Furthermore, in polling 223 chief information officers, chief technology officers, chief security officers and chief compliance officers at health care providers and health plans, KPMG found the number of attacks increasing, with 13 percent saying they are targeted by external hack attempts about once a day and another 12 percent seeing about two or more attacks per week.

More concerning, 16 percent of healthcare organizations said they cannot detect in real-time if their systems are compromised.

When asked about readiness in the face of a cyber-attack, 66 percent of execs at health plans said they were prepared, while only 53 percent of providers said they were ready. Larger organizations, in terms of revenue, are better prepared than smaller ones.

Malware, software designed to disrupt or gain access to private computer systems, is the most frequently reported line of attack during the past 12 to 24 months, according to 65 percent of survey respondents. Botnet attacks, where computers are hijacked to issue spam or attack other systems, and "internal" attack vectors, such as employees compromising security, were cited by 26 percent of respondents.

The areas with the greatest vulnerabilities within an organization include external attackers (65 percent), sharing data with third parties (48 percent), employee breaches (35 percent), wireless computing (35 percent) and inadequate firewalls (27 percent).

## **Security flaws could allow attackers to steal over 100 different cars**

Since 2012, a trio of European researchers knew that the Megamos Crypto transponder - used in a over 100 cars manufactured by Audi, Ferrari, Fiat, Cadillac, Volkswagen and two dozen more automakers around the world - sports vulnerabilities that can be exploited by attackers to start the cars without needing to have the key (i.e. the passive RFID tag embedded in it).

They managed to reverse-engineer all proprietary security mechanisms of the transponder, including the cipher and the authentication protocol, and have devised three practical attacks that allowed them to recover the 96-bit transponder secret key. One of these attacks allowed them to recover the key and start the engine with a transponder emulating device in just half an hour. And another is very hard to mitigate if the attacker has access to both the car and the transponder for a period of time (e.g., car rental, valet parking).

"It is also possible to foresee a setup with two perpetrators, one interacting with the car and

one wirelessly pickpocketing the car key from the victims pocket," they noted. "Our attacks require close range wireless communication with both the immobilizer unit and the transponder."

So, how come we're hearing about this problem only now? Well, when the researchers first tried to present their findings at the 22nd USENIX Security Symposium in 2013, they were prevented from doing so by Volkswagen, who took them to court and won an injunction by the UK High Court of Justice prohibiting them from publishing key sections of the paper. Two years later, the injunction was lifted, and they finally had the opportunity to present their work on the at the 24th USENIX Security Symposium held in August in Austin, Texas.

"Although two years have passed, this work remains important and relevant to our community," Sam King, USENIX Security '13 Program Chair, and Casey Henderson, USENIX Executive Director, noted in a foreword added to the paper, which has been amended to omit a crucial sentence that could help non-technical attackers work out how to execute the attacks.



# **Know More. Risk Less.**

## **LOOKINGGLASS Dynamic Threat Defense**

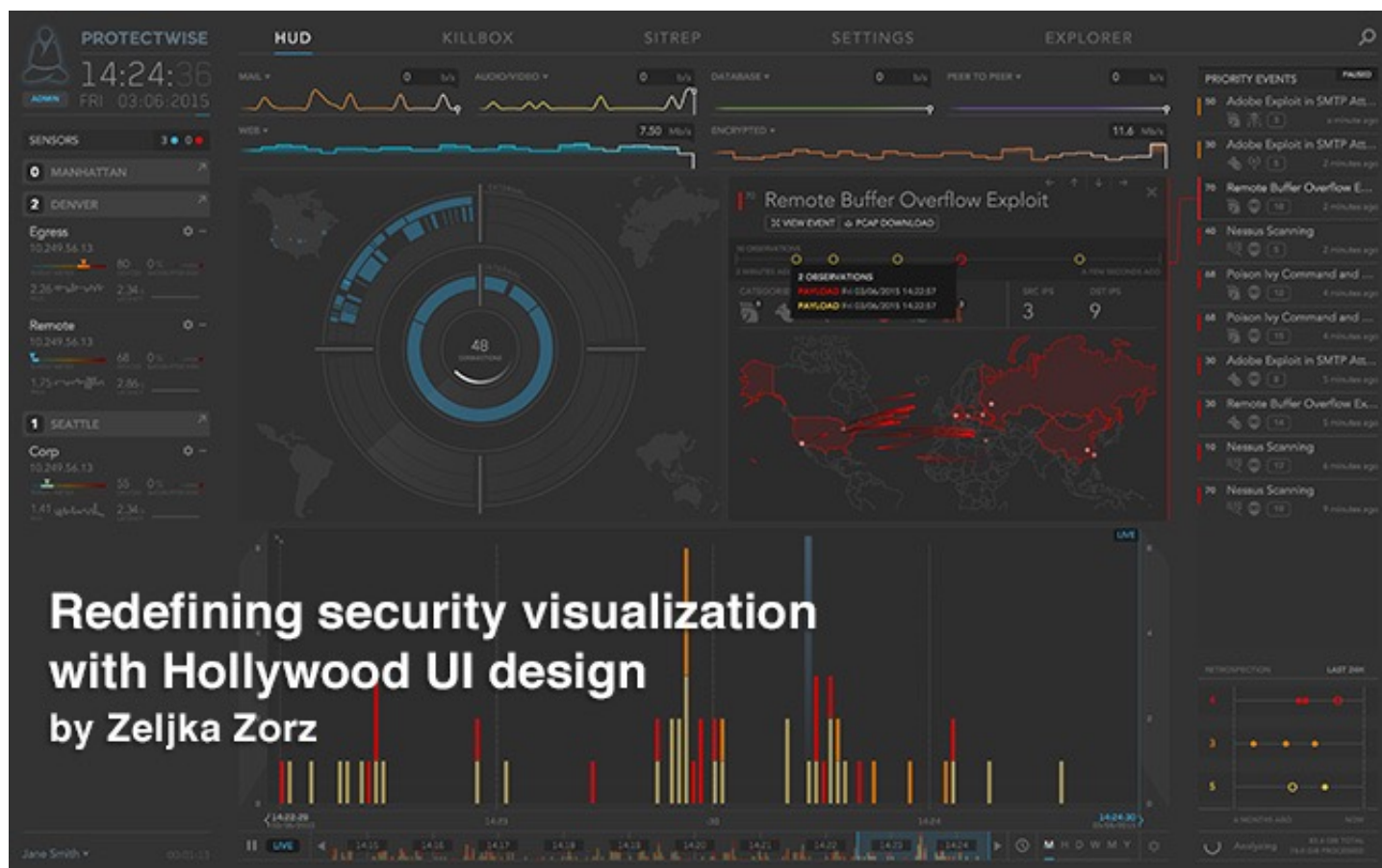
**LOOKINGGLASS delivers rich visibility and advanced mitigation techniques for cyberthreats impacting your organization, your partners, your industry, and your world.**



**LOOKINGGLASS**

[www.lgscout.com](http://www.lgscout.com)





Most security interfaces today leave a lot to be desired, and many security pros are gaming enthusiasts, accustomed to a sharp and engaging virtual world. Protect-Wise CEO Scott Chasin and CTO Gene Stevens wanted to give them a helpful security tool with an interactive visual dashboard that looks straight out of Call of Duty.

The company, founded in April 2013, recently came out with Cloud Network DVR, a virtual camera in the cloud that records everything on an organization's network. It allows security pros to discover threats in real time, and check out recorded historical data to uncover threats that were previously unknown using the latest intelligence.

The solution has a Wisdom Engine, which analyses all this network traffic data by dissecting netflow using deep-packet inspection, identifying and classifying threat events, and correlating the findings with threat intelligence from third-party sources.

But the thing that will delight most those who use it is the user interface.

"We wanted to give security professionals full visibility into their network and a way to quickly recognize patterns and interact with massive data sets. We wanted to create something that security professionals, incident responders

and network operations teams would want to interact with," Chasin explained.

The UI is called ProtectWise Visualizer, and its creator is Jake Sargeant, FX pro and a visual designer at MN8 Studio. If his name sounds familiar, it's because he was the Lead Animated Graphics Artist for the movie TRON: Legacy.

"My cofounder, Gene Stevens and I initially approached Jake because we are huge fans of his work on the movies TRON: Legacy, and Oblivion (starring Tom Cruise)," says Chasin. "I love the movies' concept of total immersion into a data landscape. The idea of the grid coupled with CGI and how the characters visualize data in these movies is very compelling and inspiring. This is the concept we were going for with the visualization of massive sets of network data, and Jake completely understood our desire to provide a UI that allows for immersion in data."

They met with Jake and explained what types of data they wanted to visualize - network connections, an attack spiral, a timeline, a priority view of security events.

"We'd discuss how to provide situational awareness in a beautiful interface that offers both an at-a-glance view of data at scale in a way that is actionable, so a user can quickly get a pulse on overall network health and pivot into a deep dive on a specific security event," he notes.

"We really like the idea of interfaces that give you a lot of data and enable quick pattern recognition - like the Ironman suit. Ironman didn't have to read every piece of data, he was just able to observe it, quickly recognize patterns and act on the information," he explained. "Together we'd iterate on the designs."

Sargeant saw that there was a massive amount of real data to visualize, and accepted the challenge of creating an interface that's

intuitive, structured and not visually overwhelming.

Computer GUIs found in movies are notorious for favoring interesting visuals at the expense of usability.

"On a real product like ProtectWise, it was a much more detailed process of understanding and then interpreting the data visually. It was a welcome challenge and contrast to sci-fi interfaces where I had to think about someone using this product on a daily basis," Sargeant notes.

"I'd say the most significant challenges working on the interface were the two main circular visualizations on the Heads-Up Display (HUD) that feature front and center in the interface - network connection monitoring graph (to the left) and the attack spiral (to the right). I spent the most time with Scott and team working on these two sections and am really happy with how they implemented it in code for web browsers."



His toolset for creating the visuals were Adobe Photoshop, Illustrator and AfterEffects. He used Basecamp for project management, and the Internet for "a ton" of data visualization research.

"Today, we have a team of in-house UI designers that continue to implement Jake's creative direction on the Visualizer," shares Chasin.



"We are still working with Jake to push the envelope in terms of what an effective network security user interface should look like and I'm excited about some of the new capabilities we're working on. It's exciting stuff and an area where we are committed to deliver continued innovation."

The solution's beta testing phase begun in early 2014 and officially ended in April 2015. Fifteen companies of varying sizes and across different industry verticals, including media and entertainment, technology, financial services, and healthcare, participated.

"One of the unexpected, key learnings that came out of our early access program was how valuable the pervasive visibility our UI provided not only to security analysts and incident responders - users we'd targeted from the outset - but the value it provided for network operations teams. For many on the network operations side of the house, this was the first time they had complete visibility into

what was happening on their network," he pointed out, adding that they suggest to customers to leave on the default full packet capture setting for a few days after initial deployment (before going in a policy-configuring the sensor) just to get a sense of the types of traffic on their network.

"I think until now it's largely been a very pragmatic, bare-bones approach to visualization for security products. Most of the UI design in network security products is sorely lacking in imagination and they do not provide the level of visibility security professionals require. Honestly, a lot of the UIs are more reminiscent of the interfaces to set up a router than to detect and respond to advanced threats," he noted.

"In a day and age where an increasing number of the workforce, particularly the IT workforce, is raised on the powerful visualizations found in gaming, they expect this type of visualization in advanced technology services."

---

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine and Help Net Security ([www.net-security.org](http://www.net-security.org)).



# THE NEXT GENERATION CLOUD SECURITY PLATFORM



Bringing Continuous Security to the Global Enterprise

Get a free trial at [qualys.com/trial](https://qualys.com/trial)



# Best practices for ensuring compliance in the age of cloud computing

by Amrit Williams



When was the last time you heard someone utter the sentence, “I’m looking forward to the audit next week.” Most likely, never. Since its invention, the word “audit” has elicited ... well, if not terror, then certainly groans in the individuals responsible for ensuring the resources being audited are compliant with appropriate regulations. The fact is that compliance is still largely a manual set of processes, even though the regulatory landscape is continually more complex. Finding and hiring enough qualified compliance people is difficult and, ultimately, doesn’t scale well.

Complicating things further is the move to elastic infrastructure like public and private clouds. Ensuring compliance with necessary regulations like PCI, HIPAA, SOC 2, SOX, etc. in the era of on-premise, captive data centers was challenging enough. But as organizations move to cloud-based and/or virtualized infrastructure, the job becomes nearly impossible. While the cost and agility benefits of cloud computing are simply too significant to ignore, for the compliance teams this creates special challenges, many of which have yet to be considered by the majority of enterprises.

The good news is that help is on the way. Let’s outline the major considerations organi-

zations should incorporate into their compliance programs, as well as some pitfalls that can be avoided to ensure businesses can realize the benefits of cloud computing and still maintain compliance with appropriate regulations.

## **Make security the first goal**

Many companies faced with compliance issues fall into a very common trap, often referred to as the “compliance = security” mindset. This thinking concludes that if a company goes to the trouble to be compliant (this means compliant to any number of regulations – HIPAA, PCI, etc.), then it will be effectively

“secure.” Unfortunately, nothing could be further from the truth. Witness some of the major retail security breaches of this year – most of those organizations were PCI compliant! As with many kinds of regulations, compliance really represents the absolute least amount of effort required.

That’s not to say that compliance isn’t important – it is. And even with the best of efforts, 100 percent security is never guaranteed. But if companies with cloud infrastructure want to give themselves the best chance to avoid the very severe consequences that come with a major breach, they need to focus on security first, and then on ensuring compliance.

### **Maintaining visibility in a world of multiple cloud models**

The first place to start with any security or compliance initiative is visibility. You can’t se-

cure what you can’t see. This means having 100 percent visibility into all technology assets and services: where all of your digital assets are located, as well as their status. Know what you’ve got and what it’s doing at all times.

This sounds incredibly basic, but given the automated, elastic, on-demand nature of modern virtual infrastructure, visibility can be a challenge. Compound that by firms using multiple public and hybrid cloud models, and you can begin to see the complexity involved in maintaining transparency and visibility for all of your organization’s digital assets.

Once you understand what’s going on with your infrastructure, applications, data and users, you can begin to understand how to minimize your attack surface and better prevent and mitigate attacks. This often requires great relationships with your cloud service providers, which brings us to our next point.

# Given the automated, elastic, on-demand nature of modern virtual infrastructure, visibility can be a challenge.

### **In the cloud, compliance is a shared responsibility**

If you’re going to be using cloud services of any kind, you will want to develop a great compliance and governance relationship with your service provider. Often times, organizations believe they are compliant if their service provider is compliant – that’s simply not the case. Nor is the reverse true.

Public cloud service providers have established a shared responsibility model for security and compliance. Typically, this means that the service provider is responsible for physical

security and access controls to the infrastructure at the hypervisor layer, while clients are responsible for securing everything else, including all assets running on the server instances (applications, web servers, databases, etc.).

This means that clients must monitor and log all appropriate compliance-related data for this infrastructure. Get familiar with the details of your service provider’s shared responsibility model and understand how it fits into your compliance model. The good news is that most cloud providers are paying more attention to the compliance needs of their clients.



## Automate or die!

Manual processes are killing compliance teams, who are typically understaffed and overworked. Sure, you can hire more people, if you have the budget and can find enough qualified candidates, but this approach won't scale.

With the dynamic nature of elastic infrastructure, where workloads and servers can be provisioned and decommissioned in minutes (often without notice or with the knowledge of the GRC team), the compliance workload is only going to get bigger, not smaller.

Unfortunately, compliance teams are trapped using manual processes, which can be a major obstacle to business agility. But until now, there's been no alternative as the consequences of being out of compliance are severe – fines, lawsuits, shutdown of operation and loss of customers.

The question then turns to “How do I ensure compliance while still maintaining real-time, agile work flows?” Luckily, there is an emerging set of compliance automation solutions on the market today that take much of the manual process out of the equation. These solutions work in any cloud infrastructure, are focused at the workload itself and capable of ensuring compliance with hands-free, automated data collection, organization and analysis.

Many of these solutions also enable security to be baked into a DevOps continuous delivery approach, ensuring that new workloads are protected from the start, empowering security teams to move at DevOps speed. By automating compliance at the individual workload, companies can alleviate much of the manual burden on compliance teams while retaining the business agility that drove them to cloud infrastructure in the first place.

# Compliance teams are trapped using manual processes, which can be a major obstacle to business agility.

## Compliance in motion

Ok, so you passed the audit, now what? For most organizations, the job of preparing for the next audit starts when the previous one ends, again, with lots of manual effort. However, when properly integrated with security automation solutions and DevOps methods, compliance teams can now break this pattern by adopting a strategy of compliance in motion.

This means that compliance can now become a continuous process that never sleeps; your

systems (especially the elastic ones that come and go on a dime) are constantly monitored, secured and all relevant activity logged in near real time. Preparing for an audit becomes much easier and your compliance team can now focus on anomalies and remediation.

Compliance and risk teams that adopt these best practices will go a long way towards helping the business realize the benefits of cloud computing models, while at the same time ensuring critical compliance objectives are met in a modern, automated, continuous cycle.



## The evolution of DDoS and how ISPs can respond

by Dave Larson

Today's DDoS attacks are almost unrecognizable from the simple volumetric attacks of old. They are far more sophisticated, deceptive and frequent. As the attacks evolve, so must the response. This article will examine the best approaches for mitigating the risk and outline how ISPs and carriers are uniquely positioned to protect businesses from DDoS attacks right at the internet edge.

In the early days of DDoS attacks (c. 2000), DDoS mitigation technology utilized in the Service Provider industry focused on the ability to determine that a DDoS attack was occurring, simply by sampling edge routers and interrogating NetFlow records from those routers. As a result, an operator could see the increase in DDoS traffic but they had few if any defenses at their disposal to block the attacks.

Without any true solutions available or in place, a network operator would first interpret that an attack was in progress, then manually inject a null-route – sometimes referred to as a black-hole route - into the routers at the edge of the service provider's network, and block the attack. This null-route effectively blocked all attack traffic headed toward the intended victim.

However, this approach had negative connotations as well. Null-route injections also blocked all good traffic along with the bad.

