

[+] (IN)SECURE Magazine

09 | 2018

ISSUE 59

Success in the cybersecurity industry

The importance of career pathing
in the cybersecurity industry

Securing healthcare organizations:
The challenges CISOs face

Fingerprinting HTTP anomalies to
dissect malicious operations

Introducing

Two new free services!



CertView

qualys.com/certview-free

**Full inventory of your
Internet-facing certificates**

See your SSL/TLS configuration grades
with recommended fixes

Identify the certificate issuer

Track certificate expiration

Instantly upgrade to include internal certs



CloudView

qualys.com/cloudview-free

**Total visibility into your public
cloud workloads & infrastructure**

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

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

Instantly upgrade to run security
assessments on your cloud assets



Table of contents

PAGE 04

The importance of career pathing in the cybersecurity industry

PAGE 06

SECURITY WORLD

PAGE 11

Securing healthcare organizations: The challenges CISOs face

PAGE 14

Fingerprinting HTTP anomalies to dissect malicious operations

PAGE 19

How to keep cryptominers from opening up your IT container boxes

PAGE 22

INDUSTRY NEWS

PAGE 27

REPORT:
BLACK HAT USA 2018

PAGE 35

Vulnerability research and responsible disclosure: Advice from an industry veteran

PAGE 38

Managing migration mayhem: A roadmap for success

PAGE 42

For the love of a good IT book: The No Starch Press story

PAGE 45

EVENTS

PAGE 47

Overcoming the threat of ransomware with zero-day recovery

PAGE 50

Infosec and the future: Dr. Giovanni Vigna on lessons learned over 25 years

Contributors

MATT DOWNING, Principal Threat Intelligence Researcher, Alert Logic
ALEX FAGIOLI, CEO, Tectrade

JOHN PETRIE, Global CISO, NTT Security
ADITYA K SOOD, Director of Cloud Security, Symantec
TIM WOODS, VP of Technology Alliances, FireMon

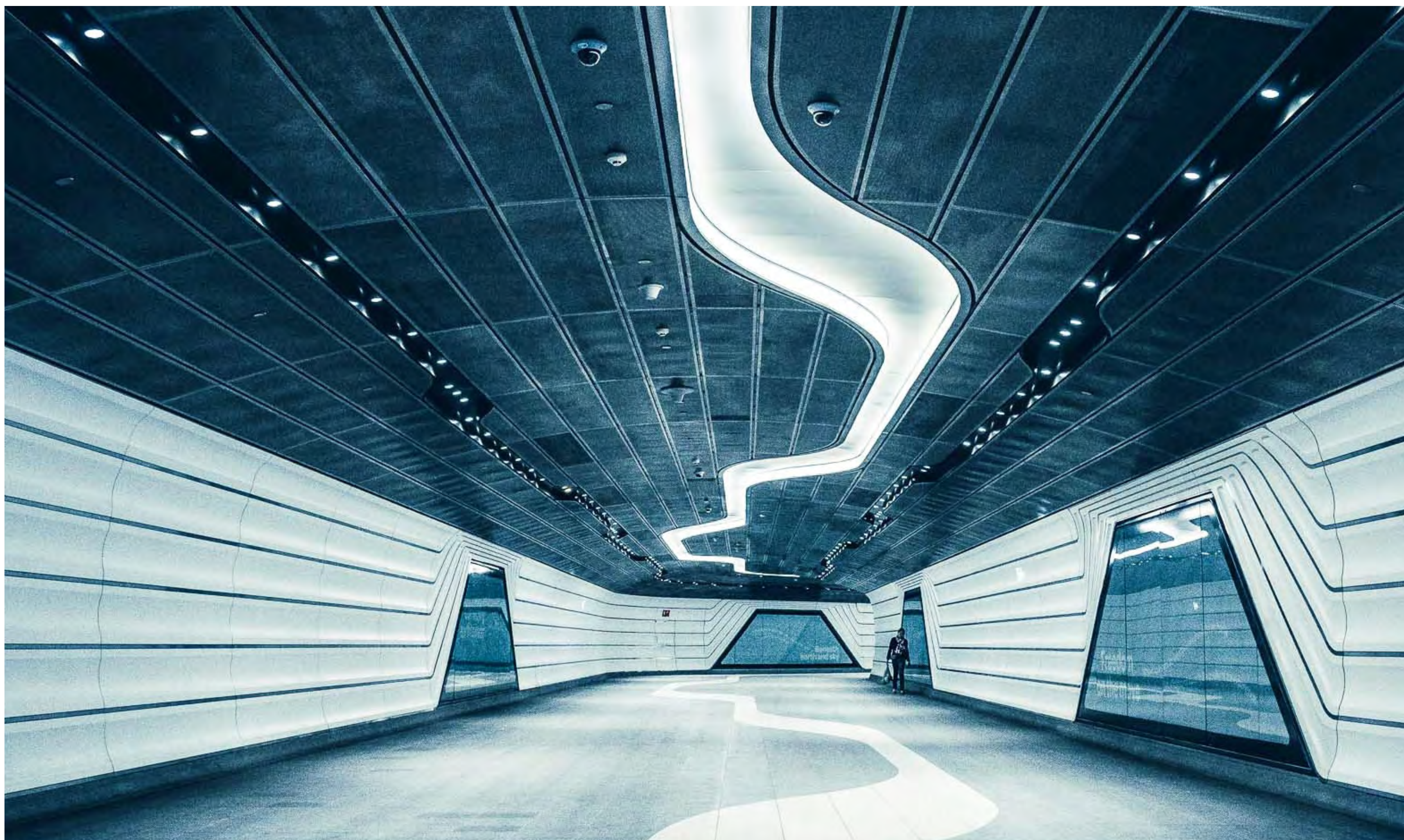
Black Hat USA 2018 photos by (IN)SECURE Magazine and Black Hat.

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

Mirko Zorz
Editor in Chief
mzorz@helpnetsecurity.com

Zeljka Zorz
Managing Editor
zzorz@helpnetsecurity.com

Berislav Kucan
Director of Operations
bkucan@helpnetsecurity.com

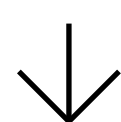


A major issue facing our industry right now is a significant shortage of talented, skilled cybersecurity professionals. Whether that's due to lack of interest or a fundamental misunderstanding of how to gain a foothold in information security, it's a problem that industry professionals around the globe are working to address.

I was recently asked by a group of my peers, "how do I become a CISO and what do I need to do to get there?" This question got me thinking about my own career path and how I didn't begin my career or intend for it to end up being in cybersecurity. At 17 years old I joined the United States Marine Corps, and for the next 20 years I had experiences that shaped who I am today – both personally and professionally – and taught me that with hard work comes success.

The importance of career pathing in the cybersecurity industry

AUTHOR_ John Petrie, Global CISO,
NTT Security



+ While there is no silver bullet to success, I'm convinced it is all about preparation, choices, decision-making and goal setting.

As I set out to embark on my career in cybersecurity, two traits I picked up during my time in the military rose to the top: leadership capability and technical knowledge in computer and satellite systems. Based on my own assessment, I chose to pursue information security as my next career move.

I had to first determine what success looked like for me at the time, and set both short and long term goals. Communications and networking became critical - maintaining your network of contacts will prove beneficial throughout your career. My contacts were fairly extensive, and I managed to land a position with a company that worked closely with the military to train information security analysts.

At this point I had to make another choice – remain technical and focus on the changing technologies, or move towards the management side of the profession. I hedged my bets and began working in both directions – obtaining my Certified Information Systems Security Professional (CISSP) and Certified Business Manager (CBM) certifications, as well as an MBA.

During this time, I became the director of security for an academic healthcare organization, where I was the senior security personnel and was able to formulate new ideas about security management, try new things, and implement security controls in an open environment. Shortly after, I became the Chief Information Security Officer (CISO) for the organization.

Over the next few years I completed additional certifications, as well as my MBA. Additionally, I was offered the position of CISO for a financial services firm growing by leaps and bounds and focusing on

building a security program. I walked through an open door and didn't look back. My new career only continued to expand from there. Over the years, I've applied leadership principles and learned the art of listening to effectively advance the teams I've been a part of and propel my own success.

The need for more information security professionals is growing every day.

+ Whether your success in the cybersecurity industry is leadership-based or tech-focused, there's a path to achieve it – even if you don't have a traditional IT background.

With determination and a willingness to walk through open doors, I was able to take myself from a member of the Marine Corps to CISO of an international security company. Whether you're beginning your career in cybersecurity, or considering a career change, three tips for a successful start include:

1_ Map out a plan and set goals. Figure out what you want to achieve and how you're going to go about doing it. Then set an actionable timeline to follow through.

2_ Complete certifications. The cybersecurity industry evolves so rapidly that keeping up-to-date on certifications is key to success.

3_ Hone in on required skills. Determine which area of cybersecurity you're most interested – technical or business – and develop skills that best align with that career trajectory.