The target victim was taken completely offline by the null route and this actually perfected the attack by dropping all packets destined to the victim's IP addresses. This approach provided a way of at least blunting the flow of the attack and served as a tool to eliminate the collateral damage to other customers or infrastructure as a result of the DDoS attack.

Fast forward several years and we find improvements to DDoS mitigation, and an evolution in protection techniques available to operators. It became clear that a null-route was not an approach that operators preferred to use. Instead of injecting a null-route when an operator observes a large spike, they were now able to inject a new route instead.



By implementing a new route, operators could now gain the ability to redirect all traffic through an appliance or bank of appliances that inspected traffic and attempted to remove the DDoS attack traffic from the good user flows. This approach spawned the existence of DDoS scrubbing-centers and DDoS scrubbing-lanes that are commonly deployed today.

This DDoS scrubbing approach, while a significant improvement, still required a considerable amount of human intervention. A DDoS attack would have to be detected (again by analyzing NetFlow records) then an operator would have to determine the victim's destination IP address(es). Once the victim was identified, a BGP route update would take place to inject a new route to redirect or "swing" the victim's incoming traffic to a scrubbing lane. The appliances in the scrubbing lane would attempt to remove the DDoS traffic from the good traffic and forward it to the downstream customer.

In order to forward the good traffic back to the original destination, in most cases an operator would also have to create a GRE tunnel from the scrubbing lane back to the customer's border router. This approach represents a significant improvement over null-route solutions but it also introduces significant complexity to the carrier network topology and requires dedicated and costly security personnel in order to ensure proper execution.

Recently, the complexity of the DDoS challenge has been evolving and attacks have been increasing in size, sophistication and frequency. Additionally, as large network operators have succeeded and grown, the sheer size and scale of their infrastructures and their massive customer base presents an incredibly attractive attack surface due to the multiple entry points and significant aggregate bandwidth that acts as a conduit for damaging and disruptive DDoS attacks.

The combination of these trends is now driving the need for an even more sophisticated approach to DDoS mitigation that utilizes purpose-built technology to enable a better economic model for defeating these attacks and creating new revenue streams around clean-pipe services.

As we approach the modern day DDoS threat, with advanced mitigation techniques that have evolved over the last decade, innovative protection, sophisticated visibility and scalable deployment options are emerging.

In-line deployments of mitigation technology at the Internet or transit and peering points offer much needed relief from the frequent and damaging attacks that providers are dealing with on a regular basis. Alternatively, many providers prefer a scrubbing-lane approach, but require enhanced visibility into the traffic patterns as well as the ability to scale the scrubbing operation for increased bandwidth.

### **DDoS mitigation approaches and real-time threat responses**

The weaknesses of old methods - being slow to react, expensive to maintain and unable to keep up with shifting and progressive threats – tell us that solutions appropriate for today need to be always-on and instantly reactive. It's clear they also need to be adaptable and scalable so that defenses can be quickly and affordably updated to respond to the future faces of DDoS threats – whatever those may be.

The increasingly popular method of fulfilling these aims is dynamic, in-line DDoS mitigation bandwidth licensing. With this technique, an in-line DDoS mitigation engine is employed but the operator pays for only the bandwidth of attacks actually mitigated. The benefit of this approach is that it delivers full edge protection for locations in the network that are most affected by DDoS, at a fraction of the cost of traditional scrubbing centre solutions.

The desirability of these tools is due to the fact that they can be constantly on, with no need for human intervention, and they provide non-stop threat visibility and network forensics.

Another aspect of effective DDoS mitigation is security event reporting. One of the Achilles heels of traditional DDoS scrubbing centre solutions is that they rely on coarse sampling of flows at the edge of the network to determine an attack is taking place. DDoS attackers are well aware of the shortcomings of this approach and have modified many of their

techniques to ride under the radar, below the detection threshold, in order to evade ever being redirected to a scrubbing centre. Your security posture will only be as good as your ability to visualize the security events in your environment, and a solution that relies on coarse sampling will be unable to even detect - let alone act on - the vast majority of the modern DDoS attack landscape. A robust modern DDoS solution will provide both instantaneous visibility into DDoS events as well as long-term trend analysis to identify adaptations in the DDoS landscape and deliver corresponding proactive detection and mitigation techniques.

Real-time responses are possible with new software and hardware thanks to the fact DDoS attacks generally have a bell-shaped barrage of traffic. This is to throw off sample-based anomaly detectors – however, it plays into the hands of DDoS mitigation solutions that utilize modern data analytics platforms that are optimized for detecting that a DDoS attack is underway before the system has reached a critical threshold.

In short, there's no reason that companies should resign themselves to eventually getting "DDoSed". The technology exists to provide an effective defense, and even if not all organizations can afford this, there is a common partner who can - Internet Service Providers.

### **The opportunity for ISPs, carriers and service providers**

As ISPs become more aware of the DDoS threat and how to deal with it, pressure mounts on them to maintain their credibility by protecting customers from DDoS attacks. After all, if a provider propagates an attack that results in the loss of a customers' data or their site being effectively shut down, this harms the service provider's reputation and potentially their revenue.

This creates a golden opportunity for service providers to take the initiative and modernize DDoS protection for their customers. If they are able to offer dynamic mitigation bandwidth licensing to their customers, a new revenue stream is open to them. Service providers can offer the use of internet scalable engines that

are operating in tandem with the network, with customers being highly incentivized to buy-in due to the efficiency, savings and protection on offer.

Carriers can also benefit from improved DDoS protection, allowing them to lose the static scrubbing centers and instead enact a better-performing system that is automated and distributed. The saving in work hours and ability to localise DDoS mitigation will allow them to scale up their protection at a fraction of the cost.

The "New IP" is widely regarded as the next big thing for carrier networks. The shift from fixed infrastructure to the free flowing distributed networks is allowing organizations to leverage improvements such as Software Defined Networking and virtualization. These advancements have the potential to improve services offered and broaden revenue opportunities, but they also complicate security options.

In addition, a hardened DDoS defense is the first step a carrier must consider before rolling out Network Functions Virtualization (NFV) services. Commercial and open-source hypervisor technology is enabling the new NFV economic model to emerge, but this same technology is tremendously susceptible to DDoS. A hardened edge with respect to DDoS will be essential to ensure that this new service model is not compromised by DDoS attacks.

ISPs can also extend their DDoS protection and offer it to customers as a service, charging a premium for "smart pipes" that have been cleaned of bad traffic. A chance to change the shape of the market in light of the altered DDoS landscape emerges – as businesses will eagerly sign up a cost effective and scalable solution for protection if service providers can take care of it for them, thus saving their company from having to organize its own protection in that area. ISPs and carriers therefore have both a responsibility and an opportunity to offer smart pipes, enhance user experience and improve protection across their infrastructure.





# Trusted Identities | Secure Transactions<sup>TM</sup>

For Citizens, Consumers & Enterprises

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. They also expect the ecosystems that allow this freedom and flexibility to be entirely reliable and secure. Entrust Datacard offers the trusted identity and secure transaction technologies that make these ecosystems possible.

To learn more, visit [entrustdatacard.com](http://entrustdatacard.com)





## NowSecure Lab cloud: Mobile app assessment environment by Berislav Kucan

NowSecure was one of the companies that caught my attention at this year's RSA Conference in San Francisco. While it initially seemed like a new player in the field, the company was actually started back in 2009 under the name viaForensics.

Last December, they decided to ditch the forensics-focused name and rebrand themselves as NowSecure. Around the same time, the company raised \$12.5 million in a Series A round and started working heavily on their line of security assessment products.

NowSecure Lab is mobile app security assessment environment that comes in two versions - as a standalone, on-premise solution, and a "lighter" cloud offering. The on-premise solution runs as a VM instance of Santoku Linux and requires an Apple Macbook Pro. This workstation version of NowSecure Lab includes both static and dynamic analysis, as well as the ability to customize the testing environment for specific applications that need to be assessed.

The cloud version I've been using for a couple of months is now in open beta and you can see that the team behind it is actively upgrading functionalities. It is important to note that the cloud offering currently supports only static analysis, but in a discussions with NowSecure representatives I was assured that the addition of dynamic analysis is in the pipeline for H2 2015.

Assessing mobile applications seems like a complex task, but NowSecure Lab definitely disproves this notion: it mostly requires you (the user) to point and click, and occasionally to interact with the service a bit more. You upload the .apk or .ipa file to the system, select the tests you want to run and, in a couple of minutes, you get a detailed report. It is as easy as that.





com.\_\_\_\_.le

ANDROID

VERSION 1.34

FILE \_\_\_\_-1.apk

Finished Testing Apr 28, 2015 - 10:59AM



13 TESTS



8 RISKS

100% TEST COVERAGE

The user interface is simple but very smooth. The Apps screen lists all the applications you've tested, together with the information on the times when tests were done, number of different builds assessed, and the number of discovered security threats.

Reports are available in an online, browsable version, or in the form of a downloadable PDF file.

Every security issue found in the mobile application you've tested is labeled as low (blue), medium (orange) or high (red) risk. You get a short description of the problem, a set of contextual findings (identifying the actual "offending" lines of code), downloadable artifacts

(decompiled app code), as well as very informative recommendations on what you should do to fix them.

Here is an actual example of a recommendation for an issue related to the SecureRandom implementation in an Android app: "Developers who use JCA for key generation, signing or random number generation should explicitly initialize the PRNG with entropy from /dev/urandom or /dev/random. Also, developers should evaluate whether to regenerate cryptographic keys or other random values previously generated using JCA APIs such as SecureRandom, KeyGenerator, KeyPairGenerator, KeyAgreement, and Signature."

## Assessment Report

Fiskal 1 | 1.34

APR 28, 2015



## Tests | Static Analysis

### ▲ APK Signing Key Check

#### DESCRIPTION

Your application was signed using a key length less than or equal to 1024 bits, making it potentially vulnerable to forged digital signatures.

#### RECOMMENDATION

We recommend signing your application using a key with a length of at least 2048 bits (preferably 4096 bits) to provide optimum protection against forged digital signatures. Keytool, used to sign Android applications as described here: <http://developer.android.com/tools/publishing/app-signing.html>, can be used with the parameter -keysize <size> to specify a longer key length than the 1024-bit default.

#### ADDITIONAL BEST PRACTICE

APK Signing Key Check: <https://www.nowsecure.com/resources/secure-mobile-development/android/android-apk-signing>

#### REGULATORY

CWE: 310, 326 OWASP Mobile Top 10: M6-Broken Cryptography

#### CONTEXT INFORMATION

{u'key\_type': u'RSA', u'key\_length': 1024}

### ▲ AllowBackup Flag

#### DESCRIPTION

Your application is declaring the "allowBackup" flag as true in the Android Manifest (or using the Android default value, which is true as well). This can potentially allow an attacker to backup your application folder and recover private data from it.

#### RECOMMENDATION

It is recommended to explicitly set the "allowBackup" flag to false in the Android Manifest.

#### REGULATORY

OWASP Mobile Top 10: M4-Unintended Data Leakage

I really liked the level of additional context NowSecure Lab reporting provides. For instance, I got one issue qualified as medium risk, but it was noted that if the app in question is an electronic wallet or is being used for processing monetary or Bitcoin transactions, its risk status should be elevated to high.

Also, in one of the screens it was noted that if the application uses reflection or a shared-id, static analysis may result in false positive results.

I presume they are actively working on minimizing false positives, as the same app I've assessed two months ago, now shows one less security issue.

From the user perspective, testing applications within the NowSecure Lab environment is rather straightforward, so it is important to see what type of tests are currently enabled.

New tests are being added to the web app - for instance, between my first post RSA Conference usage of NowSecure Lab and the assessment I did recently, there were several new tests added for Android alone. Here is what is checked when you feed the system an .apk file:

- **APK Files Check:** Shows the files contained in the APK package.
- **APK Signing Key Check:** Checks if the key used to sign the application has a size superior to 1024 bits.
- **AllowBackup Flag:** Checks if the application allows for saving of potential sensitive information during backups.
- **App Assembler Decompilation:** Determines if an application can be decoded and if its resources can be extracted for further analysis.
- **App Certificate Validity:** Checks if the certificate used during the application compilation is valid.
- **App Debug Flag:** Checks if the application was compiled with the debug flag set.
- **App Source Decompilation:** Source code is decompiled and made available to the analyst in several formats (Java/Smali).
- **App Source Obfuscation:** Checks if the source code has been obfuscated either







by Proguard or Dexguard in order to make class identification less obvious.

- **Application Overprivileged:** Checks if the application is declaring permissions that are actually never used or called in the code.
- **Dynamic Code Loading:** Allows advanced users to dynamically hook up and manipulate classes during a dynamic-analysis of the application.
- **Hardcoded URLs:** Checks for embedded URLs in the source code, which can point to sensitive company servers or assets and provide valuable information to potential attackers.
- **Javascript Interface:** Checks if WebView elements are potentially vulnerable to Remote Code Execution.
- **Master Key:** Checks if the application is protected against the Master Key vulnerability
- **Native Methods Check:** Shows the method calls in the APK that call native code.
- **Reflection Code Check:** Shows the method calls in the APK that leverage reflection.
- **Secure Random Check:** Ensures that the binary was compiled with the ASLR (Address Space Layout Randomization) flag.

Compared to the checks for Android, there are significantly less tests available for iOS applications:

- **Address Space Layout Randomization Check:** Ensures that the binary was compiled with the ASLR (Address space layout randomization) flag.
- **Automatic Reference Counting:** Checks if the application was compiled with flags, improving its performance and preventing some stack overflow vulnerabilities.
- **Heartbleed Check:** I assume this doesn't need a description
- **Local Authentication:** Checks if your application uses an insecure implementation of the Local Authentication framework.
- **OpenSSL:** Checks whether the app is bundled with a vulnerable version of OpenSSL
- **Stack Smashing Protection:** Checks if the application was compiled with flags preventing some stack overflow vulnerabilities.



RISK ▼	TEST NAME ▼	TYPE ▼	ACTIONS
 Medium	App Source Obfuscation	Static Analysis	<a href="#">View Details</a>
 Medium	Secure Random Check	Static Analysis	<a href="#">View Details</a>
 Medium	AllowBackup Flag	Static Analysis	<a href="#">View Details</a>
 Low	App Source Decompile	Static Analysis	<a href="#">View Details</a>
 Low	Application Overprivileged	Static Analysis	<a href="#">View Details</a>
 Pass	APK Signing Key Check	Static Analysis	<a href="#">View Details</a>

Over the past couple of years, there were numerous reports of malicious applications found in the Google Play store.

When I got the first media release on NowSecure Lab, I was intrigued to see that one of the specified features was "checking for issues in apps already publicly available in the app stores". When creating a new assessment, you can skip uploading the file and choose to test a public application.

For obvious reasons, only Android apps from the Play Store are supported, but unfortunately this feature didn't work for me. I tried all the possible inputs, from specific app names and full package names to random words, but the search always resulted in the message saying the requested app doesn't exist. This functionality seems interesting, but I would definitely spin it in a separate project, as the target audience for it is much broader than just mobile app developers with security on their mind.

## CONTEXTUAL FINDINGS

Lab has identified the following as being the cause for the current risk status. The following information and recommendations should help you resolve.

```
{
  "code_locations": "
  [{\"class\":\"Lcom/securitycompass/androidlabs/base/RestClient;\", \"method\":\"setLaxSSL\", \"signature\":\"()V\"}]\"
}
```

One of the upcoming additions to NowSecure Lab is the possibility of continuous integration. First it was planned to support Jenkins CI (application that monitors executions of repeated jobs, in this case building a software project), but now I see that they are mentioning support for multiple CI platforms. The script will automatically detect new builds, send them to the service for testing and provide the reports.

NowSecure Lab cloud, the online version of NowSecure Lab is currently in free public beta. Have in mind that some tests are only available for premium subscriptions. Pricing

details are not public, so you should contact the company directly if you are interested in leveraging the whole arsenal of security tests.

Whether it's used by developers to test some security aspects of the applications they've built, or is integrated into a Secure Software Development life cycle, NowSecure Lab cloud is a much needed security solution. I hope that by the end of the year we will see it maturing from its beta phase, together with the addition of dynamic analysis testing capabilities and continuous integration.



## Why vulnerability disclosure shouldn't be a marketing tool

by Brian Honan

There have been many arguments within the security community on how researchers should disclose the existence of a security vulnerability. Some argue that full disclosure is the best approach as it makes defenders aware of the security issue and they can take steps to reduce their exposure to it. Full disclosure advocates also say that this approach embarrasses large corporates and motivates them into taking action to address the security vulnerability.

Responsible disclosure advocates argue that their approach is better as it gives companies time to examine and fix the issue properly, and also encourages better relationships between researchers and developers.

They also argue that full disclosure provides attackers with the information they need to exploit vulnerable systems, a point counter-argued by the full disclosure advocates, who say that attackers are probably aware of the vulnerability anyway, so it's best to make defenders aware of it, too.

I am not going to discuss the merits of either side of the above debate. Instead, I want to

talk about a vulnerability disclosure trend that I have recently noticed – a trend that I believe may ultimately cause more harm than good: security vendors using vulnerability disclosure as a marketing tool with the goal of enhancing their company's bottom line.

It seems lately that no vulnerability can be announced without being provided with a catchy name and cool logo (e.g. Heartbleed and Shell Shock). Also, the technical material released about it often makes it seem that the Internet - or possibly even society as we know it - is destined to be destroyed forever.



So now we have three approaches to vulnerability disclosure: full disclosure, responsible disclosure, and marketing disclosure. My concern with the latter is that by its very nature it will get more coverage in both the IT industry and mainstream media.

This can result in senior management becoming increasingly concerned over a vulnerability that may have no impact on their organization, but because it was on the evening news they now look to their security team to deal with it.

In the cases where the vulnerability does affect the organization, the security team is called into action to remediate it, but this remediation may be based more on the impact the vulnerability has had on the news headlines rather than on the impact it actually may have on the environment. This results in already overstretched security teams being distracted from other core tasks.

I have talked to a number of CSOs who are frustrated by this approach by vendors as it means their valuable time is lost.

These highly publicized vulnerabilities can also have wider ranging impacts when lobbyists and politicians use them to support their arguments for introducing draconian measures to curb (what they believe are) “evil” security researchers. So when governments introduce laws to ban security research or make criminals out of researchers we should not be overly surprised.

The security industry and people in it need to realize that they are responsible for keeping technology secure for those who use it. This means taking a measured and often reserved approach to dealing with security issues and vulnerabilities. Vendors need to realize that the discovery of a new vulnerability is not the time to develop a new marketing campaign, but the time to engage in a mature way with others, in order to ensure that the vulnerability is dealt with in the most appropriate way.

If we continue to act like the boy who cried wolf, we should not be surprised when the wolf is ignored and we are the ones governments set in their sights.

Brian Honan ([www.bhconsulting.ie](http://www.bhconsulting.ie)) is an independent security consultant based in Dublin, Ireland, and is the founder and head of IRISSCERT, Ireland's first CERT. He is a Special Advisor to the Europol Cybercrime Centre, an adjunct lecturer on Information Security in University College Dublin, and he sits on the Technical Advisory Board for several information security companies. He has addressed a number of major conferences, wrote ISO 27001 in a Windows Environment, and co-authored The Cloud Security Rules.

Want to reach a large audience  
of security pros by writing for  
(IN)SECURE?

Send your idea to  
[mzorz@net-security.org](mailto:mzorz@net-security.org)



# **HITB GSEC SINGAPORE**

**THREE-DAY SECURITY CONFERENCE  
REGISTER. VOTE. NETWORK.**



## **KEYNOTE SPEAKERS**

**Kristin Lovejoy (President, Acuity Solutions)**


**Ofir Arkin (VP / Chief Architect, Intel Security)**

**Winn Schwartau (Founder, SecurityExperts.com)**

**Barry Greene (30-year veteran of Internet Security)**

**<http://gsec.hitb.org>**





# Malware world

## Cyber crooks opt for APT method for delivering malware

Delivering malware without it being flagged by users and security solutions is one of the biggest challenges malware peddlers face. Luckily for them, if they don't know how, they can outsource that task to more knowledgeable and/or resourceful malicious actors. Or, they can use a malware construction kit that allows them to package the malware into a payload that will (hopefully) foil all defenses.

One of these kits is Microsoft Word Intruder (MWI), which has been recently analyzed by SophosLabs researcher Gabor Szappanos.

"MWI generates Rich Text Format (RTF) documents that exploit multiple vulnerabilities in Microsoft Word," he explained. "The latest versions support multiple vulnerabilities within the same document. Each of the vulnerabilities has its own exploit block; these blocks are stored sequentially in the RTF document. This gives a higher chance of success, because a victim who has forgotten any one of the needed patches is therefore at risk."

Since May 2013, when it first appeared and used an exploit for only one vulnerability, the toolkit has been used by a variety of attackers. Sold on underground markets, the kit be-

came so popular that, in early 2014, security researchers noted that it was used more and more by run-of-the-mill cyber crooks who were simply after money. Prior to that, exploited documents were used almost exclusively by APT players.

MWI's creator, who is believed to be Russian and who goes by the online handle "Objekt", worried about this increased popularity as it meant that, in time, the exploits the kit uses and the documents it creates will be flagged by more and more security solutions.

So he tried to do some damage control, and instructed paying customers to use the kit only for low volume, targeted attacks. And they seem to have complied.

According to Sophos, the samples they collected contain mostly money-stealing Trojans, commercial password stealers, and RATs, and the kit remained largely unknown to the general public until 2015.

"It seems that its primary users are money-making cybercriminals aiming for smaller, less obvious, malware campaigns," says Szappanos, pointing out that some cybergangs (Sophos follows a dozen) obviously discovered that sometimes less can be more.

## Adware installer gives itself permission to access Mac users' keychain

Malwarebytes researcher Adam Thomas has made an interesting discovery: an adware installer created by Genieo, a well-known distributor of unwanted software, is taking advantage of an OS X feature to access information stored in the "Safari Extension List" in the users' keychain.

The problem is the installer doesn't allow the user to make the choice of whether they will allow it to access to the keychain. Instead, it "hijacks" the users' mouse cursor and clicks on the "Allow" button - and it does it so quickly (in mere seconds) that the users might not even notice it.

The installer does this so it could install a Safari extension named Leperdvil, which is used to distribute additional potentially unwanted software and change certain Safari settings.

"This seems like an unnecessary hack, considering that Genieo installers have been installing Safari extensions for years. Perhaps it's an attempt to get around changes to handling of Safari extensions in the upcoming El Capitan (OS X 10.11)," Malwarebytes' Thomas Reed posits.

"More concerning, though, is the question of what's to stop this adware from accessing other confidential keychain information... like, say, passwords? With a few minor changes, the adware could get access to other things from the keychain, like the user's iCloud password."

And what stops malware peddlers from using this same approach? "I'm surprised nobody thought of that before," Reed commented for Ars Technica.

The vulnerability - or rather, the feature - has likely been introduced by Apple in order to help visually or physically impaired users use the computer. But with this approach having been made public, it's more than likely that Apple will have to come up with a solution to the problem.

This particular installer has been spotted over a month ago exploiting a privilege escalation bug (DYLD\_PRINT\_TO\_FILE vulnerability) that allows it to gain root access machines running OS X 10.10, and has since been squashed by the company.

The feature / vulnerability misused by the installer was initially discovered by Antoine Vincent Jebara and Raja Rahbani, the CTO and lead engineer (respectively) of identity management company MyKi.

## Malvertising campaigns increase 325 percent

Cyphort investigated the practices used by cyber criminals to inject malicious advertisements into legitimate online advertising networks. Researchers found that malvertising campaigns carried out by hackers increased 325 percent in the past year. Often times, the hackers will put legitimate ads on trustworthy web sites to build up support. They are basically trying to trick the network by appearing to look legitimate.

Once trust is built, the hacker inserts malicious code or spyware behind the ad on a limited basis, just long enough for malware to be launched. Malware is then unknowingly incorporated into web pages through a corrupt or malicious ad. Consumers are the most direct

victims as their computers and contained files are infected by simply clicking on a malicious ad or in some cases, by simply going to a site they visit frequently.

The problem of malvertising isn't going away and cyber criminals will continue finding ways to monetize their attacks. According to the Association of National Advertisers, ad-fraud will cost global advertisers more than \$6 billion in 2015.

To help combat the growing threat of malvertising campaigns, Cyphort Labs recommends the following steps to implement an effective cybersecurity defense:

1. Advertising networks should use continuous monitoring that utilize automated



systems for repeated checking for malicious ads.

2. Scans should occur early and scan often, picking up changes in the complete advertising chains instead of just ad creatives.
3. Ad networks should leverage the latest security intelligence to power their monitoring

systems to stay up to date with global threats.

4. Individuals should avoid “blind” surfing to reduce their exposure to drive-by infection. Keeping your computer system and security software patched in timely manner will go a long way in protecting you when you do have to venture into the “dark night.”

## 49 new Regin backdoor modules discovered

Since Symantec and Kaspersky Lab researchers presented their findings on the Regin backdoor late last year, there has been only one additional publicly revealed sighting of (a part of) the sophisticated espionage tool, and it pointed to the conclusion that the malware is wielded by the Five Eyes intelligence alliance.

The Regin backdoor has been used since at least 2008 to mount spying operations against government organizations, infrastructure operators, private sector businesses, but also researchers and private individuals, mostly in the Russian Federation and Saudi Arabia, but also in Mexico, Ireland, India, Iran, Belgium, Afghanistan and Pakistan. The malware is not used to collect specific information - it is used for the collection of various types data and the continuous monitoring of targeted organizations or individuals.

"Regin is a five-stage threat, with each stage loading and decrypting the next one. The malware is modular in structure, which allows its controllers to add and remove specific features depending on the target," Symantec researchers explain. "Some Regin modules control basic functions of the malware, such as networking or handling Regin's encrypted virtual file system (EVFS). Other modules act as payloads, dictating the functionality of each Regin infection."

Since their initial report on the backdoor in 2014, they still haven't obtained the initial dropper, but they have discovered 49 new modules (the total number has now reached 75), which provide a wide variety of spying, exfiltration, forensics, transport, filtering, and cryptographic capabilities.

The malware uses six transport protocols for communication and data exfiltration: CMP, UDP, TCP, HTTP Cookies, SSL, and SMB. The communication traffic to the C&C servers is relayed through a network of Regin-infected computers.

"Regin's P2P communications capability sees each Regin infection assigned a virtual IP address, forming a virtual private network (VPN) on top of the physical network of the infected computer. This P2P capability allows the attackers to maintain deep access to critical assets within compromised organizations and mask core infrastructure belonging to the group," the researchers pointed out, and explained that traffic between nodes can be configured to match expected protocols based on where the nodes are placed on a network, adding a further degree of stealth to communications.

Despite the fact that the researchers haven't managed to get their hands on newer versions of the malware, they say it's unlikely that the group using it has stopped developing it.

It's also unlikely that the group has ceased operations.

"Its track record and available resources mean it is probable that the group will re-equip itself with a new threat or upgrade Regin in a bid to evade detection. The latter is the most likely course of action, given the time it would take to develop an equally capable malware framework from scratch," the researchers noted.

On the other hand, it's also possible that they have been working on another attack framework for years now, getting it ready to replace Regin as soon as its exposure makes it too dangerous and ineffective to use.



# SOLUTIONARY®

AN NTT GROUP SECURITY COMPANY



**Services and  
Intelligence  
to Optimize  
Security and  
Mitigate Risk.**



**Managed Security Services**  
**Targeted Threat Intelligence**  
**Security Log Monitoring**

**Log Management**  
**Critical Incident Response**  
**Professional Services**

**Visit [Solutionary.com](http://Solutionary.com) for More Information**





## Report: Black Hat USA 2015

by Mirko Zorz



In its 18th year, Black Hat USA 2015 welcomed more than 11,000 infosec pros. Boasting more than 110 research-based briefings presented by more than 190 researchers and speakers, as well as 70 in-depth trainings, attendees experienced the most intensive schedule to date.

Jennifer Granick, Director of Civil Liberties at the Stanford Center for Internet and Society, delivered her dynamic presentation about the dying dream of Internet freedom to a packed keynote room, filled with more than 6,000 attendees.

The Black Hat Arsenal returned for its sixth year, offering researchers and the open source community a venue to demonstrate tools they develop and use in their daily professions – from visualization and phishing to collaborative analysis and pentesting. This year's event featured 58 tools, the largest Arsenal event to date.

Black Hat's "Beyond the Gender Gap: Empowering Women in Security" panel featured some of the top women in the security field sharing their paths to success, as well as insight on recruiting, retaining and the profes-

sional advancement of women in the security industry.

The Business Hall was action-packed, as more than 200 of the industry's top companies showcased their latest technologies and solutions alongside the newly launched International Pavilion and Career Zone, as well as the Innovation City for startups.

### **Malicious advertisements surge! 260% spike in 2015**

RiskIQ announced its latest findings on the prevalence of malvertising across the nearly two billion publisher pages and 10 million mobile apps it monitors per day.

In the first half of this year the number of malvertisements has jumped 260 percent compared to the same period in 2014.



The sheer number of unique malvertisements has climbed 60 percent year over year. Meanwhile, fake Flash updates have replaced fake antivirus and fake Java updates as the most commonly method used to lure victims into installing various forms of malware including ransomware, spyware and adware.

“The major increase we have seen in the number of malvertisements over the past 48 months confirms that digital ads have become the preferred method for distributing malware,” said James Pleger, Director of Research at RiskIQ.

“There are a number of reasons for this development, including the fact that malvertisements are difficult detect and take down since they are delivered through ad networks and are not resident on websites. They also allow attackers to exploit the powerful profiling capabilities of these networks to precisely target specific populations of users.”

The rise of programmatic advertising, which relies on software instead of humans to purchase digital ads, has generated unprecedented growth and introduced sophisticated targeting into digital ad networks.

This machine-to-machine ecosystem has also created opportunities for cyber criminals to exploit display advertising to distribute malware. For example, malicious code can be hidden within an ad, executables can be embedded on a webpage, or bundled within software downloads.

### **79% of companies release apps with known vulnerabilities**

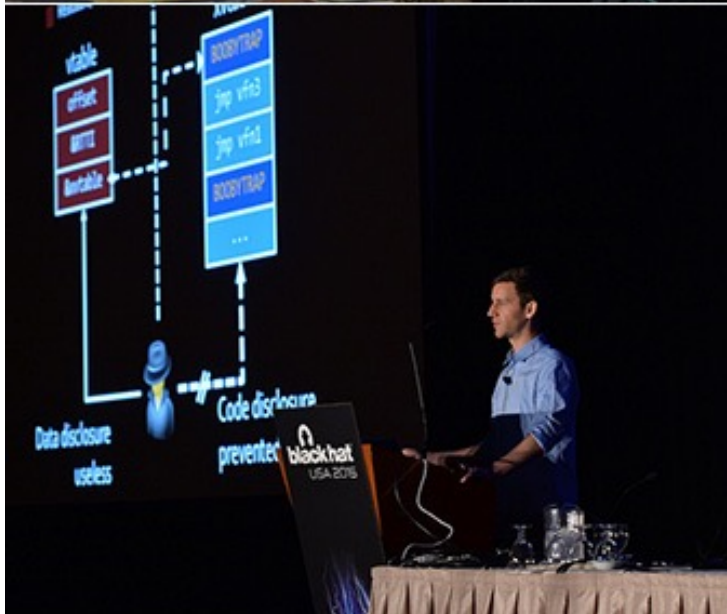
The application development process is rampant with security risks due to current business pressures, according to new research by Prevoty.

From competing business pressures to secure code training to scanning false negatives, developers have their backs to the wall when it comes to developing and releasing applications that not only perform the function they are designed to perform, but also do so in a way that protects the company’s prized data.

Security is left to the last minute -- if considered at all. Nearly half of those surveyed say they knowingly release applications with vulnerabilities at least 80 percent of the time. Key takeaways from the survey responses include:

- 85 percent say vulnerability remediation has a significant impact on the ability to release applications and features on schedule and on budget.
- More than 70 percent admitted that business pressures to quickly release application updates often override security concerns.
- Nearly 80 percent of developers worry that their clients won’t trust their applications if they admit there is a security flaw.
- Nearly half (43 percent) admit to releasing applications with vulnerabilities at least 80 percent of the time.







## Qualys announces free global asset inventory service

Qualys announced the availability of Qualys AssetView, a free cloud-based asset inventory service that enables companies to search for information on any IT asset where an agent is deployed, scaling to millions of assets for organizations of all sizes. Global IT assets can be searched in seconds and an up-to-date inventory continuously maintained.

IT teams are looking to move beyond traditional scanner-based approaches to efficiently tackle endpoint security, but are often challenged with getting full visibility and control of all IT assets needed to maintain security and compliance within their organization.

The availability of AssetView gives IT professionals a fast, actionable view of IT assets in their environment, enabling more effective management and security of endpoints. The service leverages the Qualys Cloud Agent Platform (CAP), a platform of lightweight agents that continuously assess and address security and compliance of IT assets in real time, whether on-premise, mobile or in the cloud.

## API security becoming a CXO level concern

Akana released the findings of a survey of over 250 security practitioners, including CSOs, CISOs, and security architects.

Aimed at quantifying the maturity of API security practices amongst the leading digital enterprises, the survey results reveal that while the majority of respondents are taking steps to

secure API access, only few had taken steps to ensure that sensitive data was being securely handled in the apps that access the APIs.

Just as the emergence of Web brought web-based threats and resulting countermeasures to the forefront, the survey indicated universal recognition from security practitioners of increasing threats and vulnerabilities that are unique to the API channel.

### Key findings:

- More than 65% of the respondents reported that they do not have processes in place to ensure that the data that is being accessed by applications consuming APIs is managed securely. With mobile apps and IoTs increasingly being API consumers, enterprises face exposure to threats of unauthorized access to data once accessed through an API. Almost 60% of survey respondents indicated that they were not securing API consumers.
- A large proportion of survey respondents (>45%) also did not rate limit access to their APIs, a control that can reduce the risk of hacking.
- API security is as much an issue for the business as it is for IT, with 75% of respondents said that API security was a CIO-level concern. 65% said it was an issue for business managers. As APIs are increasingly being adopted to drive digital initiatives, both business and IT see increasingly value in securing them.
- JSON Scheme, DDoS, Message-Level security, Encryption were amongst the top API security threats.



## The state of the mobile ecosystem

Appthority released their second Q2 2015 Enterprise Mobile Threat Report, for which their researchers analyzed security and risky behaviors in three million apps and assessed how these risks are impacting enterprise environments. Enterprise and government workforces depend on mobile solutions for increased productivity, while adopting Bring Your Own Apps (BYOA) and Bring Your Own Device (BYOD) policies in an effort to protect against corporate security and privacy risks.

Enterprise data crossing international borders – Appthority mapped the geographic flow of enterprise data and discovered that apps are sending PII (personal identifiable information) and other sensitive information all over the globe, often without the enterprise's knowledge. The top iOS apps sent data to 92 different countries while the top Android apps sent data to 63 different countries.

The risk of the third party library – Overstretched enterprise app development teams increasingly rely on third party libraries and SDKs. With no policy in place to analyze mobile app security, enterprise data is put at risk when one of those popular third party packages carries a major vulnerability.

Zombie apps, a threat that won't die – Zombie apps are apps that have been revoked by the app store and are no longer receiving security updates. App stores are under no regulatory obligation to inform users of revoked apps, and Appthority's research shows that 100 percent of enterprises surveyed have zombie apps in their environments, leaving the door wide open for cybercriminals and other security threats to access sensitive data.

### Microsoft expands Bug Bounty programs, increases rewards

Microsoft is continually tweaking its Bug Bounty programs, and the latest step in this evolution has been announced at Black Hat USA 2015.

"We are raising the Bounty for Defense maximum from \$50,000 USD to \$100,000 USD," Jason Shirk of the Microsoft Security Response Center noted, and explained that the

company is eager to "reward the novel defender equally for their research."

The Online Services bug bounty has also been expanded to include vulnerabilities in RemoteApp, the solution that lets users run Windows apps hosted in Azure anywhere, and on a variety of devices (Windows, Mac OS X, iOS, or Android).