We're all after the same thing: data protection. True success in this field is convincing executive leadership there is value in implementing a security program to benefit the business and support the strategic mission.

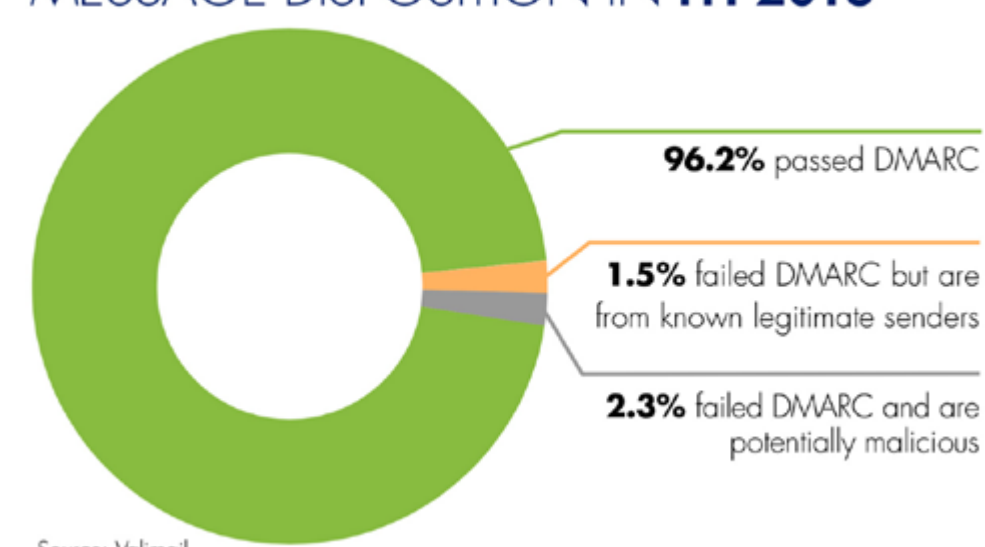
Security world

6.4 billion fake emails sent every day

The Valimail Q2 2018 Email Fraud Landscape shows that fake email continues to be a serious problem, with an estimated 6.4 billion fake emails sent every day.

That total includes only exact-domain sender spoofing, in which senders put a fake email address in the From: field of their messages. This is one of the most difficult to detect and damaging types of fake emails. For example, the FBI recently reported that business email compromise (BEC) costs have reached \$12 billion over the past several years.

MESSAGE DISPOSITION IN H1 2018



Cybercriminals shift tools, tactics and procedures to improve infection rates

Trend Micro released its Midyear Security Roundup 2018, revealing that cybercriminals are moving away from attention-grabbing ransomware attacks to more covert methods intended to steal money and valuable computing resources.

Cryptojacking attempts are making the biggest impact so far this year. Trend Micro recorded a 96 percent increase in cryptocurrency mining detections in 1H 2018 compared to all of 2017, and a 956 percent increase in detections versus 1H 2017. This indicates cybercriminals are shifting away from the quick payout of ransomware in favor of the slower, behind-the-scenes approach of stealing computing power to mine digital currency.

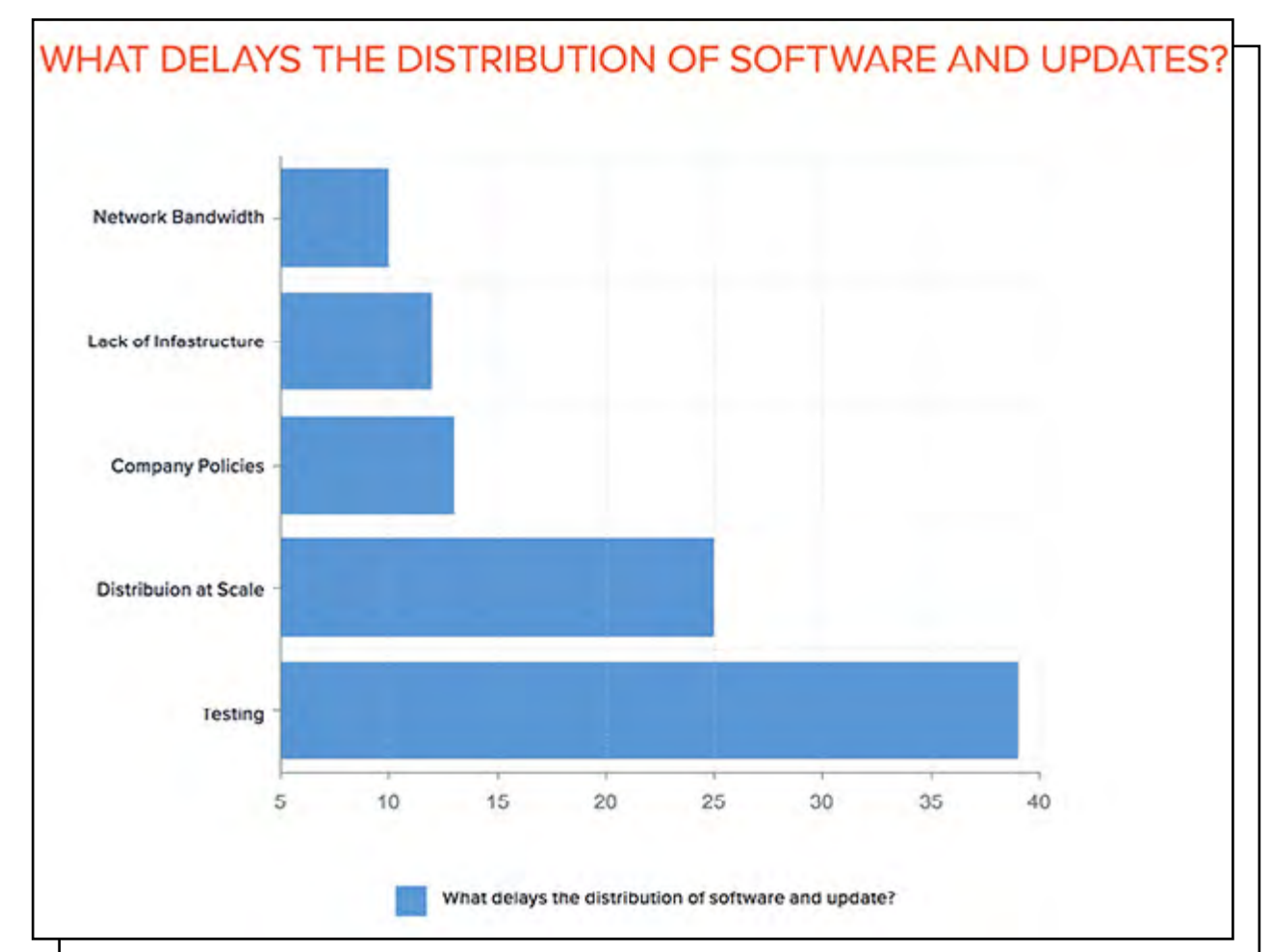
“The recent change in the threat landscape mirrors what we’ve seen for years – cybercriminals will constantly shift their tools, tactics and procedures (TTPs) to improve their infection rates,” said Jon Clay, director of global threat communications for Trend Micro. “Standard spray and pray ransomware attacks and data breaches had become the norm, so attackers changed their tactics to be more covert, using entry vectors not previously seen or used extensively. This means once again, business leaders must evaluate their defenses to ensure sufficient protection is in place to stop the latest and most pressing threats.”

Why do enterprises take a long time to install vital security updates?

More than a quarter (27%) of enterprise IT departments in the US are forced to wait at least a month before installing vital security updates, due to budgetary restraints and overly complex infrastructures. That's according to Kollektive's new "State of Software Delivery" report, which examines the software testing and distribution bottlenecks throughout large organizations.

The report incorporates research from 260 IT managers, leaders and decision makers and highlights how the network security of

US businesses is failing to meet industry expectations. These failings are especially common among large organizations – with 45% of those with more than 100,000 computer terminals waiting at least a month before they install vital security updates.



Global information security spending to exceed \$124 billion in 2019

Worldwide spending on information security products and services will reach more than \$114 billion in 2018, an increase of 12.4 percent from last year, according to the latest forecast from Gartner. In 2019, the market is forecast to grow 8.7 percent to \$124 billion.

“Security leaders are striving to help their organizations securely use technology platforms to become more competitive and drive growth for the business,” said Siddharth Deshpande, research director at Gartner. “Persisting skills shortages and regulatory changes like the GDPR are driving continued growth in the security services market.”