Researchers who discover and responsibly disclose authentication vulnerabilities in Microsoft Account (MSA) and Azure Active Directory (AAD) from now until October 5, 2015, will receive twice the normal payout. It can now reach as high as \$30,000 - previous reward amounts varied between \$500 and \$15,000.

"These additions to the Microsoft Bounty Program will be part of the rigorous security programs at Microsoft. Bounties will be worked alongside the Security Development Lifecycle (SDL), Operational Security Assurance (OSA) framework, regular penetration testing of our products and services, and Security and Compliance Accreditations by third party audits," Shirk added.

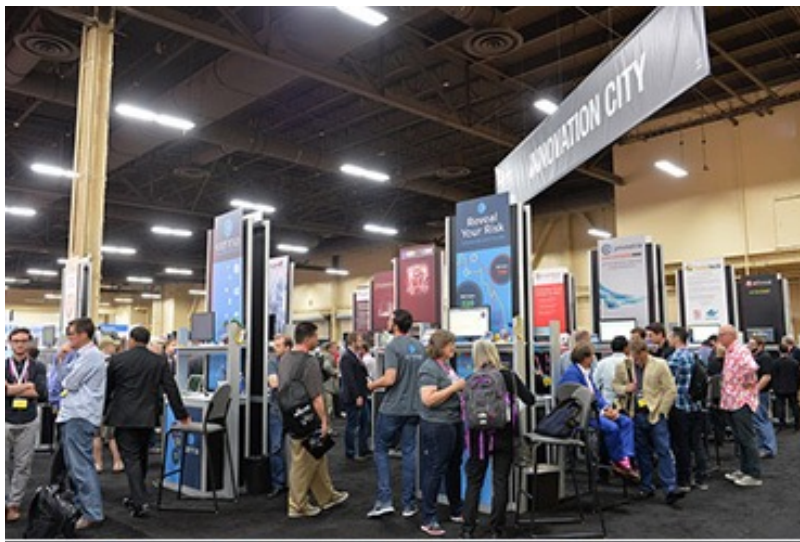
### CDNetworks showcased Cloud Security 2.0

CDNetworks, the global content delivery network (CDN), showcased Cloud Security 2.0 during Black Hat USA 2015. Cloud Security 2.0 includes intelligent, next generation behavioral-based WAF technology and DDoS mitigation. This comprehensive solution combines web application and website acceleration with end to end security including DDoS attack mitigation at the network and application layers with 24/7 monitoring and customer portal visibility.

CDNetworks Cloud Security is a proven solution for DDoS attack protection and mitigation where malicious traffic is filtered and quarantined while legitimate traffic continues to follow, thus reducing the impact on end-users and revenue.

Now, next generation WAF technology from industry leader Fireblade is integrated into CDNetworks' global network, providing an intelligent firewall that is self-learning and self-evolving as opposed to older signature-based firewall technology.







## Corporate networks can be compromised via Windows Updates

Researchers from UK-based Context Information Security demonstrated how Windows Update can be abused for internal attacks on corporate networks by exploiting insecurely configured enterprise implementations of Windows Server Update Services (WSUS).

WSUS allows admins to co-ordinate software updates to servers and desktops throughout their organisations, but the Microsoft default install for WSUS is to use HTTP and not SSL-encrypted HTTPS delivery. By exploiting this weakness, the Context researchers were able to use low-privileged access rights to set up fake updates that installed automatically.

These updates could potentially download a Trojan or other malware and be used to set up admin access with a false user name and password. Any Windows computer that fetches updates from a WSUS server using a non-HTTPS URL is vulnerable.

“It’s a simple case of a common configuration problem,” says Paul Stone, principal consultant at Context. “While Microsoft does not enforce SSL for WSUS, it presents the option and most companies will go through this extra stage to use HTTPS. But for those that don’t it presents an opportunity for an administrator to compromise complete corporate networks in one go.”

Organisations can quickly find out if they are vulnerable by checking the WSUS group policy settings, while it is possible to check if an individual machine is incorrectly configured by looking at the appropriate registry keys. If the URL does not start with https, then the computer is vulnerable to the injection attack.

While following Microsoft’s guidelines to use SSL for WSUS will protect against the described attacks, Context also suggests that there are further ‘defence in depth’ mitigations that could be implemented by Microsoft to provide further protection.

“Using a separate signing certificate for Windows Update would increase protection and the update metadata itself could be signed by Microsoft to prevent tampering,” says Alex Chapman principal consultant at Context and

joint presenter at Black Hat. “Signing the tags that contain the main detail of the updates with a Microsoft certificate would avoid the necessity of setting up a trust relationship between the client and WSUS server.”

During the Black Hat presentation, the Context researchers also raised concerns about third-party drivers installed via Windows update. There are over 25,000 potential USB drivers that can be downloaded – although this list includes many duplicates, generic drivers and obsolete versions.

“We have started to download and investigate some 2,284 third-party drivers,” said Stone. “Our concern is that when plugging in a USB device, some of these drivers may have vulnerabilities that could be exploited for malicious purposes. Everyone is familiar with the ‘searching for Drivers’ and ‘Windows Update’ dialog boxes on their desktops – but these seemingly innocuous windows may be hiding some serious threats.”

## Vulnerabilities in 2015: 0-days, Android vs iOS, OpenSSL

Secunia has taken an early peek at the trend in vulnerabilities for 2015, and has presented the results at Black Hat USA 2015. Seven months into the year, the number of detected zero-day vulnerabilities has risen substantially compared to 2014, while the total number of vulnerabilities is largely the same as this time last year.

15 zero-days have been discovered so far in 2015, making it likely that the total 2015 number will exceed the 25 discovered in 2014.

The 2015 zero-days were all discovered in popular Adobe and Microsoft products widely in use across private and professional IT systems.

At 9,225 the total number of vulnerabilities discovered from January 1 to July 31st is on a par with the 9,560 discovered over the same period in 2014, but Secunia’s preliminary findings do indicate a shift in criticality ratings: A slightly higher share of the vulnerabilities discovered are rated as “extremely critical” (from 0.3% to 0.5%) and “highly critical” (from 11.1% to 12.7%) while there is a drop in the “moderately critical” category (from 28.2% to 23.7%).





## Attackers use Google Drive, Dropbox to breach companies

A new type of attack, “Man in the Cloud” (MITC), can quietly co-opt common file synchronization services, such as Google Drive and Dropbox, to turn them into devastating attack tools, Imperva has revealed in a report released at Black Hat USA 2015. This next-generation attack does not require compromising the user’s cloud account username or password, and could be a very effective way of delivering malware.

"MITC does not require any particular malicious code or exploit to be used in the initial 'infection' stage, thus making it very difficult to avoid. Furthermore, the use of well-known synchronization protocols make it extremely difficult (if not impossible) to distinguish malicious traffic from normal traffic. Even if a compromise is suspected, the discovery and analysis of evidence will not be easy, as little indication of the compromise is left behind on the endpoint," the company explained.

An additional unwelcome result of such an attack is that it might be very difficult and often impossible for the companies to recover the compromised account, so they would have to create a new one.

## Privileged accounts are still easy to compromise

A Thycotic survey of 201 Black Hat USA 2015 attendees found that a majority (75%) have not seen a fundamental change in the level of difficulty in compromising privileged account credentials, despite an overall increase in IT security spending over the past two years.

Among other topics, the survey also asked hackers how often they come across privileged account credentials in unprotected files like spreadsheets. Only 6 percent of respondents said they had never seen this, meaning 94% find privileged credentials in unprotected files at least some of the time.

Other key findings from the survey include:

- Hackers indicated that privileged account credentials are the best targeted assets for

gaining direct access to large amounts of critical data. 45% identified privileged credentials as their favorite target, while only 33% chose end user credentials as the easiest way to get what they are after.

- 9 out of 10 respondents said it is as easy or even easier to compromise privileged account credentials now than it was two years ago
- Healthcare organizations were indicated (29%) to be the primary target for breach vulnerability, followed by financial services companies (25%) and government organizations (24%).

“Perhaps not surprising to those in the cybersecurity industry, it is apparent that for all the new defensive solutions that have been introduced, we still haven’t cracked the code on how best to protect mission-critical data and company secrets, and in fact, in some cases we’re only adding additional layers of complexity which provide attackers more attack vectors to use to break in,” said Nathan Wenzler, senior technology evangelist at Thycotic.

## Hope is not a strategy, we need more healthy paranoia

35 percent of security experts believe leadership within their organization lacks a healthy paranoia, with 21 percent of leadership "relying on hope as a strategy" to avoid a cyber security breach.

Conducted live during the week of Black Hat USA 2015, DomainTools' findings indicate that nearly half of those polled worry that the DNA of their organization is not security-driven, citing a lack of situational awareness within the company.

Not surprisingly, the number one complaint was that the leadership team was making decisions without involving the security team – those closest to the risk.

Budgets are not keeping pace with the acceleration of cyberthreats, with nearly half (47 percent) of respondents stating their budgets were inadequate for the task at hand and two-thirds of the remaining group stating a desire for more funding above the current "acceptable" levels.

# Cyber Risk Predictive Analytics

## Risk Fabric<sup>®</sup>

Bay Dynamics<sup>®</sup>

### Solutions



#### **Insider Threat**

Someone inside your organization is missing or leaking information.



#### **Outsider Threat**

Someone outside your organization is seeking to gain protected information.



#### **Attack Surface Threat**

Proactively identify and protect your most valuable and vulnerable assets.

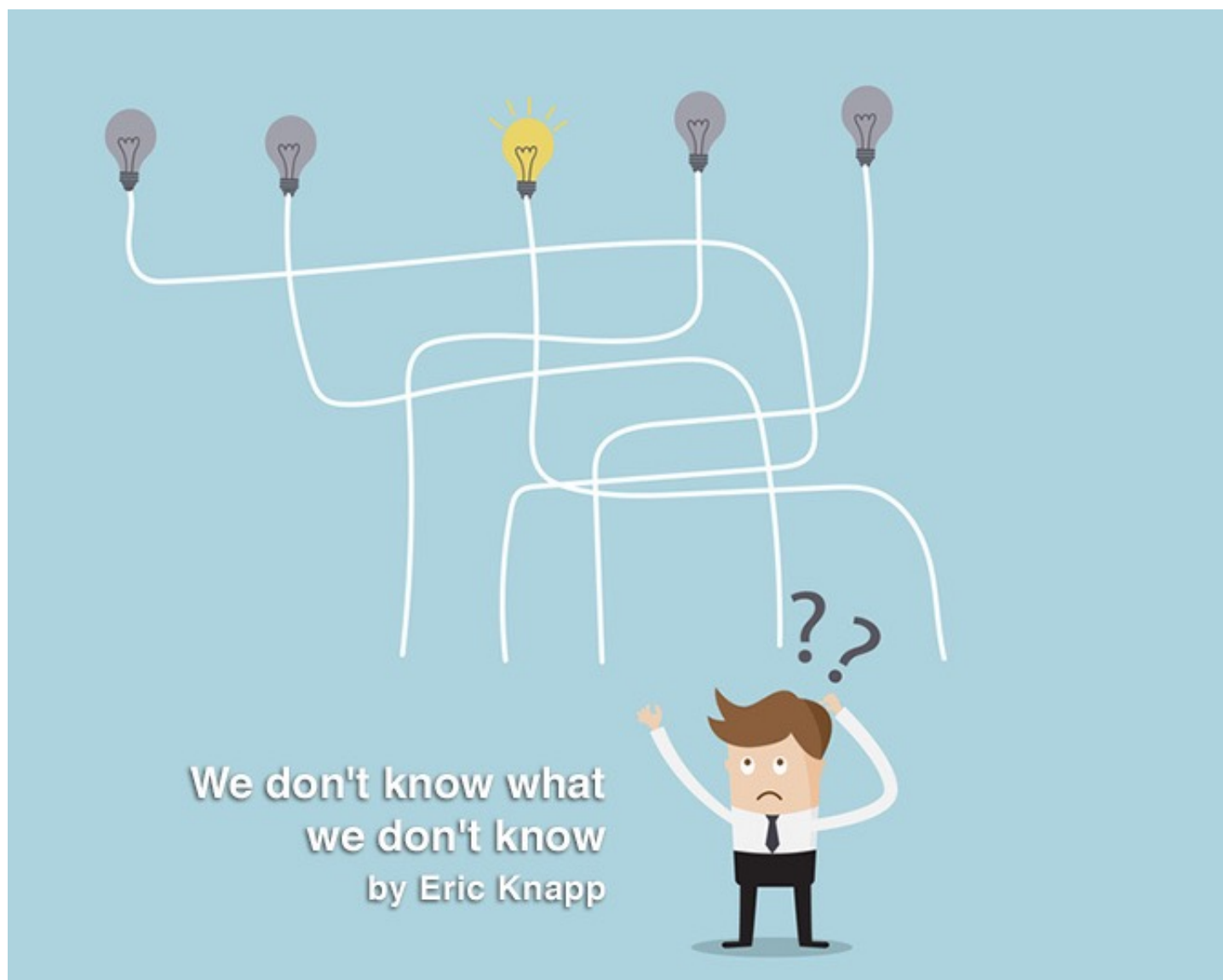


#### **High Privilege Access Threat**

Proactively provide cyber counterintelligence for high privilege accounts and high risk users.







## We don't know what we don't know

by Eric Knapp



Citing the latest cyber security statistics is a popular way for security companies to show that they are keeping a watchful eye on the threat landscape. Where does the majority of threats come from? What industries are being targeted? Which countries are involved? Which mobile OS is better? We want answers to these and dozens of questions more, and we want those answers in nice, concise, tweetable metrics.

But the problem is that we simply don't know. Sure, some companies claim to know, but here's a secret: they're wrong. They might know something, probably even a lot, but not everything.

Various CERT organizations, for example, often know more about security issues than most companies because that's what they do: they track security issues - vulnerabilities, exploits and incidents.

Still, even they don't know what they don't know, because not everyone needs to or wants to report what they know to a CERT, not

all vulnerabilities have been discovered, not all exploits have been dropped, and not all incidents are reported.

Yes, we're all trying, and every data point helps. But are 59 percent of cyber security incidents unintentional? No, 59% of reported incidents are unintentional. That's probably because it's relatively painless to report that you made a mistake - some companies may even reward you for it. Still, not everyone will report their incidents to the same organization, and a good method of information sharing between organizations, industries and nations is still absent.

Are there six new malware samples created every 6 seconds? Several sources claim that there are six new malware samples captured every second, but there may be more that remain uncaught. We know as much about the true murky depths of malware in the wild as we do about what lies at the bottom of the Earth's oceans.

As Albert Einstein once said, "If we knew what it was we were doing, it would not be called research, would it?"

Ironically, one of the world's great malware research labs was recently breached by hackers who wanted to gain an offensive advantage by learning more about the firm's security solutions' detection capabilities. Is this a first-time-ever event? Surely other research facilities have also been targeted. Have they been successful in their defense, or are they simply unaware of their exposure? Don't forget that malware is sophisticated these days. In fact, it's so sophisticated we don't even know how sophisticated it is.

Albert Einstein once said, "If we knew what it was we were doing, it would not be called research, would it?"

The truth is that our current state of knowledge on cyber security is transient. Like a mayfly, we have a very short time to understand our surroundings and to learn. When we glance at the latest threat maps from companies like Norse (which admittedly are fun to watch), what we learn from them fades just as soon as we turn our heads.

Our adversaries are always changing, evolving. The targets change, and the vectors shift, branching out or converging. It's a research project of truly epic proportions and everything we learn is quickly outdated.

Luckily, unlike the poor mayflies, we get to live another day and gain a collective experience

that makes it a little bit easier to figure things out this time, and then easier still the next time. Thanks to the organizations and individuals mentioned here - the CERTs, labs, analysts and innovators - our defensive capabilities are evolving, too.

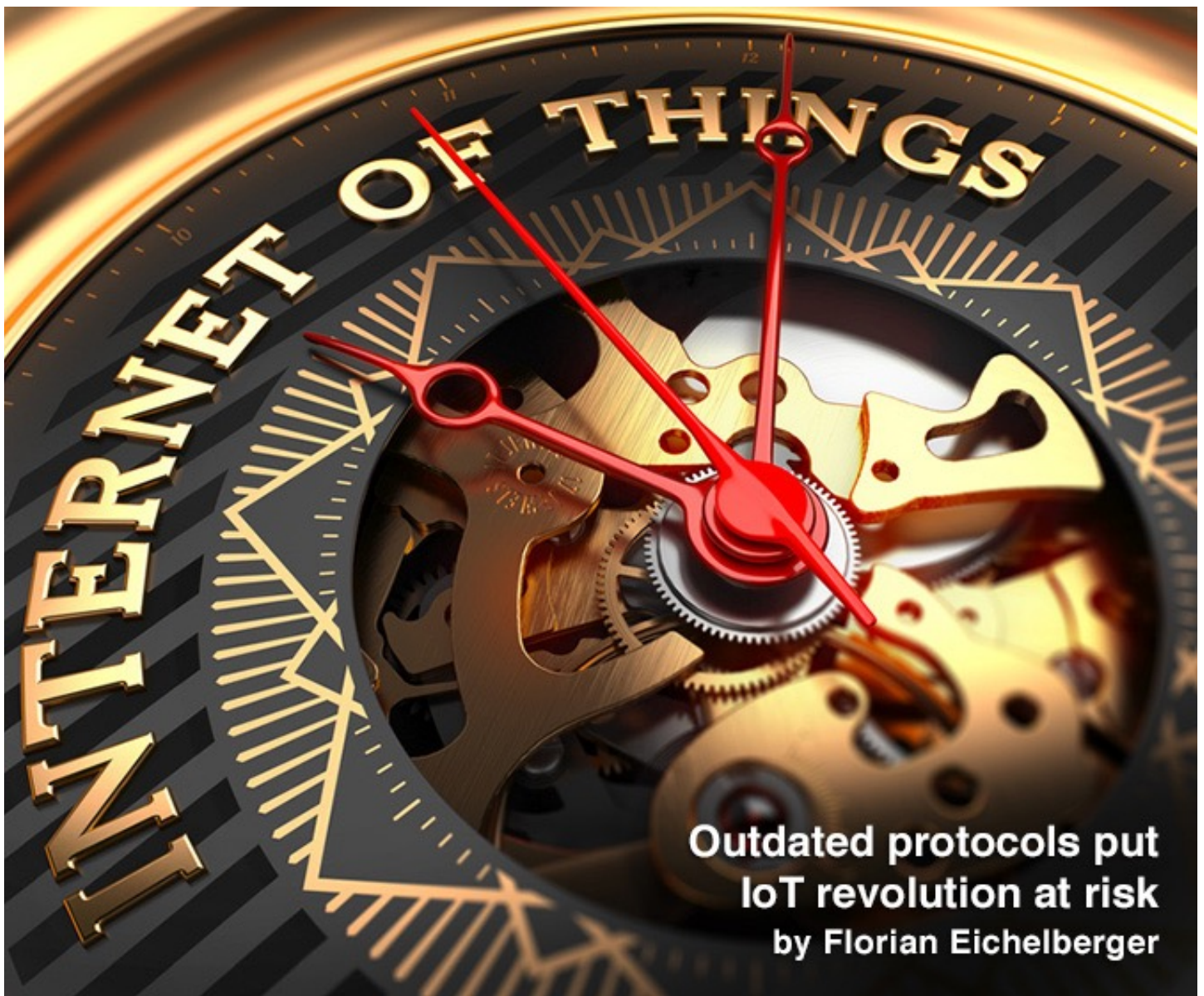
But even cyber security's venerable and respected long-beards don't know everything. Unlike the laws of nature, cybercriminals are actively trying to elude us.