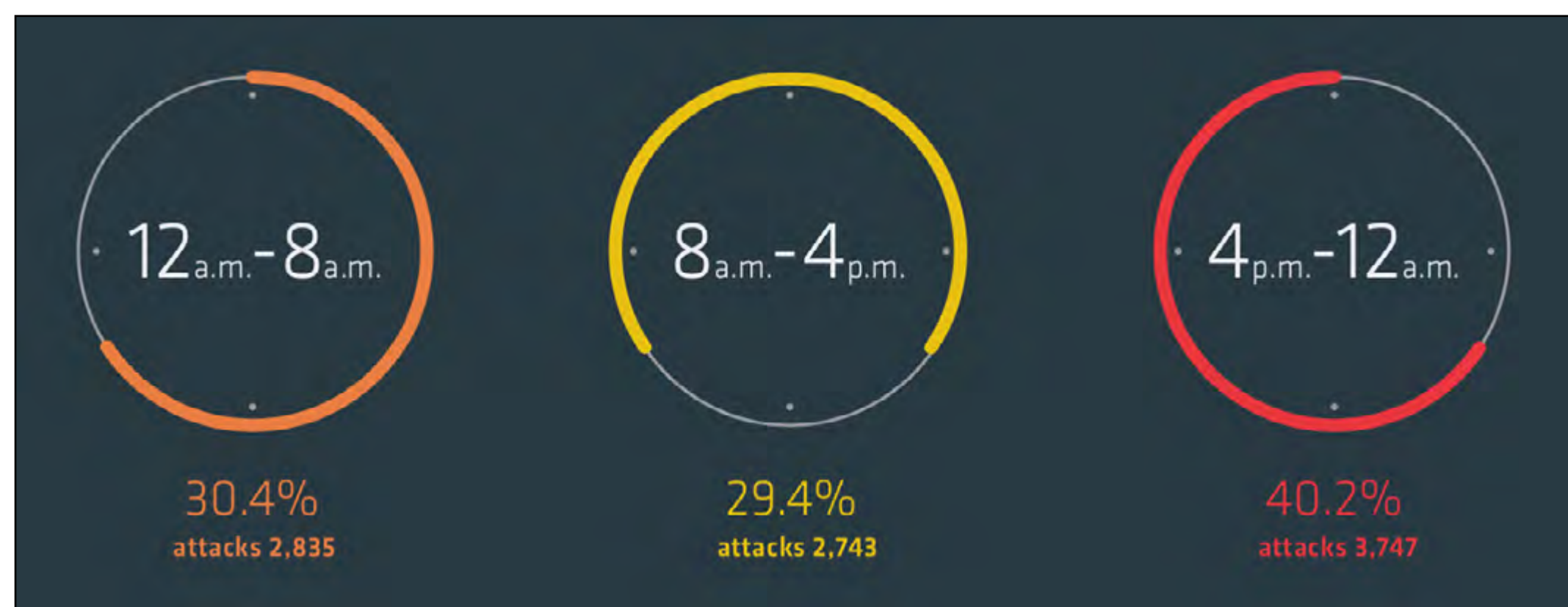
Nearly half of businesses suffered an unrecoverable data event in the last three years

Over 90% of respondents do not consider their organization to be IT resilient and nearly half have suffered an unrecoverable data event in the last three years, according to IDC.

While the majority of businesses surveyed have a cloud, digital transformation or modernization project already planned for the next two years, these same businesses rate themselves as immature on resilience objectives. This gap highlights the current demands on IT teams who are being tasked with cloud and modernization projects even as they struggle to keep pace with basic protection and recovery.

DDoS attackers increasingly strike outside of normal business hours

DDoS attack volumes have increased by 50% to an average of 3.3 Gbps during May, June and July 2018, compared to 2.2 Gbps during the previous quarter, according to Link11. Attacks are also becoming increasingly complex, with 46% of incidents using two or more vectors.



While attack volumes increased, researchers recorded a 36% decrease in the overall number of attacks. On average, there were 102 attacks per day during the quarter.

Half of Alexa Top 1 Million sites now use HTTPS

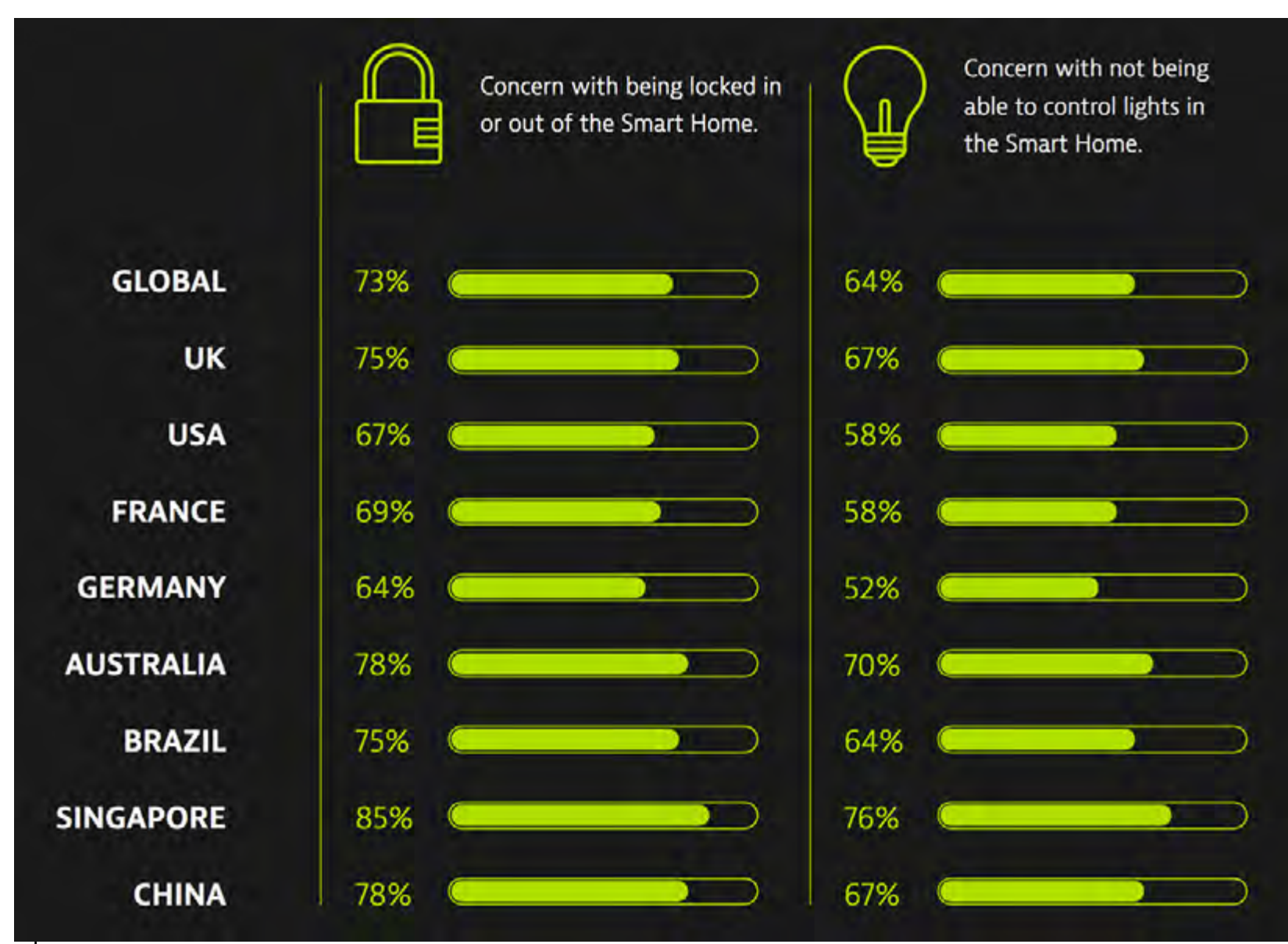
According Scott Helme's latest analysis of the one million most visited websites according to Alexa, 51.8% are actively redirecting to HTTPS. To compare: that percentage was at 38.4 only six months ago.

"The growth (...) is unrivaled in any other security mechanism and if you think about the effort required to achieve this, how impressive it is becomes crystal clear," he pointed out.

IoT failures plague most users worldwide

52% of consumers worldwide are now using Internet of Things (IoT) devices, yet 64% of those have already encountered performance issues – according to Dynatrace. On average, consumers experience 1.5 digital performance problems every day, and 62% of people fear the number of problems they encounter, and the frequency, will increase due to the rise of IoT.

For organizations deploying IoT strategies, these results indicate a critical need to master two things. Firstly, escalating IT complexity, thanks to new cloud technologies, microservices and the pressure to innovate faster. Secondly, the necessity to build



out well-planned IoT monitoring and performance strategies to ensure sound application delivery and a great digital experience.

Data from 316 million real-world attacks in AWS and Azure environments

In evaluating 316 million incidents, tCell found it clear that attacks against the application are growing in volume and sophistication, and as such, continue to be a major threat to business.

The majority of web application attacks are the result of overall scanning for vulnerabilities; however, many others are real attempts to compromise a particular target. Last year, tCell reported that the attack to breach ratio for web applications is 1,200 to 1. This year’s report confirms that ratio is still in effect and identified

Average Time to Patch a Vulnerability (Regardless of severity level)	38 days (from discovery to patch)
Average time taken to patch High Severity Vulnerability	34 days
Average time taken to patch Medium Severity Vulnerability	39 days
Average time taken to patch Low Severity Vulnerability	54 days
Oldest unpatched CVE	340 days

five confirmed XSS breaches. Web application attacks are noisy because hackers are using automated attacks to probe web applications for weak spots. The findings showed that 47 percent of companies were targeted by automated attacks.

2.6 billion records exposed in 2,300 disclosed breaches so far this year

Risk Based Security released its Mid-Year 2018 Data Breach QuickView report, showing there have been 2,308 publicly disclosed data compromise events through June 30th. After a surprising drop in the number of reported data breaches in first quarter, breach activity appears to be returning to a more “normal” pace. At the mid-year point, 2018 closely mirrors 2016’s breach experience but still trails the high water mark set in 2017.

“2018 has been a curious year. After the wild ride of 2017, we became accustomed to seeing a lot of breaches, exposing extraordinary amounts of information. 2018 is remarkable in that the

Threat Vector	Records Exposed
Unknown	1,228,832,055
Inside-Accidental	886,192,311
Outside	535,433,226
Inside-Unknown	40,671,411
Inside-Malicious	1,574,000
Total	2,692,703,003

number of public disclosed breaches appears to be leveling off while the number of records exposed remains stubbornly high,” said Inga Goddijn, Executive Vice President for Risk Based Security. “It’s not easy to characterize 2.6 billion records exposed as an improvement, even if it is less than the 6 billion exposed at this time last year.”



CROWDFENSE

VULNERABILITY RESEARCH HUB

WWW.CROWDFENSE.COM





Healthcare organizations are ideal targets for criminals looking to steal personal and other sensitive information, as the industry is lagging behind when it comes to cybersecurity.

Healthcare breaches involving ransomware increase year over year, but this is just one of the problems information security professionals in the healthcare sector need to face, minimize or, better yet, head off.

Challenges specific to the healthcare industry

To be sure, healthcare CISOs' work is not easy: one of the biggest challenges they face is the open and diverse IT environment of the industry.

“Healthcare systems’ internal IT architecture are comprised of complicated, vast networks that are extremely vulnerable by design. For example, when trying to secure one hospital, CISOs need

Securing healthcare organizations: The challenges CISOs face

AUTHOR_ Zeljka Zorz, Managing Editor,
(IN)SECURE Magazine

to consider and secure a seemingly endless number of data access points crossing all lines of businesses,” says Mark Beckmeyer, Director of IT Security at Binary Fountain.

“Within a hospital’s health IT environment, data can be accessed by a plethora of personnel including, but not limited to: physicians, nurses, clinicians, administrative, information technologists, compliance, receptionists, patients and numerous other medical and support personnel. If the hospital is part of a larger network, other remote campuses may require access to a patients’ personal and protected healthcare information (PHI). Additionally, ancillary locations (i.e., pharmacies, physician offices, insurance companies) need access to patients’ data. In general, the larger the network the more risk that’s associated with trying to keep networks/systems secure.”

Another challenge with fending off targeted healthcare attacks involves the industry’s open IT permission culture.

“Healthcare systems tend to grant multiple people (e.g., students, vendors, etc.) ‘permanent access’ to various systems/networks and these permissions largely go unchecked. Healthcare organizations need to better monitor and limit who they grant IT access to as well as place time-limits on employees’ ability to access certain networks,” he notes.

+ One of the security challenges specific to the healthcare industry is the wide open physical environment intentionally designed into hospitals.

With all the unguarded points of ingress/egress and lack of any real visitor control, these organizations are subject to theft/damage of IT assets,

unauthorized access to patient medical files (both electronic and hardcopy) as well as many other threats to assets and people that may result in a breach of PHI.

Finally, healthcare data can be found in a multitude of medical devices and instruments, and both legacy and modern devices often don’t come equipped with access controls and data safeguards capable of providing the proper level of security and privacy protection.

Preparing the ground

For those that took on the role of CISO at a healthcare organization with a large workforce, a plethora of departments and decision makers, Beckmeyer advises getting executive management attention buy-in, getting to know and understand the organization’s IT environment, supply chain and office.

+ CISOs need to know the entire architecture of a healthcare organization’s IT environment and how it supports each line of business.

“They need to fully understand the environment’s technological composition and nature of all the data contained therein, the process for storage and transmission, as well as the process of all critical and sensitive data and the complete flow of data in and out of the organization,” he says.

Knowing and securing the supply chain is of vital importance, as a security breach of a supplier can have tremendous legal consequences for the organization. “CISOs need to know the security posture of their suppliers, especially where PHI is involved, and to establish and implement a comprehensive supplier risk management program,” he advises.

Beckmeyer also argues that employees must be made to feel comfortable asking questions and/or reporting security situations that arise to the CISO.

To achieve that step, the CISO should put together a clear, concise and comprehensive set of security policies that is easily accessible to the entire company and, if possible, he or she should conduct in-person, mandated, classroom training for all employees. If it's a large organization, the training should be divided into different departments and/or staff levels so the CISO can provide customized, targeted training with real life examples for each group.

"Security protocol is something that should be discussed on a weekly, if not monthly, basis so the staff is constantly reminded that your organization takes security very seriously," he adds.

Addressing current and future threats

Beckmeyer believes that, in the next five years, CISOs should play close attention to the significant increase in functionality and use of patient portals, IoT technology, continued increase in the number of sophisticated medical devices and the use and

storage of genetic information as vulnerable to potential threats.

+

"CISOs will never be 'ahead of the curve' when it comes to defending incoming threats; however, CISOs should aim to be as close to 'the curve' as possible," he notes.

At the moment, though, data compromise and ransomware are the most imminent threats. The latter especially because healthcare organizations often use a plethora of equipment running a variety of operating systems and software that sometimes can't be patched.

When it comes to defending the organizations against ransomware attacks, Beckmeyer advises establishing a comprehensive security incident response program (SIRP) and investing in a robust data backup and recovery program.

The former can help detect, analyze and identify threats, contain exposure, eradicate the problem and begin the recovery process, and the latter can minimize the depth and breadth of a ransomware attack.

↓

"The SIRP requires an enormous level of effort to develop with the need for frequent training and testing (incorporating real life scenarios) to ensure the maximum potential for successfully combating a ransomware attack," he forewarns.

"The data backup and recovery plan should be directly based on a thoroughly conducted business impact analysis (BIA), which will help determine the accurate restoration sequences and timeframes of the hospital's critical clinical and business functions, as well as their supporting IT operations. This BIA will provide the needed information that will allow the CISO to select and adopt the correct recovery strategy on which the data backup/recovery plan will be based."

Fingerprinting HTTP anomalies to dissect malicious operations

AUTHOR Aditya K Sood, Director of Cloud Security, Symantec

Cyber criminals have adopted a number of techniques that abuse the Hypertext Transfer Protocol (HTTP) and result in traffic anomalies.

Cyber criminals are building botnets for conducting cybercrime across the Internet. Botnets are operated via the standard protocols used for communication between client and server over the Internet. This article is primarily focused on the abuse and exploitation of HTTP for data exfiltration and Command and Control (C&C) communication.

Encrypted HTTP POST payloads

Many bots transmit sensitive information in an encrypted payload as a part of an HTTP POST

request. On the network, a cleartext HTTP request is observed having an encrypted payload. The bots opt for this technique to send data in encrypted form without using SSL/TLS. It means that the complete channel is not end-to-end encrypted. Nevertheless, if the HTTP POST request is captured, it is hard to decrypt the payload.

Listing 1. The encrypted payload is sent with a “Host” parameter that includes an IP address. This is doubly beneficial. Firstly, as no domain name is used, and no DNS resolution is required, no DNS traffic is observed on the network. Secondly, a direct connection is initiated with the C&C server to transmit content and this IP address can be easily hardcoded in the bot binary.

LISTING 1: ENCRYPTED PAYLOAD IN AN HTTP REQUEST

```
POST /Victory/connect.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:31.0)
Gecko/20120101 Firefox/31.0
```




```
-----  
  
GET /2001uk11/HOME/1/0/0/ HTTP/1.1  
User-Agent: Mozilla/5.0  
Host: [IP Address]:33384  
Cache-Control: no-cache
```

Communication over non-standard HTTP ports

HTTP communication happens primarily over standard HTTP ports such as TCP port 80, 443, 8000, 8080, and a few others. Attackers can use the standard HTTP ports to hide the communication in normal traffic, but that's not the practice followed

by attackers in all bot and C&C deployments.

Listing 3 highlights that the bot is communicating by using HTTP GET with encoded payload and domain name and TCP port “[hostname]:99” in the HTTP “Host” header.