My advice? Remind yourself every day that you don't know what you don't know, and let your imagination become the greatest source of threat intelligence in your cyber security arsenal.

Eric D. Knapp is an expert in industrial control systems cyber security.







Linking physical objects in the real world to the virtual world and enabling “anytime, anyplace and anything” communication was once the stuff of science fiction. However, it is made real today with the Internet of Things (IoT), which is widely considered to be the next phase of the Internet revolution.

Knowing this, you would expect the protocols and infrastructure supporting IoT to be just as advanced. However, this is not the case. More often than not, the technology underpinning the IoT is straight out of the 1990s or early 2000s – more Sega Dreamcast than Playstation 4.

As one of the most publicly known, accepted and widespread applications of IoT, the trend of automating buildings and making homes smarter - to save energy, increase comfort or simply add capabilities for remote monitoring and control - is on the rise. Home automation is likely to cover the following areas within a “smart home”:

### **HVAC control**

Smart HVAC units control room temperature as well as automated ventilation systems, which can be switched on to replenish clean air based on temperature, moisture, smoke, heat, dust, or carbon dioxide level in the unit.

### **Light control**

In conjunction with smart bulbs, these units can adjust lighting behavior according to the presence of inhabitants. Smart lights can be automatically switched off when the unit is unattended and automatically dimmed when there is natural light.

## Smart surveillance

Intelligent surveillance systems record activity in the smart home, allowing also authorities to remotely monitor where (and if) necessary.

## Smart door lock

Smart door locks can be opened or locked remotely by a user. They can also track people entering or leaving the premises and can act upon this by notifying the inhabitants or authorities.

Home automation systems are prone to a variety of threats. While some threats, like an attacker turning off lights, might be just a nuisance, an attacker disabling a HVAC system might have a more significant impact. Should an attacker be able to turn off the alarm system or open the front door of a smart home remotely, the threat quickly becomes critical. These attacks are possible due to the decisions made when designing IoT protocols such as ZigBee, Z-Wave, and KNX (compatibility and time-to-market issues), and because of errors and vulnerabilities in the device implementations.

The ease-of-use of wireless IoT protocols is their greatest asset, but also their greatest weakness. Wireless networks are prone to jamming (attackers try to prevent sensors from contacting the central hub by blocking the signal), the communication can be eavesdropped on to gather secret keying material, and is vulnerable to replay attacks (attackers inject recorded packets, e.g. a “door open” command to a door lock, or a “no-motion” command to a motion sensor, into the communication destined for the connected device or sensor).

## The ZigBee standard

ZigBee is a standard for personal area networks developed by the ZigBee Alliance, which includes companies like Samsung, Philips, Motorola, Texas Instruments and many others, with the aim of providing a low cost, low power consumption, two way, reliable, wireless communication standard for short range applications. The standard is completely open and was ratified by the Institute of Electrical and Electronics Engineers (IEEE) in 2003. The protocol stack of ZigBee

is based on IEEE 802.15.4. The advantages of choosing ZigBee are the provision of long battery lifetime, the support of a large number of nodes (up to 65000) in a network, easy deployment, low costs, and global usage.

ZigBee is used in the following areas:

- Remote control
- Input devices
- Home automation
- Healthcare
- Smart energy.

The key to the communication between devices on a ZigBee network is the use of application profiles. Application profiles are agreements for messages, message formats, and processing actions that enable developers to create an interoperable, distributed application employing application entities that reside on separate devices.

An example of a profile would be the home automation profile that covers a broad range of devices. These devices are designed to exchange well known messages to effect control such as turning a lamp on or off, sending a light sensor measurement to a lighting controller, or sending an alert message if an occupancy sensor detects movement.

If a manufacturer wants a device to be compatible with certified devices from other manufacturers, the device has to implement the standard interfaces and practices of this profile.

The Home Automation Public Application Profile states that: "The current network key shall be transported using the default TC link key in the case where the joining device is unknown or has no specific authorization associated with it."

This allows for the case where alternative pre-configured link keys specifically associated with a device can be used as well. As the network key is used to encrypt the communication between the ZigBee devices, it's a critical component of ZigBee Security. An issue arises from the fact that there is a default fallback mechanism that requires vendors to use a default TC link key of "ZigBeeAlliance09".



Since the security of ZigBee is highly reliant on the secrecy of the key material and therefore on the secure initialization and transport of the encryption keys, this default fallback mechanism has to be considered as a critical risk. If an attacker is able to sniff a device joining the network and using the default TC link key, the active network key is compromised and the confidentiality of the whole network communication can be considered compromised. As the home-automation profile covers devices from lights to HVAC and door locks, this compromise might lead to serious security issues.

Another threat for ZigBee devices is tied to lights using the ZLL profiles. Those devices support a feature called “Touchlink Commission” that allows devices to be paired with controllers. As the default and publicly known TC link key is used, devices can be “stolen”.

Tests showed that amateur radio hardware such as a Raspberry Pi extension board with normal dipole antennas already allowed Touchlink Commission from several meters away, whereas for security reasons this should only work in close proximity.

In order to enable devices from multiple vendors to talk to each other, Z-Wave implemented command classes to differentiate between actions and responses on the network.

## Z-Wave

As one of the leading wireless protocols in smart home automation, Z-Wave stands on the forefront of the IoT revolution.

The Z-Wave protocol was designed in 2001 by a company called Zen-Sys, which was later acquired by Sigma Systems. The Z-Wave Alliance was founded in 2005 and is a group of over 325 companies that manufacture wireless home control products and services based on the Z-Wave standard. Principal members include ADT, Evolve Guest Controls, FAKRO, Ingersoll Rand, Nexia Intelligence, Jasco Products, LG Uplus, Nortek Security & Control, SmartThings, and Sigma Designs.

Z-Wave is targeted at the home-automation / consumer market and is used in the following areas:

- Door locks
- Lights
- Gas sensors / fire sensors
- HVAC
- Switches
- Motion sensors.

Z-Wave operates in the industrial, scientific and medical radio frequency (ISM) and the Short-Range-Devices (SDR) band using 850 or 950 MHz frequencies, unlike ZigBee, which operates in the 2.4 GHz range. Those bands

were chosen to limit possible interferences with other devices like Bluetooth headsets or wireless networking devices and to provide better penetration of walls and less reflections.

In order to enable devices from multiple vendors to talk to each other, Z-Wave implemented command classes to differentiate between actions and responses on the network. Each command class supports one or more defined commands that define its functionality, so for example a class might be used to shut-down all devices that support it with a single button press. Unlike ZigBee’s, Z-Wave’s protocol specifications are not publicly available.

The security of network communication is based on the secrecy of a network key that is generated by a central controller unit. Even though the network key is random, the key used to encrypt the network key is known to be sixteen times 0x00 and is thus recoverable. Z-Wave implemented a low-power pairing process that should limit the possibility of eavesdropping, and thus key recovery. However, as not all Z-Wave devices are portable, overrides have been implemented that foil this protection. As the standard does not mandate encryption support, it can safely be assumed that, based on the experience with ZigBee and KNX, vendors will only implement the bare minimum needed to get their products to the market. This leaves Z-Wave networks vulnerable to replay and eavesdropping attacks.

As with the ZigBee Touchlink Commissioning, device stealing is also possible with Z-Wave – the identity of the central controller unit is not verified by a joining device, so it's possible to get a device to join a malicious network. Besides those threats, implementation errors have been found in door locks that allow an attacker to control the lock and preventing the lock from reporting its state to the central controller unit.

## KNX

KNX is a popular standard in Europe. It is an open EN and ISO standard and the convergence of three previous standards: the European Installation Bus (EIB) to which KNX is backwards compatible, the BatiBUS, and the European Home Systems Protocol (EHS). KNX (spoken Konnex) was created in 1999 by the KNX Association in Brussels with the aim to provide a new and commonly defined one-single-standard for field bus applications in homes and buildings. The association is also responsible for the certification of KNX products. KNX is a bus system for home and building automation.

Traditionally all devices are connected and exchange data over a shared bus. A wireless transmission, the KNX RF+ protocol, is one of the used transmission modes supported, as are twisted pair cabling. KNX is one of the

systems used that do not include any specific security measures. This results from the fact that by using cabling as the transport medium, direct physical access to the premise is needed for an attack and therefore security for the KNX system was considered a minor concern. But by adding the radio RF+ protocol, this no longer holds true.

According to KNX material, "It is quite unlikely that legitimate users of a network would have the means to intercept, decipher, and then tamper with the KNXnet/IP without excessive study of the KNX Specifications. Thus the remaining security threat is considered to be very low and does not justify mandating encryption, which would require considerable computing resources." (KNX Association 2013c, p. 12). KNX therefore provides a good example of a home-automation vendor trusting the "security by obscurity" principle.

There is a draft version of the KNX standard that addresses these issues and adds security measures. However, this draft version is vulnerable to DoS attacks, and the security of the communication depends on the secrecy of key material in non-tamper resistant hardware, as well as short message authentication codes. Currently there are no devices that support these security features and, because the standard is still in draft state, no further details have been provided.

# The more devices we connect, the more opportunities there are for cyber criminals.

## Conclusion

It's no surprise that the tech industry and the public are falling head-over-heels for the possibility to connect everything, from our city infrastructure to our toothbrushes and our livestock.

The more devices we connect, the more opportunities there are for cyber criminals. By getting carried away by the opportunity tech-

nology brings, we are charging ahead without considering the risks, and without securing the technology. We did the same when we developed our critical infrastructure in the 1970s, and we're repeating our mistake now with the IoT, but on ten times the scale. There are critical vulnerabilities at the very core of many IoT networks. Until we can resolve these issues and create new, secure protocols, IoT hacks will increase exponentially in terms of volume and severity.



People spend  
over 700 billion  
minutes per month  
on Facebook.

Research by Facebook



*The Internet is full of temptations.  
Can your users resist them?*

The Internet is one of the most useful resources in the office – but only if you can manage the potential issues:

- » Productivity losses due to employees spending time on sites with little work-related content
- » Security risks: from unsecure sites and from legitimate sites that have been compromised
- » Bandwidth losses from people downloading large files or watching streaming media.

Run the 30-day trial of GFI WebMonitor to find out exactly how your Internet connection and remote machines are being used and what security risks you are exposed to.

Quality web filter

Comprehensive web security

Highly competitive pricing

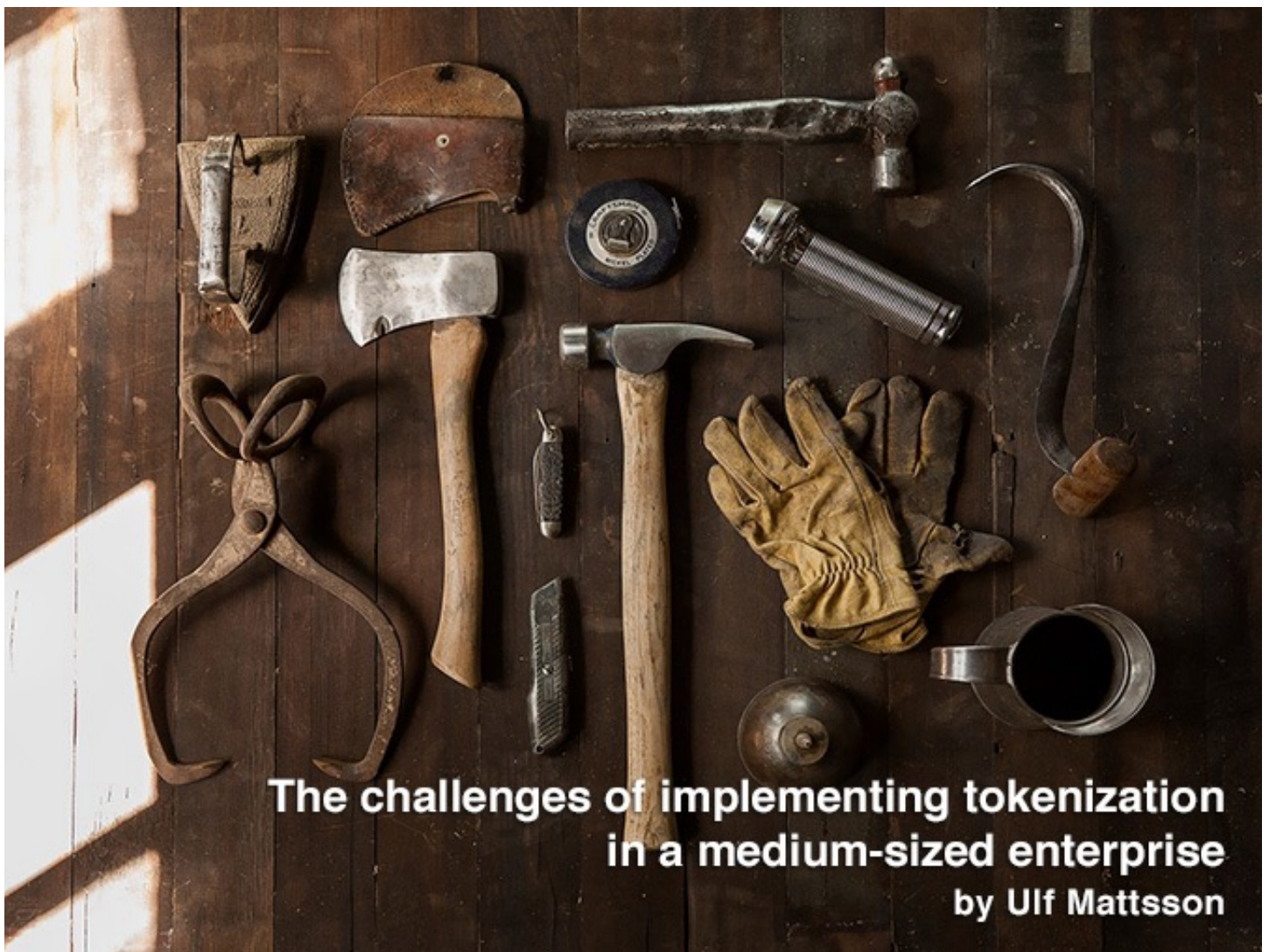
Thousands of customers

Download your free trial from <http://www.gfi.com/webmon>



**GFI WebMonitor**<sup>TM</sup>

Web security, monitoring and Internet access control



## The challenges of implementing tokenization in a medium-sized enterprise by Ulf Mattsson

We have seen a concerning pattern in the recent data breaches, including the breach at the Internal Revenue Services (IRS) and other US government agencies, in that the primary target was Social Security Numbers (SSN) and other Personal Identifying Information (PII). Criminals typically started by stealing data from smaller, less protected organizations and then used that data to attack larger but better protected organizations.

Organizations handling SSN and other PII should secure all sensitive data across all data silos, but medium-sized enterprises in particular face the following challenges:

- In-house resources with limited budget for IT security
- Traditional IT security mindset and skills
- Less flexibility to customize security and IT solutions
- Fewer compliance audits driving security posture improvements
- Extensive use of cloud services
- Holding data attractive to attackers targeting partners elsewhere in the data flow.

Businesses in this position should adopt modern data protection technologies to thwart attackers targeting less protected enterprises as the first step.

### **Risk and breaches**

Many big name big data breaches have hit headlines over the last two years but little attention has been paid to the "main street" breaches that account for 62 percent of the 34,529 known computer security incidents every day in the U.S., according to Travelers.

Breaches of small and medium-sized businesses without the technological advantages



that larger enterprises have often do not even realize they have been attacked until the breach is identified by a third-party. “These things are stressful—they’re a wild pain in the butt... it’s a small and medium-sized company killer,” according to Travelers’ Timothy Francis, Enterprise Lead for Cyber Insurance. “In proportion to the size of the companies, the expenses can be pretty big.”

### **Lack of resources**

There is much evidence that while most organizations are aware of the technology solutions that help improve performance and outcomes, many do not have the resources necessary to address their security and compliance concerns. According to TeamLogic IT’s

President Stewart Paul, of the 86 percent of medium-sized companies that have internal IT staff, these teams tend to consist of generalists with neither the expertise nor ongoing training and certification in newer technologies and security areas or industry compliance requirements.

### **Solutions for the extended enterprise**

To secure against breaches medium-sized enterprises need to look for data security that can secure payment card information (PCI), healthcare and privacy data, including SSN, names, addresses, etc. and select solutions that provide multiple protection options such as coarse and fine grained encryption, vaultless tokenization, masking, and monitoring.

To secure against breaches medium-sized enterprises need to look for data security that can secure payment card information, healthcare and privacy data.

### **Tokenization**

Tokenization is a reversible security method that replaces sensitive data with fake data that looks and feels just like the real thing while making it worthless to potential thieves. Tokenization can provide equal or better security than encryption, while retaining the vital usability of data for analytics and other business processes.