LISTING 3: USE OF
NON-STANDARD HTTP
PORTS FOR COMMUNICA-
TION

```
GET /down.asp?action=install&u=cpmcpm&p=  
2366A64BAA384EA6AB9CEF73E8E2BE12&t =7393  
  
User-Agent: Update  
Host: [hostname]:99
```

User-agent (UA) anomalies

A user-agent string is sent as a part of an HTTP request header that contains information related to the browser, operating system, vendor, software version, etc. Building an anomaly detector by using techniques such as machine learning, or data analytics can result in fingerprinting bot communication over HTTP. Some malware authors hardcode the user-agent string in the binary and data is exfiltrated over the HTTP channel by using

a hardcoded HTTP request. The attackers can use different types of UAs.

Listing 4 highlights some of the UAs used by malware to either exfiltrate data, perform Command and Control (C&C) communication, or fetch malware (exploit code). Attackers can use legitimate UAs or other strings of their choice. On the C&C server-side, some bot fingerprinting techniques can be built using UAs. However, when it comes to detection and prevention technologies, UAs analysis is an important part.

LISTING 4: USER-AGENT
ANOMALIES

```
GET /mandoc/eula012.pdf  
  
Accept: text/*, application/*  
User-Agent: Mozilla/5.0  
Host: [hostname]  
Cache-Control: no-cache
```



```
GET /s/blog_b2afd7fe01019tkf.html
User-Agent: getURLDown
Host: [hostname]

GET /album/w=1600;q=90/sign=862e65d610dfa9ecfd2e52115
2e0cc72/9358d109b3de9c82a5a5fe456d81800a18d84333.jpg
User-Agent: loadMM
Host: [hostname]

POST /releases/index.php
Content-Type: multipart/form-data, boundary=7DD02020A
0D0000
User-Agent: gsa-crawler
Host: ---.---
Content-Length: 226
Connection: Keep-Alive
Cache-Control: no-cache
```

Misspelled HTTP headers

Analyzing HTTP headers for misspellings is another interesting way to look for potential anomalies in HTTP traffic. Attackers hardcode the HTTP request

headers in the malware binary and make mistakes, especially when they are not native English speakers. A number of examples are presented in **Listing 5**. The “Content-Type” HTTP header is misspelled as “Conent-type”.

**LISTING 5: MISSPELLED
HTTP HEADER**

```
POST /sys.php HTTP/1.1
Host: [hostname]
Conent-type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X
Mach-0; en-US; rv:1.0.1) Gecko/20021216 Chimera/0.6
Referer: http://www.gmail.com
Conent-length: 112
```

HTTP version analysis

The presence of HTTP 1.0 in an HTTP requests is another indicator of potential malicious communication that occurs as a result of hardcoding HTTP requests in the binary. The attackers simply add HTTP requests (including an

HTTP header) and issue those requests by opening sockets for network communication with the C&C server. **Listing 6** highlights an example taken from the communication between a bot and the C&C server. Per HTTP standards, the “Host” header is typically used with requests using HTTP 1.1 and not HTTP 1.0.

LISTING 6: HTTP/1.0
VERSION IN USE

```
POST /process.php HTTP/1.0
Accept-Language: en
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Host: [IP Address]
Content-Type: multipart/form-data
Content-Encoding: gzip
Content-Length: 135
Connection: Close
----- Other potential HTTP GET / POST requests to
C&C servers -----
GET /wp-content/plugins/cached_data/w2.exe HTTP/1.0
POST /vbulletin/post.php?qu=cfg&crc32=0 HTTP/1.0
POST /vbulletin/post.php?qu=cmd HTTP/1.0
POST /gate.php HTTP/1.0
```

HTTP resources reference

Another interesting HTTP traffic analysis technique consists of looking into the web resource being referred in the request. The analysis of the resource can reveal the source of the request (a legitimate

client or a malicious program). **Listing 7** highlights a few samples taken from the communication between a bot and a malicious server. A random resource name with additional data could result in fingerprinting of potential anomalous traffic.

LISTING 7: HTTP WEB
RESOURCES LAYOUT

```
GET /1799.asp
GET /3955.html
GET /20111230.jpg
POST /boi854tr4w.php
GET /6K8gL8.html
POST /~bars/cgi-bin/qfa.cgi?20120311_06:44:06.bin.
FFFFFFFFFS
GET /XEuPCLrf?e
```

→ Conclusion

To detect malicious communication in network traffic, it is essential to follow a two-step process:

1_ Use algorithms to detect anomalies in HTTP traffic.

2_ Use the detections to correlate the indicators to gain insights into malicious communication involving compromised hosts. Correlation of indicators obtained from HTTP traffic anomalies unveils the true nature of malware and highlights C&C operations and data exfiltration. Without correlation, it is significantly harder to detect and prevent attacks.





In “real life,” containers are about simplifying things. We buy Tupperware to store food. We use garment bags for our clothes. To de-clutter our houses, we may take an old box and pack it with family photos, and another for magazines, and another for DVD movies we never watch anymore, and so on.

In technology, containers bring the same value of simplification, as they allow organizations to run virtualized applications in an isolated “single package” that contains all needed computer code, configurations and dependencies. Containers are created from images – reusable static files with system libraries, tools and other components – that essentially serve as a “mold” capable of producing multiple containers.

Containers were initially used for testing, but IT teams have noticed the ease and efficiency of containers and deploy them in their production

How to keep cryptominers from opening up your IT container boxes

AUTHOR_ Matt Downing, Principal Threat Intelligence Researcher, Alert Logic

environments with growing frequency. They're finding that, because containers are small, a single computer and its host operating system can run a significant amount of them.

+ What's more, according to research from Forrester Consulting, 75 percent of organizations have increased application deployment speed through containers, while 73 percent of them have improved the consistency of deployments and 66 percent are boosting development efficiencies.

Given these advantages, interest in the technology is on the rise: Nearly one-third of companies are spending \$500,000 or more annually on license and usage fees for containers, up from 5 percent in 2016, according to research from Portworx. Kubernetes remains the most popular container orchestration tool, with 43 percent of organizations using it. About one-third of companies indicate that that Kubernetes is their primary container orchestration solution.

But because running production workloads this way is so new, few companies command the skills to secure containers and manage them properly, triggering a "running with scissors" situation. While containers represent a novel, streamlined approach, they require complex orchestration systems that can be difficult to manage without people making mistakes leading to compromises. It's not surprising, then, that the Enterprise Strategy Group (ESG) has found that 94 percent of IT and cybersecurity professionals believe that containerization is having a negative impact on security. ESG reports that nearly nine of ten organizations are either already deploying containerized product applications or plan to start testing or deploying these over the next 12 months.

The absence of a tried and true best practices blueprint coupled with limited internal resources

to successfully manage containers have created an enterprise knowledge gap that is expanding the attack surface of containers. And cryptominers are eager to leverage this: In June, the Kromtech Security Center revealed that cryptominers had exploited 17 malicious Docker containers to earn \$90,000 in 30 days. In February, researchers from RedLock indicated that hackers were running cryptomining scripts on an unsecured Tesla Kubernetes pod.

+ Despite these incidents, containers may eventually fulfill the promise of more efficient security due to their streamlined nature.

An enterprise ecosystem may deploy thousands of containers while only using a dozen or so images to run them. In removing all entry points, dynamic linking, etc., you can "super secure" the images to support a large volume of business-driving containers. If you discover a flaw within an image, you can fix it and then send it back out to a huge container "fleet" – a repair that involves far less personnel resources than with security teams monitoring traditional, more widespread infrastructure.

The aforementioned incidents reveal, however, that cybersecurity remains very much a learning process with this workload approach. Here are two, fundamental reasons why organizations leave themselves potentially vulnerable to cryptomining exploits:

They don't properly authenticate application programming interfaces (APIs). Many container APIs fail to go beyond basic default authentication methods. And, unfortunately, cryptominers find the basic defaults fairly easy to overcome, thus gaining "keys to the kingdom" access to the entire container cluster. If you don't layer in additional, proven forms of authentication, you greatly increase the risk of a compromise.

They don't scan images from remote repositories to "clear" them of malicious, mining code. You can't blindly trust images from an outside source because they could be infected. If you need to use an image from another party, conduct a scan of the image to validate that it's "clean." As the old adage goes, "trust but verify."

Improve container security

In the bigger picture perspective, you can think of coin miners as "canaries in a coal mine" of sorts – their presence in your container ecosystem reveals how readily exposed you are. And if you shrug your shoulders and dismiss cryptominers as a relatively small concern since they're not stealing your proprietary and/or sensitive data, you're demonstrating that your "alarm" system isn't working as it should. The key here isn't to focus strictly on kicking out the miners, but fixing the alarms, i.e., issues that allow them to enter the ecosystem. To do that, IT teams should consider the following optimal security "checklist" practices:

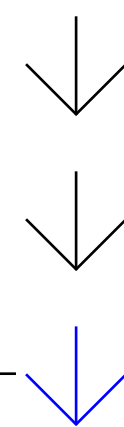
Keep everything simple. Remember that, as with our Tupperware containers, garment bags and old boxes, we're trying to keep things lean and clean. Teams run into problems when they deploy a container to do many different things – act as a web server, a database manager, etc. – instead of "one thing right." If the container takes on a multi-purpose, complex quality, it transforms into a virtual machine with lots of backend vulnerabilities and a widened attack surface. When you limit containers to doing that one thing, working alongside other containers which similarly function in isolation, you reduce the attack surface.

Build an environment of trust. If you pull a container image from a remote repository, you can't know for sure where it originated or whether cryptomining capabilities are "baked" into the image. It's quite common for IT team members to

take a container and leave it running overnight to test workload performance. Over that eight to ten-hour period of time, cryptominers can make lots of currency. It's best to pull images from trusted sources and scan them for malicious code.

Don't expose your underlying container infrastructure or management tools to the Internet. The Internet is arguably the number one attack vector for compromising container infrastructures.

Make sure your intrusion detection capabilities cover containers. Even if you think you've configured this perfectly, you aren't necessarily protected. Your intrusion detection tools should keep an "eye" on your entire container environment so cryptominers can't hide there.



Conclusion

In a sense, we should go about securing virtualized containers just as we do the ones in our home. We seal that Tupperware so our food stays fresh. If the items stored in the boxes are valuable, we put them somewhere they are not easily accessible. Then, we invest in a security system with alarms and alerts that protects everything we have, including the containers.

For modern organizations, vigilant authentication, scans, application simplification, earned trust and ever-watchful intrusion detection combine to deliver the kind of container "alarms and alerts" you need. With this, your containers continue to get the job done, without exposing your enterprise.

Industry world

SailPoint's IdentityIQ extends identity governance for AWS and SAP environments

SailPoint continues to drive innovation with IdentityIQ to help organizations embrace the new frontiers in identity governance, which address the explosion of new users, applications and data driven by digital transformation.

With IdentityIQ 7.3, SailPoint expands the definition of identities beyond humans, providing the ability to govern non-human identities such as software bots, including robotic process automation (RPA) bots.

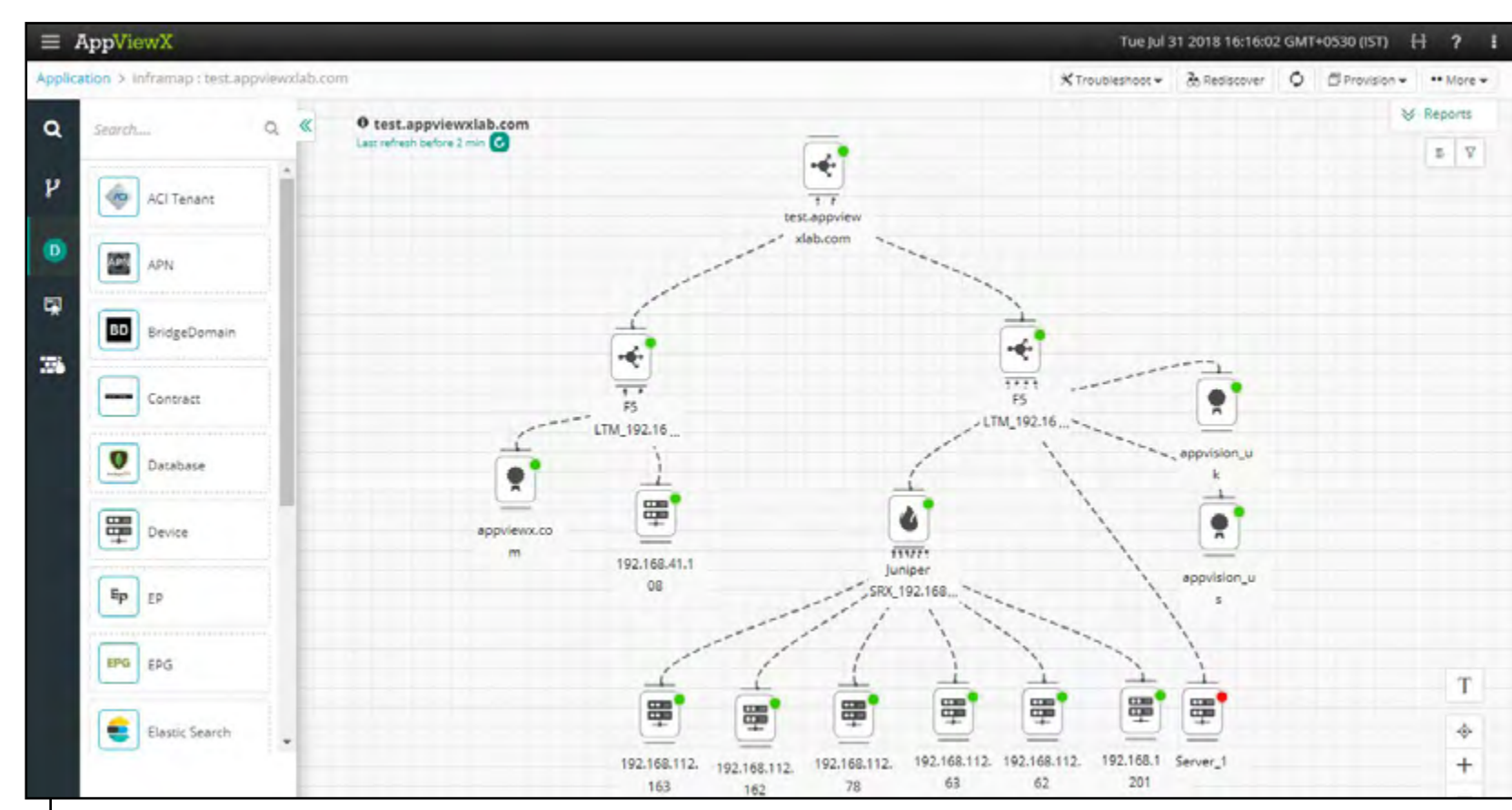
With the new IdentityIQ Accelerator Pack, SailPoint enables organizations to onboard the thousands of applications their business users now rely on into IdentityIQ, accelerating their identity governance deployment and time-to-value.

IdentityIQ 7.3 also deepens the functionality for governing access to AWS and SAP environments, ensuring they are secured in the same way as the rest of an organization's infrastructure.

AppViewX 12.4 takes low-code network automation to the next level

AppViewX announced the launch of AppViewX 12.4. With the new version of the platform, NetOps and SecOps teams can leverage low-code automation on an enterprise-ready platform.

The AppViewX 12.4 release will include more pre-packaged automation workflows and elements to enable service delivery. Automation engineers can access these reference workflows from GitHub. The platform also extends its certificate automation