Flexible, format-preserving token types, including numeric, alphanumeric, date, time, address, and other structured tokens can be created with “bleed through” with parts of the original data exposed for business purposes, preserving privacy when applications require only part of the sensitive data for processing.

Next generation tokenization eliminates all of the challenges associated with standard “vault-based” tokenization – no stored sensitive data, no performance drains and no scalability limits – and offer high performance and unlimited scalability with the fast creation of new data tokens and quick recovery of the original data when needed.

Medium-sized enterprises that require solutions to scale linearly and increase throughput as their business requirements demand should look for flexible deployment in a distributed environment, including on each node in an MPP system, or in a central topology to allow optimized performance and security for each unique use case.

As part of a comprehensive solution, platform-agnostic tokenization capabilities can be leveraged throughout a heterogeneous enterprise and solutions should support cloud environments, a wide range of operating systems and databases, and in some cases EDWs, Mainframe and Big Data platforms.

### **Security administration**

A diverse set of functions is needed to protect sensitive data across heterogeneous environments throughout the enterprise. Solutions that provide central security policy management integrated with distributed protection points and enterprise key management for encryption offer easier, cost-effective, controlled data protection across different platforms.

Security Officers can take a "separation of duties" approach to apply automated protection attributes that define the proper data protection method to make data unreadable and to control what type of access to the sensitive data is given to the various groups of users.

For example, database administrators will not be able to view encrypted sensitive data in the clear but will be able to continue to perform their responsibilities in administering and optimizing the database.

### **Use of cloud services**

Cloud services often offer dramatically reduced overheads and increased flexibility over traditional solutions for stretched medium-sized enterprises. However, corporate risk management policies, privacy standards and compliance concerns create numerous data security challenges for businesses that are increasingly relying on cloud services that are holding more of their sensitive data.

Cloud data protection gateways easily leverage tokenization and encryption to transpar-

ently isolate and protect sensitive data before it gets to the cloud and offer activity monitoring, including cloud-based big data, databases, or applications giving businesses the freedom to use any type of private or public cloud service without the risk of exposure.

### **Conclusion**

Tokenization can enable responsible data management, analytics and monetization of PII to medium-sized enterprises while keeping the data secure.

Medium-size enterprises should look for solutions that provide a comprehensive path beyond the duties of due care required by industry regulations to keep customer and employee data and their brand reputations secure.

As Gartner put it in their report covering enterprise and cloud data protection and data access governance solutions, "Organizations that have not developed data-centric security policies to coordinate management processes and security controls across data silos need to act."

Ulf T. Mattsson is the CTO of Protegrity. Ulf created the initial architecture of Protegrity's database security technology, for which the company owns several key patents. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's Research and Development organization, in the areas of IT Architecture and IT Security. Ulf holds a degree in electrical engineering from Polhem University, a degree in Finance from University of Stockholm and a master's degree in physics from Chalmers University of Technology.







# ARE YOU ADEQUATELY PROTECTED AGAINST DDoS ATTACKS?

**DOSarrest's fully managed, cloud-based DDoS protection service guarantees website availability and keeps attackers out!**

Traffic scrubbing centers in  
**London, NYC,  
LA and Singapore.**

DOSarrest has been  
**protecting websites against  
DDoS attacks since 2007**

DDoS attacks are larger and more sophisticated than ever before. It can paralyze your website, leaving you unable to process transactions, accept payments, and disseminate information. A combination of attack methods can lead to data loss, ID theft, and fraud.



US/CAN Toll Free: **1.888.818.1344** \* Press 1 for Sales

UK Free Phone: **0800 086 8812** \* Press 1 for Sales

Singapore Toll Free: **800 - 101 - 1796** \* Press 1 for Sales

Email: **sales@DOSarrest.com**

**Head office:**  
Vancouver, B.C., Canada





The industry approach to detecting threats is inherently reactive, ceding the first-mover advantage to the cyber criminals. Defenses – based on signatures, reputation lists and blacklists – are only designed to recognize threats that have been previously seen. This means someone needs to be the first victim, and everyone hopes it's not them.

We keep doing the same thing over and over, expecting different results. The security industry has put a massive effort into delivering signatures faster and faster, trying to close the gap between when a new threat is detected to when the corresponding new signature is delivered.

But moving faster hasn't made us demonstrably safer. Instead, it has led to more nimble attackers, who easily create and hide their exploits in an infinite number of ways.

The key to understanding the value of signatures is to understand their weaknesses. Signatures are valuable for detecting large-scale commodity threats, such as the command-

and-control communications of botnets, automated crawlers and vulnerability scanners that scour the Internet.

But the signature model falls flat with attackers who value stealth over the number of systems they control. And unfortunately, these more sophisticated attackers are more apt to think strategically and can pose a significant risk to organizations.

Attackers can always change malware – requiring a new signature – but they can't change what they need to do to achieve their goal – spy, spread and steal from the victim's network. And those behaviors can be observed, giving organizations real-time visibility



## Custom-made malware

Most malware is unique to the organization that received it, which means it won't be caught by signature-based solutions. According to Verizon's 2015 Data Breach Investigations Report, 70 to 90 percent of malware samples have characteristics that are exclusive to the targeted organization.

Attackers aren't handcrafting malware – they use the same malware and alter it just enough to throw off signature-based defenses.

Malware signatures work by creating hashes of a known bad file.

Attackers simply add a few bits to a malware file to change the hash so it's not recognizable as the same malware to signature-based security solutions. These changes occur automatically, with no human interaction required. Vast volumes of seemingly custom malware are generated daily in this way.

The key is that while the malware's bit pattern may differ, its behavior is the same. The changes, which are designed to avoid signature-based detection, are superficial.

A behavior-based approach can detect the behaviors in the network, regardless of the attacker's attempt to evade signatures.

# Zero-day vulnerabilities are virtually impossible to detect via signatures, making them some of the most valuable pieces of information to the world's most sophisticated attackers.

## Every day is a zero-day

Attackers also exploit vulnerabilities in software and operating systems. And, like the Heartbleed vulnerability in OpenSSL, these mistakes can lurk silently for years until they are exploited. And unfortunately, prevention systems only protect against known vulnerabilities.

Zero-day vulnerabilities are virtually impossible to detect via signatures, making them some of the most valuable pieces of information to the world's most sophisticated attackers.

Even if a vulnerability and its exploit are unknown, the attack behavior that follows exploitation of the vulnerability generally remains the same.

The Duqu 2.0 malware, identified in June 2015, illustrates the power of using behavior-based systems to detect advanced attacks rather than relying on signatures or reputation

lists. Duqu 2.0 is a new version of Duqu, which is related to the Stuxnet worm.

While Stuxnet was used to damage uranium centrifuges, the original Duqu was more intent on surveillance and collecting information in a compromised network. Like its predecessor, Duqu 2.0 uses zero-day vulnerabilities to compromise its victims.

Duqu 2.0 performs reconnaissance to map the internal network, uses a Kerberos pass-the-hash attack technique to spread laterally, elevates privileges to a domain administrator account, and uses those privileges to infect other hosts.

The core behavior of the Duqu attack creates an indelible marker, even if the bits delivering the malware change. By focusing on the actions that an attacker needs to perform to infiltrate a network and steal data, even the most advanced attacks can be detected using a behavior-based approach.

## Watch your behavior

Think of a sentence as an analogy. Signatures try to give every subject a proper name, while a behavior-based approach focuses on the verb. While the names may change, the malicious action remains the same.

By focusing on behaviors and actions, automated threat management solutions can identify all phases of an attack, including command and control, botnet monetization, internal reconnaissance, lateral movement and data exfiltration – without signatures or reputation lists.

A behavior-based approach can be used to detect activities like internal reconnaissance scans and port scans, Kerberos client activity and the spread of malware inside a network. Data science also can be effective at neutralizing attackers' use of domain-generation al-

gorithms to create an endless supply of URLs for their threats.

Attackers always look for new ways to hide their traffic, and one of the most effective – and fastest-growing – ways is to tunnel their traffic within another allowed protocol. For example, an attacker can use benign HTTP communication but embed coded messages in text fields, headers or other parameters in the session. By riding shotgun on an allowed protocol, the attacker can communicate without detection. Data science also can be used to reveal these hidden tunnels by learning and analyzing the timing, volume and sequencing of traffic.

It's time to jump off the signature hamster wheel and get ahead of attackers with advanced threat intelligence that actively watches and analyzes the behaviors and actions that conceal an attack, and neutralize the threat to your business as it happens.

Oliver Tavakoli is the CTO at Vectra Networks ([www.vectranetworks.com](http://www.vectranetworks.com)).

Want to reach a large audience of security pros by writing for (IN)SECURE?



Send your idea to [mzorz@net-security.org](mailto:mzorz@net-security.org)







# Events around the world



## **(ISC)2 Security Congress**

**congress.isc2.org** - Anaheim, USA / 28 September - 1 October 2015.

Now in its fifth year, (ISC)2 Security Congress 2015 will take place September 28 - October 1 in Anaheim, CA. This conference will offer more than 80 education sessions along with networking and career advancement opportunities.



## **Cyber Security Europe 2015**

**www.ipexpoeurope.com** - ExCeL London, UK / 7-8 October 2015.

Cyber Security Europe at IP EXPO Europe offers expert insight and cutting-edge solutions to help you protect your business from cyber-attacks. You can also learn how to recover more quickly from an attack, and how to minimize the negative impacts.



## **HITB GSEC Singapore**

**gsec.hitb.org/sg2015/** - Hotel Fort Canning, Singapore / 12-16 October 2015.

HITB GSEC Singapore is a three-day security conference where attendees get to vote on the final agenda and are introduced to speakers and each other based on the votes they cast.





# Watchful

Keep IT secret.

Watchful helps keeping information safe from security breaches or disclosure, resulting from malicious wrongdoing or inadvertent misuse.



Are you controlling  
**INFORMATION  
DISCLOSURE?**



## RightsWATCH

data-centric security

A layered Information protection solution to keep data safe and secure regardless of whether it is at rest, 'on-the-fly', or even if it's totally outside your network perimeter.



## TypeWATCH

e-biometrics security

An advanced Persistent Security mechanism, using state-of-the-art e-Biometrics, to continuously verify that the people using your systems are who you think they are.

Do you want to know more? See us today at [www.watchfulsoftware.com](http://www.watchfulsoftware.com)



## Re-thinking security to detect active data breaches

by Gonen Fink

Protecting themselves from a targeted data breach is a top priority for most (if not all) organizations and their IT departments. The concern rises up to the board of directors level, where many have it as a standing agenda item. None of the anxiety is unwarranted, given that the recent breaches at the Office of Personnel and Management (OPM), the White House and even that of the loathsome Hacking Team demonstrated the grave consequences of a targeted data breach.

Most organizations are primarily focused on preventative security and have little or no effective ability to detect an active data breach quickly or accurately. The average attackers' dwell time in the target's network – around six months - is evidence of this deficiency. What's more, according a security report from Trustwave, only 19 percent of organizations discover the breach themselves. Most of the breaches are discovered by a third-party, long after the damage has been done.

The information security industry has been focused on singular events since its inception. Security has been oriented towards a specific

file, a particular network connection, a protocol anomaly, and similar things. However, while identifying those technical artifacts is crucial for preventing a specific intrusion attempt, they usually provide very little context as to the broader attack process, which remains a concern for post-damage investigation.

As a result, an organization may detect and block thousands of intrusion attempts without realizing they are under a targeted attack. To find these attackers requires a re-thinking of some of the most basic tenets of security.



Many of the technologies in place today labeled as “detection” are really some form of “prevention”. Sandboxing, for instance, and Intrusion Detection/Prevention (IDS/IPS) is another form of detection—it is based on statically defined elements from a singular bit of software. The flawed assumption is that stopping a breach involves stopping this one bit of malicious software. It is also flawed in that it is based on spotting something malicious thanks to a known signature or “technical artifact”.

Other systems that are designed to flag anomalies produce an overwhelming number of alerts—hundreds or thousands each day—that are heavily dominated by false positives. Often times, there is an indicator of an active breach among these alerts, but it would be like finding a needle in a haystack to actually locate it.

When you stop to consider it, attackers have a nearly unlimited number of attempts to break into a network. The attack surface is too big and too complex to fully protect, particularly with employees susceptible to social engineering or increasingly clever spear phishing, which makes them often the weakest link. A defender has to be successful 100 percent of the time to prevent a breach. An attacker needs to be successful only once to break into the network. The odds are clearly in the attacker’s favor.

Once inside a network, an attacker should be at a disadvantage. He or she needs to explore and understand the new, unfamiliar network, locate assets and work towards accessing them. All of these activities can be detected, if one knows what to look for and at. Unfortunately, since most organizations do not have an effective way to quickly and accurately find an active intruder, the advantage that should belong to the defender once again goes to the attacker.

Detecting an active data breach requires a blend of new strategies, tools and procedures.

In terms of strategy, there are several things to consider. First of all is the notion that breach detection after an intrusion is viable and necessary. This may seem like an obvious point, but there is already a tremendous amount of self-defeatism in the security field

when it comes to data breaches. Many discussions revolve around more stringent data access, acquiring cyber insurance and developing contingency, post-damage communications and incident response. Most dialogs that I have witnessed do not include breach detection. Organizations need to see that early breach detection is possible and commit budget and resources to it. Companies accept the fact that they likely will be breached, but they have not committed to true breach detection, largely out of ignorance. The ability to find an active data breach and the tools that can accomplish this are relatively new.

Another strategy involves personnel. Most organizations have a limited security operations team, and fewer have trained, experienced security analysts. It’s amazing how many large companies have security responsibilities shared by a small IT team responsible for other operations as well, including networking, storage and applications. To effectively detect a data breach, the organization must be comfortable with—and even value—a certain amount of automation. The “investigate everything” mentality of a SIEM or IPS and other devices must go.

A breach detection system must provide smart, careful analysis to pinpoint a potential breach with a high level of accuracy and actionability. Instead of hundreds or thousands of alerts, a breach detection system should produce only a handful each day to maximize the procedural work done by personnel and minimize wasted time. Team productivity is key so they can spend time on the most important activities.

Personnel efficiency will become an even greater concern over the next several years. There is a shortage of security professionals already, and it will become acute before we enter the next decade. Don’t send a team on a daily wild goose chase. Let them focus on real threats and issues, and give them time to become more proactive.

Finally, another strategy consideration involves shifting from a heavily malware dominated mentality to one that is focused on attack behaviors from a live intruder. While malware is clearly bad, hunting for it does not generally uncover a data breach.

Often, malware is not used in an attack, or its role is not readily discernible. Many security organizations have gone “malware crazy” to the detriment of being able to see the larger threats. It may seem like an obvious point, but the organization needs to prioritize the detection of much more insidious threats.

### **What’s important in a breach detection system?**

To meet the challenges of targeted breaches, a breach detection system needs to be highly accurate and enable an operator to be highly

efficient. In this way, even an IT or networking professional without much security experience should be able to detect an active breach and stop the attack in an early phase.

Breach detection requires four main capabilities to provide the accuracy and efficiency needed by today’s organizations that are trying to prevent theft or damage to assets:

- Broad set of inputs
- Continuous behavioral profiling
- Comprehensive attack detection
- Actionable breach indicators.

Endpoint intelligence can associate processes or applications with the specific network behaviors and also see prevalence—what might be unique or rare for that particular endpoint as compared to the others.

### **Broad set of inputs**

To detect an intruder, it is essential to look at internal connections and operations, administrative tasks and outbound communication. In particular, the internal “affairs” are the most telling for breach activity. This means that breach detection has to start with the network.

While complete coverage of all networks and subnets is not necessary, it is important to view network activity at a deep level to be able to accurately profile the activity of all users, applications and endpoints / devices. This is accomplished by deep packet inspection (DPI) looking at traffic in the core of the network.

Network DPI enables a detection system to strongly associate network activity to specific users and devices. This is critical to enable accurate behavioral profiling of all users and all IP-connected devices on the network. In addition, network DPI provides a great deal of application metadata. For instance, it can show the particular interactions with a database or details about file access, including share and directory information.

A system limited to network flow data can only see Layer 4 information, which might be helpful in seeing massive, noisy activity, but is generally useless in spotting a quiet active data breach. Flow data is limited mainly to IP addresses and ports. A port may give an indication as to the type of application being used, but even that is mostly uncertain, and it lacks important investigative metadata.

Input from endpoints helps corroborate suspicious network behavior and adds important investigative details. It adds to the overall accuracy of determining breach activity and provides actionable details for investigation and remediation.

Endpoint intelligence can associate processes or applications with the specific network behaviors and also see prevalence—what might be unique or rare for that particular endpoint as compared to the others. It can also see if the process or application is new or never before used. All of this information is extremely helpful in boosting the accuracy and efficiency of breach detection.



Breach detection cannot be limited to endpoint details. It's critical to start with behaviors on the network and then use endpoint as augmentative. A view of the endpoint only will tend to miss most of the signals or activities of an active intruder. It may be possible to see a suspicious operation from the endpoint, but it will likely be singular and lack the detail needed to accurately detect a breach.

Of course, most networks are noisy and crowded, perhaps even a bit chaotic, and always in flux. This makes the detection of breach activity even more difficult. Every network generates a huge amount of traffic and data and contains a countless variety of executables on endpoints.

The problem of monitoring such complex environments is significant. Alone, taking in such broad inputs tends to emphasize gathering and storing of all this vast data.

Data science can channel this data into ongoing profiling of users and devices and change the problem from being a classic big data problem to one of machine learning and continuous intelligence. The intelligence is channeled into developing profiles of normal activity and the detection of anomalous activity.

Broad inputs also enable much better detection coverage across the entire lifecycle of a data breach. A data breach consists of many different activities over time, and it is best detected by an ability to see multiple activities and, ideally, how they work together.

Seeing a single anomaly may not provide much value for a fast, accurate detection of a breach. Seeing multiple anomalies that are connected increases the speed and accuracy of the overall detection.

## Most networks are noisy and crowded, perhaps even a bit chaotic, and always in flux.

### **Continuous behavioral profiling**

Critical to successfully detecting breach activity is the continuous behavioral profiling of users and devices. Using a broad set of inputs, the goal is to establish what "normal" looks like for users and devices, by taking into consideration group, role, history, and other factors. This profiling can help reveal which users usually access which machines, for what purpose, where machines usually connect, who performs administrative operations, which machines are servers, and which workstations, and a near-endless number of other important observations.

Profiling must be an automated process based on machine learning. It would be an impossible task to manually build profiles for all users and devices with the associated network and application activity. Keeping them constantly updated and evolved would be an even greater nightmare.

Profiling needs to be built on baselines of what is normal across ever-expanding time

windows: what is the average per minute for the last hour, per hour for the last day, per day for the last week, per week for the last month, etc. This enables detections across vastly different timescales as appropriate, but without burdening the system with the external storage costs that plague other approaches.

Profiles are specific to each company, department, role, individual, season, etc. The profiles must be created from "scratch" - there can be no boilerplate profile to start the process or assumptions about anything. To be accurate they must be built based on real behaviors. While this represents a lot of work, it also means that such an approach cannot be "gamed" by an intruder, nor can the activities stay hidden.

Once a baseline of normal is developed, the system should be looking for anomalous behaviors—significant deviations from the established profiles. The key is to not "cry wolf" with every anomaly. It's important to differentiate between a benign anomaly and malicious one.

## Comprehensive attack detection

After an attacker spreads through the network, there are numerous operational activities they need to perform. To be sure, these are human-led functions. This is not an automated process such as might be used to establish a botnet or create a malware delivery service. Real cybercriminals are behind these targeted breaches, and they are in direct control of each step and sequence of the attack. With comprehensive, accurate profiling from a broad array of inputs, these activities are difficult or impossible to hide.

There are four basic types of breach activities after the initial intrusion. The two most commonly understood are communication and control (C&C) behaviors and exfiltration. C&C is the so-called “phone home” activity that enables an external attacker to learn about the network, orchestrate the ongoing breach and install any software that would be useful in conducting the breach. Exfiltration is the act of moving data out of the victim’s network and to a site controlled by the attacker. This stage of the attack is late in the process, and should obviously be avoided. Breaches should be identified and stopped prior to exfiltration.

Even so, there is tremendous value in deploying a breach detection system even late in the breach process. While exfiltration may have been accomplished, there could likely be follow-on steps to the breach, including addition theft, damage, extortion or leap frogging to a partner, customer/client, supplier or any other entity connected to the victim.

While being the most widely understood breach activities, C&C and exfiltration are also the two activities that can be best obscured by an attacker. Once an attacker has a foothold in the network and owns the “home base,” they can carefully manage these communication processes and hide communication flows in tweets, Gmail messages and other seemingly benign activities. They can sometimes be difficult to spot.

The two other active breach activities are sometimes known as “East-West” activities. They go hand in hand and help the attacker get to know the network and identify assets and key vulnerabilities (reconnaissance) and move to gain additional points of control and to get positioned to access target assets (lateral movement).

Successful breach detection requires seeing the forest and not just the trees. The trees can be seen by a good breach detection system, but discerning a real active data breach generally requires seeing multiple activities, perhaps at different points in the attack lifecycle.

## Breach indicators

Due to the failure of legacy systems to detect an active breach and the well-known frustration of mountains of security alerts, I like to think in terms of “breach indicators.” Rather than simply an alert of something anomalous and without context or confidence, a breach indicator presents a probable indication of a breach with a high level of assurance and with contextual details to show why such an assessment was made. These breach indicators should be based on multiple events or actions, ideally over a span of time.

The detection of advanced attackers within live production networks poses a significant challenge. Many legacy security vendors are attempting to shift their focus to this broadly-recognized problem, but most are ill-suited to the task. Most unfortunately combine both a limited degree of visibility (inputs) with an analysis model that cannot drive highly accurate or actionable alerts. An effective breach detection system learns what is normal on your network through profiling, and then detects active attackers based on anomalous behavior.

Only through a new approach to breach detection can organizations win against a targeted attacker. Prevailing against an attacker is certainly possible, but it requires new strategies, plans and system.

Gonen Fink is the CEO at LightCyber ([www.lightcyber.com](http://www.lightcyber.com)). Gonen was one of the earliest employees of Check Point Software, a member of the core team that developed its flagship firewall product (FireWall-1) and stateful inspection technology. Prior to Check Point, Gonen served for seven years in the Israeli Defense Force’s elite intelligence unit and as a strategic planning consultant to the Ministry of Defense.




# Your Data is Showing... *What's your Plan?*

Enterprise organizations are in possession of more sensitive information than ever before and data breaches are inevitable. The new priority of CISOs around the globe is how to "secure the breach" so organizations can ensure that any data obtained from a breach is encrypted and therefore useless.

Learn how to  
Secure the Breach in 3 steps!

[www.securethebreach.com](http://www.securethebreach.com)



A black and white photograph of a person in silhouette, standing in front of what appears to be a server rack or a similar industrial setting. The person's face is obscured by shadow, and the background is slightly out of focus, showing the structure of the server rack.

## How to prevent insider threats in your organization

by Zeljka Zorz

Time and again, organizations of all sizes and in all industries fall victim to insider threats: disgruntled, malicious insiders - employees, former employees, contractors or business associates - who want to hurt the company or make money, or, more often, bumbling or indifferent employees who accidentally put sensitive company information at risk.

"Insider threats aren't always malicious, there are incidences where they are unintentional and therefore training has a very important role to play in reducing the risk of these unintentional threats," says Greg Day, VP & CTO, EMEA, FireEye.

"The key to getting the training right is making it relevant. Focus on behaviors and aspects that you wish your employees to be aware of - typically companies will include aspects like recognizing social engineering in phishing emails, and awareness of what information they share about themselves and the company online."

This type of training has also the additional benefit of acting as a deterrent to the malicious insider by showing that the business has a strong security focus and outlining repercussions to intentional acts, Day pointed out.

When it comes to preventing malicious insiders from hurting the company, it's important to understand their psychology.

"Insiders are not impulsive. They can move along a continuum from idea to action and therefore demonstrate a discernible pattern of behavior that can be proactively detected," Dr. Michael Gelles, a Director with Deloitte Consulting LLP Federal practice, points out.

"Through the use of analytics, anomaly detection through employee monitoring can proactively identify potential risks. Identifying behaviors that are potential risk indicators such as performance, physical access, compliance, sites visited, size of downloads, printing large quantities of data or emailing large files outside the organization - when correlated using technology and analytics - can identify activity that warrants further inquiry in order to



determine if an insider may be moving towards action," he adds.

But if a person has legitimate access to a certain piece of information, how can any technology prevent the person from leaking the data?

"The first aspect to recognize is that leaking information doesn't cause business impact, it's how it's used once it has been leaked. As such, being able to audit behavior both in real time and post leak can often allow the recovery of information before it is used," notes Day.

"Typically, if a user is looking to steal information, they are often detected by an increase in data being accessed, both DLP and network monitoring tools can identify such spikes away from the norms of the user's behavior. Depending on the businesses perceived value of the information, DLP tools can also be used to control who and how information is accessed. The most critical may be contained to limited use on internal only systems."

Dr. Gelles says that technology is just one half of the equation when looking to prevent, detect and respond to insider threats.

"Today, organizations must develop a holistic approach to mitigating the insider threat that looks at the whole person and specifically at 'what a person does' in the virtual space as well as 'what a person does' in the non-virtual space," he explains.

"An insider threat program is not just about the use of technology to detect anomalous behavior, but also to examine the way an organization does business to include: policies; the employee lifecycle from vetting and hiring to managing and separation procedures; and communications and training - all are critical elements that are beyond just the technology focus of an insider threat program."

Charles Foley, Chairman and CEO of Watchful Software, says that there are two things CISOs should keep in mind when trying to address the problem of insider threats within their organization:

- Go back to common sense

- Carbon's out, Ether and Silicon are in.

"For a hundred years, common sense ruled the flow of information. If it was sensitive, there were very real controls applied to it," he says.

Government agencies, large banks and companies in the 50s, 60s, and 70s had firm control over information by classifying it, stamping/marketing it, and only allowing certain, trusted people to have access to it.

"Then came PCs, email, file servers, and smartphones – not to mention 'the cloud' – and everything fell apart," says Foley.

"Once it became difficult to 'stamp' the words CONFIDENTIAL across a document (or more importantly, it became too easy to create one without it), and you couldn't control information by locking a file room or filing cabinet, people entered the realm of the 'trust paradigm'. Companies began to 'trust' their employees to do the right thing. And this has led to 90% of companies reporting that they've been breached in the last 12 months, over half from insiders either malicious or accidental."

"'Going back to common sense' means using today's technology (which got us into this trouble in the first place) to dynamically identify sensitive / confidential information, automatically mark and tag it, and encrypt it so that only employees with the right level of clearance can open it, regardless of whether they get their hands on the file or not. This is how we apply the hundred-year old term of 'data classification' with today's current technologies," he explains.

"Carbon is out, Ether and Silicon are in" refers to the fact that, as much as you'd like to have your 10,000 employees know and enforce your security policy, it's not going to happen.

"Honestly, it's not their data, and it's not their job," Foley points out. "Read your own Employee Handbook; it's a good bet that it clearly states that all data is the property of the COMPANY. And it's likely not in the job description of the salesman, or clerk, or R&D associate to classify / mark and tag / secure data - it's the company's job."

"Consider this: the average 5,000 person company generates a half-million emails daily and over 25,000 files/documents of which about 20%, or over 100,000 items could cause significant loss/damage to the company. Do you really want to trust that to people that have other jobs?" he asks, and advises companies to rely on "Silicon and Ether", i.e. technology and software.

Malicious insiders working in a critical infrastructure environment are a particular worry, because of the devastating problems they can generate.

"In looking at insider threat we must look at activity driven behavior that could result in the exploitation of information, damage to material, sabotage to facilities or targeted violence, not just information in any circumstance," notes Dr. Gelles. "Insider programs should look to mitigate risk surrounding the loss of information and data as well as sabotage and workplace violence."

Insider threats in government and law enforcement are also exceptionally scary scenarios.

"Not only can they leak / disclose massive amounts of harmful information, but they also have a much higher likelihood of access to non-informational, operational systems. Think critical infrastructure, nuclear energy plants, traffic control, waste processing systems, power grids, etc," says Foley.

"For this reason, government and law enforcement are two of the verticals that are not only embracing the 'Go back to common

sense' and 'Carbon is out...' mantras, they are actively pursuing a third, which is: It's not WHAT you know, or even what you HAVE, but WHO you ARE."

Consequently, they are increasingly turning to biometrics to assure the person who wants access is the person they say they are.


"Today's state of the art is eBiometrics, or types of biometrics that don't require hardware - more Ether, less Silicon," Foley explains.

"Today's systems know who you are because of how you interact with the system, your interface patterns, or your geolocation or through a combination of these things. It could be facial recognition married with behavioral metrics, or geolocation cross-referenced with language patterns. Only in this manner can you, with any degree of scale, ensure that the people using critical infrastructure systems are who they SAY they are, and who they are SUPPOSED to be and that's how we're going to be safe in an increasingly dangerous world."

Things are obviously changing, and organizations are aware that they have to address insider threats. According to the results of a survey published earlier this year, currently 56% of IT professionals in the US have an insider threat program already in place, and 78% of those remaining, or 34% of the total, are planning to put one in place this year.

Most of them are also aware of the fact that they have to combine technology, policies, and organization-wide security training and awareness to mitigate insider threats.

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine and Help Net Security ([www.net-security.org](http://www.net-security.org)).



> Visit [www.insecuremag.com](http://www.insecuremag.com)  
> SUBSCRIBE TO (IN)SECURE MAGAZINE



# Introducing **TITUS Classification Suite 4**

Flexible. Powerful. Secure.

---

## The Industry's Most Advanced Data Classification Solution

TITUS Classification Suite 4 offers an unprecedented level of flexibility and control to make your information protection program a success. From advanced data identification to fine-grained policy control, TITUS provides a security framework to protect your organization's most valuable information assets.



For more information visit [www.titus.com](http://www.titus.com)

# ISO/IEC 27001 scoping and beyond

by Rupesh Kumar



The popularity of ISO/IEC 27001 continues unabated, with over 20,000 certifications issued and counting. The primary reasons for its increasing usage are good security ratification, meeting internationally recognized professional regulations, keeping information security as a fundamental of the business, and bringing about structural change in the business processes to accrue security dividends.

For most companies, the key challenges in meeting the standard are: understanding information security management and its nuances, compiling the right resources for compliance, creating an environment of change, and of course, the cost of implementation. However, the ultimate success of meeting the standard depends on how meticulously you implement it.

## Defining the scope

When it comes to implementation, defining the scope is the actual differentiator and the foundation on which success of the certification is determined.

Consider the example of one particular software development firm with around 200 employees and a global client base.

When taking on ISO 27001, they had the option of keeping a global, organization-wide scope, or limiting it only to the software development department, which encompasses their core competency. Restricted scope means cost reduction, while still assisting in winning global clients who consider the ISO/IEC certification as a respectable security endorsement. Though, at first, its limited scope appeared to be worthwhile, the idea was later rejected on advice of external consultants, who pointed out that auditors wouldn't appreciate a narrow scope because it can lead to loopholes in the security groundwork.

For example, the Testing department, although sitting in a separate physical location than the Development department, was part of the agile development process the company implemented, with employees from both departments working in parallel on the same product.



In addition, sales teams with vital internal, external (client related) and commercial information were totally out of the development process. Auditing only within the scope created risk if a security breach happened because of under-developed security processes in departments outside the scope.

### **Audit approach**

The next question is whether to go for an organization-wide single certificate or separate departmental certificates?

Segregating the organization in departments and creating a separate scope for each of them (Development, Testing, Web, Sales and Administration) means every constituent unit gets its own due assurance, which results in process maturity and rigid security.

As each department has its own threat vectors and risk profile, the latter option can work better than a single solution for the entire organization, as each unit needs to be assessed and certified separately.

But potential snags were observed here as well. The Development department and the Testing department were inter-reliant in the sense that the former used services of the latter during the software development lifecycle.

In this case, as per ISO guidelines, since the Testing department was external to Development, it had to be treated just like any other external service provider, which meant additional processes like risk assessment needed to be created between the departments' interface, and this would result in obvious additional overhead.

Still, keeping the true spirit of auditing in mind, every department was certified individually. As a general rule, the best solution for this type of quandary is to create a process chart of the entire organization, determine their interface, understand their inter-dependence, and then decide whether to go for enterprise-wide or individual, department-wise scope. This will enable you to weigh the benefits of audit versus cost overheads.

Segregating the organization in departments and creating a separate scope for each of them means every constituent unit gets its own due assurance, which results in process maturity and rigid security.

### **Asset register**

Your assets are the building blocks that help you achieve your business goals and objectives, and assets must be assessed against threat variables to create a risk profile, and duly noted in the risk register (risk = probability x severity).

Asset identification can get fiddly at times. We know that servers, computers, laptops and data devices are all assets, and so are computer programs like Windows And Office, as well as the files and folders stored on them.

Your email server carrying so many emails with confidential information can also easily be identified as an IT asset. People, equipment and facilities, on the other hand, will all be put down as non-IT assets in the asset register.

But consider this particular roadblock example. A company car was used by people to carry equipment from a nearby facility to the company's head office for repairs. In this case, could we simply categorize the car, the people and equipment as assets and move on? Not really.

The definition says that people, equipment, technology, processes and anything that can be owned, controlled, and creates business value is an asset. Decades ago computers were rated as a top-value asset, today they are not, but the information contained within them is.

If that information is part of a vital process, it becomes even more valuable. The idea is to look at the latent worth of the items and emphasize the processes they provide rather than seeing them as merely hardware and equipment.

Here are a few questions that should be asked to bypass the asset identification road-block.

1. What will be the cost of business disruption if this process is interrupted?
2. How much did it cost to set up?
3. How much will it cost to restore the process in case of a disaster?

Keeping process maturity and information security in mind, the entire procedure of carrying equipment (servers, laptops, etc.) from a branch location to the head office for repairs was identified as an asset rather than the car and the equipment, which are less valuable. This process was entered into the asset register as:

Operating Unit: IT Helpdesk, Process Name: Equipment Repair, Process Owner: Mr. A, Name of Asset: Equipment Movement Method, Classification: Confidential, Availability: High, Asset Custodian: Mr. C, Descriptions of Asset: a brief description, Asset Type: Enlist all hardware and software involved in the carrying out of this process like Car, People (Mr B), etc.

The main downside is the danger of falling into the pitfall of double accounting, which must definitely be avoided.

## Operations security

This is one of the trickiest parts of ISO/IEC 27001 compliance. There are a number of clauses that have been stipulated for securing an organization's operations security, and an entire section (A.12) is dedicated to this. Within this section, requirements A.12.3 (Backup) and A.12.4 (Logging and Monitoring) are among the few that most organizations believe they are compliant with, either fully or partly. But when it comes to demonstrating this, many of them fail, and this is a major obstacle on the road to ISMS compliance.

## Why does that happen?

To use another actual example: a business decided to go for an ISMS audit when they already had the means to make regular back-

ups of their systems database. But during the audit, it was found that some backups were corrupt or ineffectual, and while system event logs were generated and saved because they were widely distributed across the network, there was a considerable delay in detecting suspect events. This happened because of improper planning and a mismatch between what was believed to be on documents and what actually was on them.

The next question was whether the company had secure log-on procedures? (ISO/IEC 27001:2013, Requirement A.9.4.2).

"Yes, we have a well-defined access control policy which is regularly reviewed", was the response from the IT manager. While this was correct officially, when investigating a little deeper, they failed to back-up their claim. Why? Because they couldn't prove that the changes made to domain policies, permissions, user accounts, etc., were being monitored and validated in REAL TIME by a trusted lieutenant. The existing controls lacked automation, and this was an operational risk with the potential to endanger information security.

To sidestep the obstruction, they chose specialized auditing software. In auditing, a major portion of the entire audit effort goes into devising a threat response plan for the assets in light of the risk assessment which, when meticulously done, goes a long way in mitigating risks arising out of internal, external, retrospective, and future threats.