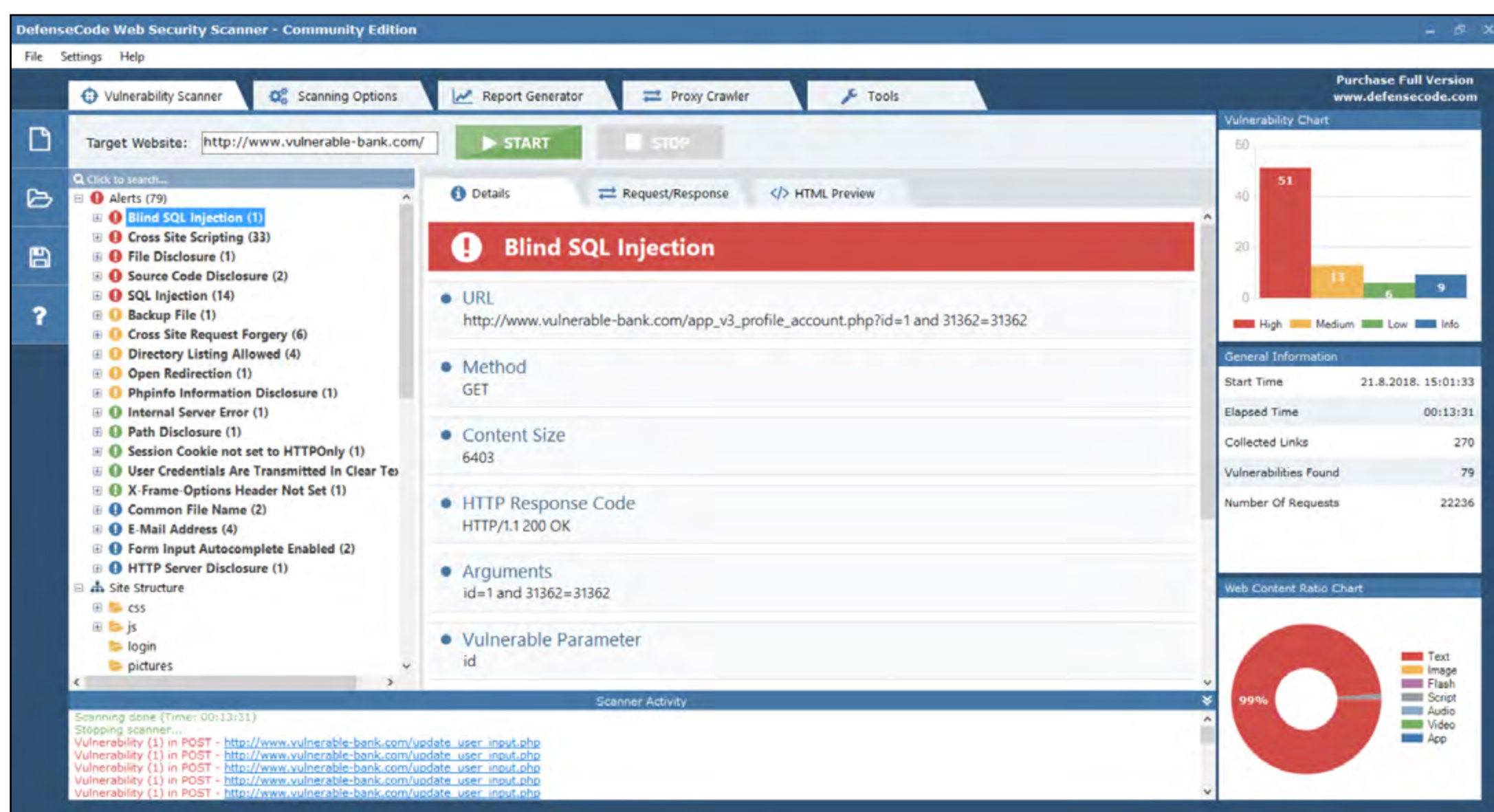


support to include code signing certificates, SSL/TLS certificates on firewalls/web-application firewalls, and IoT certificates.

DefenseCode announces free edition of their Web Security Scanner

DefenseCode is giving away a Community Edition of their Web Security Scanner 2.0 free of charge for personal and non-commercial use. All security scanning and vulnerability detection features available in the full version of the scanner are also available in the Community Edition. There are no limitations in vulnerability detection.

You will be able to scan for SQL Injection, Blind SQL Injection, Cross Site Scripting, Command Execution, Path Traversal, Code Injection, HTTP Response Splitting and 50 other vulnerability types including OWASP TOP 10 and thousands of CVE described vulnerabilities. Moreover, the scanner will even detect if there is a some sort of WAF in front of the web site that you are scanning.



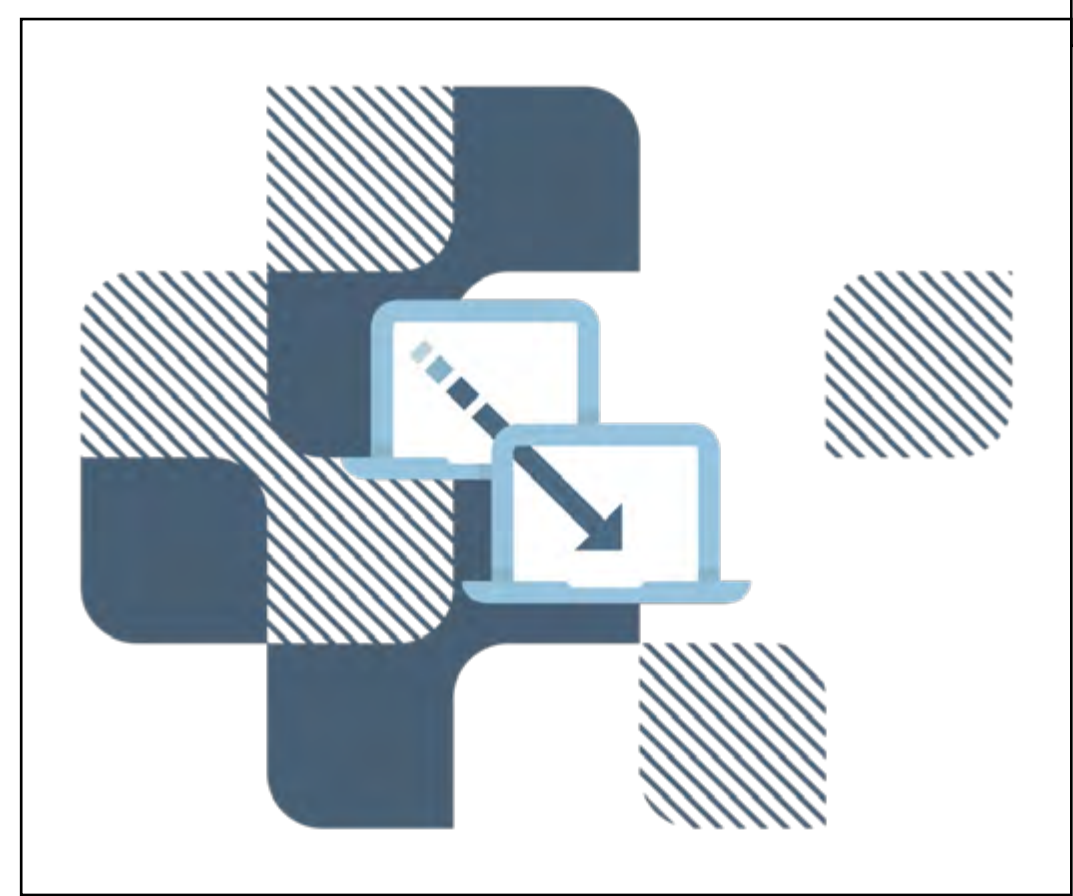
CloudPassage debuts Halo Cloud Secure, delivering security of public cloud infrastructure

CloudPassage announced the general availability of Halo Cloud Secure, which offers protection of public cloud infrastructure, delivering security and DevOps teams a “single pane of glass” view of security and compliance across all of their cloud service provider (CSP) accounts.

The Halo platform already protected cloud workloads and containers. To answer customer demands for a streamlined solution, CloudPassage enhanced capabilities of the Halo platform, now known as Halo Cloud Secure.

Code42's data security platform reduces user downtime and costs for Windows 10 migrations

Code42 announced enhancements for Windows 10 Device Migration. Designed to help organizations reduce risks and costs related to data loss, user downtime and lost productivity, this data recovery solution gets files back into users' hands by prioritizing the migration of files created recently. The new restore-priority capability maximizes the efficiency not only of Windows 10 OS migrations, but also device replacements and tech refreshes.



iStorage introduce new diskAshur range of secure portable HDDs and SSDs

One of the unique and underlying security features of the GDPR compliant diskAshur range is the dedicated hardware based secure microprocessor (Common Criteria EAL4+ ready), which employs built-in physical protection mechanisms designed to defend against external tamper, bypass laser attacks and fault injections. Unlike other solutions, all the drives within this range react to automated hacking attempts by entering the deadlock frozen state, which renders