## Conclusion

Although the ISO/IEC 27001 compliance certification by a recognized body is totally voluntary, it is becoming a key requirement requested by contractors and business associates, who see it as a form of information security assurance. So, if the compliance certificate of an organization reads "Company A, Department X", it does not reveal anything about state of the ISMS security in the other departments. If executed meticulously, ISO/IEC 27001 can be a true business enabler, adding an extra layer of trust and confidence between you and your partners.



# CDNETWORKS CLOUD SECURITY

Fully Integrated Global CDN  
with DDos Mitigation and  
Next Generation, behavioral  
web application firewall

[WWW.CDNETWORKS.COM](http://WWW.CDNETWORKS.COM)



**CDNetworks**

*Global Cloud Acceleration and Security*



## Combatting human error in cybersecurity

by Eddie Mitchell

Mistakes are part of life, but unfortunately in cybersecurity operations, mistakes have the potential to be financially devastating to the business. According to a 2014 IBM study, more than 95 percent of cybersecurity incidents are due to human error. It's a staggering number, and one that cybercriminals and nation-state adversaries alike are counting on.

When referring to “mistakes,” even within the context of the information technology field, it can have broad meaning. One of the first things that often comes to mind is poorly secured code or systems misconfigurations—the kinds of errors made by busy programmers or overworked systems and network administrators.

While these kinds of mistakes do play a part in security breaches, more often than not it's a far simpler mistake: innocent errors of judgment that are leaving businesses and government networks exposed to massive data loss and financial ruin.

### **It might be your boss...**

Or it might be his secretary. More and more security professionals are finding that one of the leading consequences of successful cyber

exploitation is the leakage of sensitive data. In addition, innocent users with elevated access credentials are accidentally e-mailing sensitive data to the wrong people or losing unencrypted media or portable devices full of personally identifiable information (PII). Other users are taking sensitive data home with them on thumb drives or putting the data up on file sharing sites so they can more easily access their work from a home office or hotel.

In and of themselves, mistakes like this are usually innocent, and often made by an organization's smartest and most successful people. They have work to do, deals to make, and problems to solve. To a Type-A problem solver on a mission, even good barriers—like the kind security policy makers and systems administrators put in place to secure data and intellectual property—can be perceived as the enemy.



Some may willfully attempt to circumvent additional security protections put in place, while other innocent mistakes can transform them into unwitting accomplices to breaches and data loss that cybersecurity professionals must attempt to defend against.

For example, think about the ubiquitous USB thumb-drive. It's hard to think of a device more beloved by business users for their convenience and simplicity.

Business users love them because they're small, hold tons of data, and they're simple to use. Yet for IT security personnel, they present a serious security risk and challenge to both control and monitor their use. The very simplicity and ease-of-use the devices offer are central to facilitating irresponsible usage and leading to an increased risk of data leakage.

## Going phishing

Other all-too-successful means of exploitation include users falling prey to phishing attacks. An email that appears to be from a friend or a co-worker may be a delivery mechanism via embedded hyperlinks or malware dropping file attachments that can take control of personal computers or redirect users to rogue websites designed to harvest user security credentials.

In spite of mandatory training in corporate and government sectors, every single day, users that should know better will click something they shouldn't and create a situation where they put themselves and their organization's data at risk. It's a simple mistake, and one that can happen in an instant, but it can also provide an attacker with an instant network foothold as part of a multiphase breach of an organization's enterprise security.

Some may willfully attempt to circumvent additional security protections put in place, while other innocent mistakes can transform them into unwitting accomplices to breaches.

## Cleaning up the mess

The combination of both simple user mistakes as well as a highly complex threat environment is that the virtual surface area that security personnel are required to defend is extremely large and continually growing. If security managers and systems administrators simply have to worry about defending network access points or hardening servers full of PII, the threat posed by mistakes would be far less damaging.

What happens when one of your users with high-level access to these same resources sends an unencrypted email full of usernames and passwords to their personal email account? As the interconnection of our work and personal worlds expands, so too does the exploitable surface area of the enterprise, regardless of whether or not they're physically connected.

Luckily, most organizations are doing the right things to get a handle on securing their far-flung digital borders. They're using multifaceted approaches that include user education, security policy, and security appliances that can "sniff out" things like leaking PII or phishing attacks, and give security personnel an opportunity to eliminate the threats before they're able to wreak havoc.

## Orchestrating future security

The missing piece in all of these well-intentioned pieces of the cybersecurity puzzle is something that can coordinate these disparate and often disjointed initiatives into something fast and cohesive. This is important because most security organizations are unable to answer the two most important problems that they face: How do they manage the volume of threats and the speed with which they can execute? For the most part, they can't.

Most organizations are suffering from data overload when it comes to their cyber security operations and incident response. They often lack sufficient human resources to adequately keep pace with the daily influx of detection events, and when real threats are found, they can't respond to them in time to stop sensitive information from being lost. Keep in mind that a timely response and comprehensive mitigation are just the most critical pieces of the puzzle. Organizations must also deal with compliance requirements, auditing trails, and change control.

To ignore the threat in favor of maintaining compliance leaves the enterprise open to attackers. To fall too far the other way leaves an organization exposed to the legal ramifications of not keeping pace with compliance requirements. Neither situation is acceptable, yet organizations in both the public and private sectors must balance these risks every single day.

Some have turned to automation as a means of accelerating defensive measures and reducing response time to threats. It's a reasonable reaction, and one that many successful organizations use in some form today.

The problem with automation alone is that simply bringing the term up in a conversation can often times elicit a knee-jerk reaction of fear and distrust. If simple mistakes and data leakage can cause so much pain, then what about the potential consequences resulting from automation of these flawed existing processes?

In most cases, this is simply an outdated view on automation, and a damaging one. When used correctly, and managed by a highly flexible orchestration platform, automation can do the one thing that every security operations center needs: it can give them the time they need to respond quickly and thoroughly to both internal and external threats.

## The problem with automation alone is that simply bringing the term up in a conversation can often times elicit a knee-jerk reaction of fear and distrust.

Organizations may realize immediate return on investment by leveraging an orchestration and automation platform for SOC teams to facilitate the contextual analysis process via data gathering and reduce human time consumed by low risk and highly repetitive tasks such as opening, updating, and assignment of trouble tickets. In other words, all of the necessary, but time-consuming work that is preventing SOC analysts from spending time conducting more inherently valuable tasks such as adversary and threat hunting.

The more they're able to focus on solving problems, and the less they're bouncing between uncoordinated toolsets and trying to write like Shakespeare in their trouble tickets, the better.

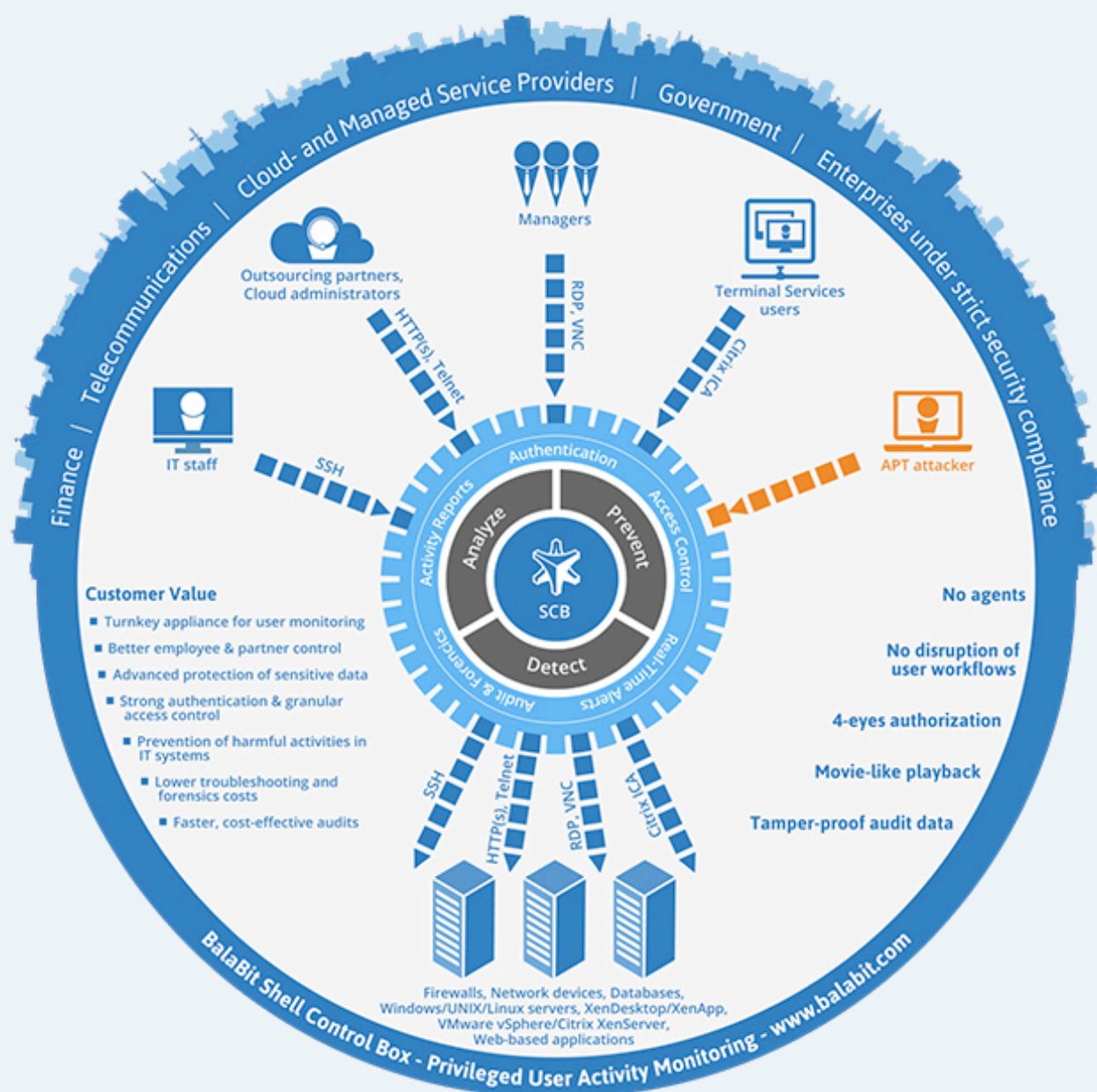
The concept of security orchestration and automation is one that is rapidly gaining ground and is a solution that is intended to directly address both the problems of increasing threat volume and complexity. It also helps address issues of human error and costly "mistakes" as described previously. Nothing introduces error to an organization faster than being overworked and under the gun.

Orchestration and automation together can start eating away at time deficits and giving security personnel more time to make complex decisions. Think of it as a time machine of sorts. A platform that lets you slow the clock down to the moment just after the "boom" occurs, so that analysts and incident responders have more time to decide and act to counter the threat, instead of rushing to gather data and make sense of what just occurred.



Presented at #RSAC:

# TOP 10 Best Practices regarding Privileged Activity Monitoring by BalaBit



Download the "The Essential Guide to Privileged Activity Monitoring" study for free at <https://balabit.com/rsa>.



## Threat intelligence matters to everyone

by Gavin Reid

Threat intelligence is one of the latest information security buzzwords. As is often the case with popular terms, seemingly every security company out there has been shoehorning threat intelligence into their marketing campaigns. Unfortunately, this creates a lot of confusion around the phrase and the underlying concept is lost. This is troubling because threat intelligence is a vital component of effective security, and its importance grows with each new data breach.

Threat intelligence was originally the purview of military and government organizations. Over the years, it has slowly trickled into the private sector, and now smart organizations are investing in it as a viable and effective component of their detection and defense strategies. At its core, threat intelligence is the studying and understanding of attackers to gain actionable insight into the biggest threats to your organization's data security. While this can take many different forms, the underlying concept remains the same.

Hackers achieve their goal by studying security measures and developing a way to circumvent them, but they will often use the same tactics as long as they still work. It is, there-

fore, our obligation to study what tactics are being used against us, so we can detect and defend against them.

### **Threat intelligence creates a more effective, less wasteful security strategy**

There are no "silver bullet" solutions. Threat intelligence doesn't solve all cyber security problems, and it can't be relied on as the only significant means of defense. To combat modern threats, we need of toolbox of different defensive measures.

What threat intelligence can do is give insight into what kind of attacks an organization is likely to experience and what are the current



trends when it comes to cyber threats. This insight is incredibly valuable when it comes to determining how to allocate security resources.

While there are many types of advanced, sophisticated threats out there, they might not be the most prevalent attacks against your network. As such, it is important for organizations to determine what the most pressing threats to their security are and how to defend against it, especially if they are working with limited resources.

Why waste money and time protecting from theoretical attacks when there are actual attacks on your network every day? For example, a company may attempt to protect only against inbound, external hackers, but most recent attacks hinge on compromising internal accounts then using normal office automation tools to facilitate a breach. If the organization is only focusing on attacks from outside their network, they will miss this type of malicious activity inside the perimeter.

If your organization is likely to face Distributed Denial of Service (DDoS) attacks, then it makes sense to invest more in mitigating these attacks. Likewise, if there is a high risk of a sophisticated attack from cybercriminals, then it would make sense for a retail organization to shore up its defenses in and around its point of sale (POS) system.

In order for organizations to do their due diligence, they need to know what assets they have that might be a target for attackers, understand what attack trends are affecting their industry, and detect any signs of that activity on their network. This information can come from a variety of sources: threat feeds, security, or the organization's own internal research. Understanding things like indicators of compromise (IOCs) and the hackers' tools, techniques and procedures (TTPs) will allow organizations to protect themselves intelligently.

However, threat intelligence is only as good as what you do with it. Many companies out there could be handed the golden threat intelligence egg and still be unable to act on it. You need to be able to use the intelligence to detect threats on your network, mitigate them and prevent similar

attacks in the future.

Here is how different areas of organization security can use this information and what benefits they can receive from it.

## **Security operations**

Over the past few years, organizations have been rushing to get as much security data as possible. SIEM, Intrusion Prevention and Detection Systems (IPS/IDS) and security analytics tools are found in most large organizations. An unfortunate side effect of this is that security teams are now inundated with alerts.

On average, organizations receive almost 17,000 malware alerts in a typical week, but only about 4 percent are investigated, according to a report from the Ponemon Institute. Valuable signs of intrusion are simply drowned out by all of the white noise. In order to rectify this problem, security teams need to be able to tune their systems to produce fewer, more accurate alarms.

Threat intelligence can help tremendously in this area. Sometimes it is a simple solution, such as using IOCs to find the needles in the malware haystacks. Other times it can be more involved like coordinating with other security professionals in your industry to identify the motivations and tactics of a common adversary.

Regardless of how you do it, threat intelligence allows you to better prioritize alarms to more quickly detect and triage an attack.

## **Incident response**

All organizations want to resolve cyber incidents fast. Responders often have to start an investigation with very limited contextual data. It could be one alert of malware activity or communication with a known command and control server.

From there, they have to reconstruct the attack by pouring over logs, emails and other data points, and by the time they have identified the scope and methods of the attack, it is often too late.

Threat intelligence provides key context around signs of an attack. If the original alert was based on information regarding a specific threat, responders may know where to look first. If it is indicative of a certain type of malware, they may already know what kind of attackers typically use that tool and what kind of information they may be after.

Having additional context around a security indicator can drastically decrease the amount of time spent on forensic investigations. This consequently allows the incident response team to more quickly shut down an attack and mitigate data loss.

### **Business management**

Far too many people consider threat intelligence to be solely in the realm of the security team. However, it has immense value to Chief Information Security Officers (CISOs) and other executives when it comes to determining the allocation of resources.

Expensive security solutions are a dime a dozen out there, and budget size is a common limitation in cyber security. Instead of reacting to headlines and marketing buzzwords, threat intelligence allows CISOs to purchase tools based on what threats are likely going to target their organization and what essential capabilities the organization lacks.

After all, the attackers became more effective as soon as they started going after specific targets and tailoring their methods to them. If defenders adopt the same tactic and shape their defense to stop likely adversaries, they can become more effective and efficient.

There is often a communication disconnect between security teams and organization executives. Terms like advanced persistent threat (APT), DDoS and social engineering mean little to those outside the realm of cyber security. Threat intelligence can help security managers explain the risks and needs of security in real-world terms, including:

- The motivations of threat actors
- Business risks of a data breach such as the loss of revenue or reputation
- What attacks are other similar organizations are falling victim to or are faced with
- What attack types the company will likely to be faced with on a prioritized basis
- Most importantly, what is needed to maintain an effective security posture.

### **Threat intelligence is a must-have for organizations seeking to protect sensitive data**

Threat intelligence is a force multiplier to the teams that use it. By understanding what threats you are facing and how to detect them, you can use your other security measures more effectively and efficiently.

Contrary to popular belief, this is not a tool exclusive to large, well-financed security teams. In fact, threat intelligence is equally helpful to those who aren't well resourced, because it enables them to get the most value out of what is available to them.

With the right people, tools and intelligence, organizations can significantly improve their security posture. While everyone should keep up with the prevailing trends in cyber security, it is more important to understand the context of your business and what threats you are actively experiencing.

Using this information, implement security practices and solutions that help prevent and mitigate attacks before valuable data is lost, and continue the cycle of gaining intelligence, adapting it to your environment and adjusting security appropriately.

The bad guys have become more advanced, and we can no longer afford to build security against imaginary attackers. Real threats are out there and they capitalize on those who are ill-prepared and unaware of their tactics. Cyber threat intelligence is one important step to leveling the playing field between defenders and attackers.

Gavin Reid is the Vice President of Threat Intelligence at Lancope ([www.lancope.com](http://www.lancope.com)).





## Secure Cloud & Mobile in Minutes

BYOD and Cloud Apps are unstoppable trends. The benefits are huge but you lose control of your data.

Regain control with Bitglass.

IT can enable cloud & mobile, securely.

Employees can enjoy privacy and unencumbered mobility.



### Secure Cloud

- SaaS Firewall for access control
- Full visibility and alerting
- Track data anywhere on the Internet
- Supports any cloud or internal app



### Secure BYOD

- Secure corporate data without MDM or agents
- DLP for sensitive data
- Track data anywhere on the Internet
- Supports Exchange, Office 365, Google Apps etc.

Bitglass deploys in the time it took you to read this.

Sign-up for a free trial at [www.bitglass.com](http://www.bitglass.com)