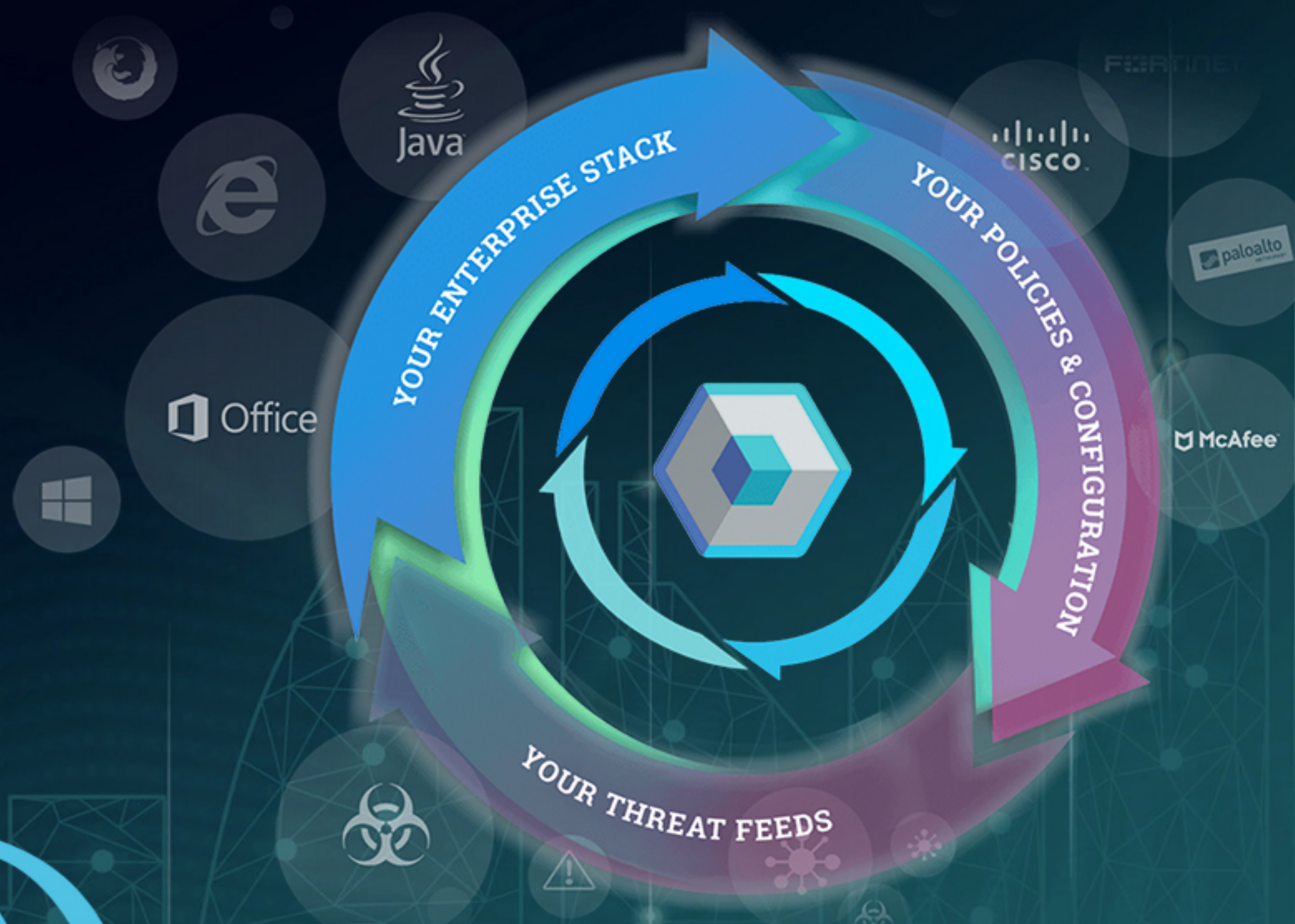


all such attacks as useless. In plain and simple terms, without the PIN, there's no way in!

The diskAshur range is platform/device independent and works across all operating systems including all versions of Windows, macOS, Linux, Android, Chrome, Thin Clients, Zero Clients and embedded systems. The drives will work on any device with a USB port.

CONTINUOUS SECURITY VALIDATION

HOW DO YOU KNOW
WHERE YOU STAND?



NSS LABS

[LEARN MORE](#) →

RapidRatings launches new APIs for risk management

The Risk Management API allows businesses to increase productivity and risk transparency, scale credit and risk management processes, and develop custom insights and analysis capabilities.

Businesses today demand high volumes of financial ratings insight and analysis scenarios to manage changing risk profiles for tens to hundreds of thousands of third parties. The Risk Management API suite automates the data entry and data extraction processes to support a new level of automation, ratings insight, and financial analysis capability.

SnapLogic accelerates SDLC with new DevOps and automation capabilities

SnapLogic announced DevOps and automation capabilities, including new integration with GitHub and support for Mesosphere to automate elements of continuous integration and continuous delivery (CI/CD).

These new enhancements to the SnapLogic Enterprise Integration Cloud provide the company's customer base with self-service application and data integration to streamline and accelerate the software development lifecycle.

Fortanix addresses enterprise blockchain security requirements with private key protection

Fortanix SDKMS eliminates obstacles to blockchain adoption – secure and compliant encryption key management – by delivering security for the generation and use of keys.

Complete key management and key usage policies are enforced inside Intel Software Guard Extensions (Intel SGX) enclaves, ensuring confidentiality and integrity of the policies and private key protection even when in use.

SDKMS delivers HSM-grade security designed for integration into blockchain environments with flexibility of deployment model, application integration with RESTful API support, support for cryptographic algorithms, and policies for key signing and access control.



SentinelOne partners with SecBI to provide threat visibility, containment and remediation

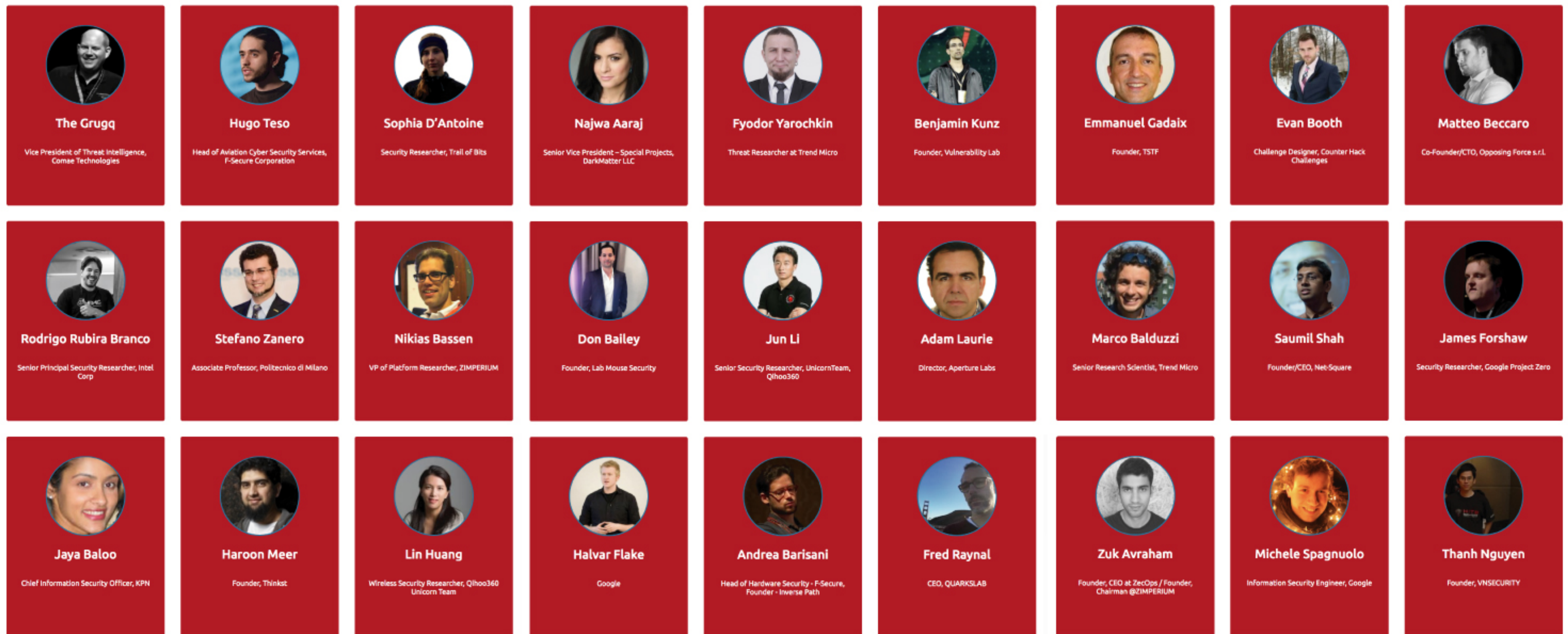
SentinelOne announced that the company has partnered with SecBI. By combining SentinelOne's threat visibility, containment and remediation capabilities with SecBI's Autonomous Investigation technology, security professionals will be able to shed light into every behavior in an organization's network, placing the spotlight on and enabling defense against all incidents that happen and/or involve activities on the endpoint and in the network.



The first HITB Security Conference in China

October 29th - November 2nd @ Kempinski Beijing

Featuring some of our most popular past HITB speakers



REGISTRATION OPENS JUNE 2018

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

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



Scan me

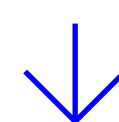


REPORT:

Black Hat USA 2018

Black Hat USA 2018 welcomed nearly 19,000 professionals across the InfoSec spectrum – spanning academia, world-class researchers, and leaders in the public and private sectors. The event's lineup featured content led by security experts who showcased the latest and greatest research currently impacting the industry.

The Black Hat Review Board, comprised of 24 security experts, evaluated more submissions this year than ever before – producing the largest program to date. This year's conference welcomed more than 300 speakers and Trainers across more than 80 deeply technical Trainings and nearly 120 innovative research-based Briefings on stage.



Show highlights

Parisa Tabriz, Director of Engineering and Project Zero for Google, presented “Optimistic Dissatisfaction with the Status Quo: Steps we Must Take to Improve Security in Complex Landscapes” to a bustling Mandalay Bay Events Center, which housed more than 6,000 attendees.

CISO Summit welcomed 200 executives from top public and private organizations for an exclusive, program intended to give CISOs and other InfoSec executives more practical insight into the latest security trends and technologies and enterprise best practices.

Arsenal returned for its ninth year, offering researchers and the open source community the ability to demonstrate tools they develop and use in their daily professions – live. This year's program featured more than 90 tools, including 11 Arsenal Theater Demos and a new space for open-source enthusiasts to work with researchers in a hands-on environment.

Business Hall buzzed with more than 300 leading companies. Attendees were given the opportunity to experience hands on learning, demonstrations and education on the latest products and technologies impacting the industry, as well as deep dive sessions presented by vendors in the Business Hall Theaters.

Community focus

Black Hat is driven by the needs of the InfoSec community - giving back and helping to foster the next generation of security professionals is a priority and Black Hat is proud to highlight some of its most recent initiatives:

New community track: Developed to provide a focus on relevant issues currently impacting the

InfoSec community, presented Briefings spanned careers, diversity, security awareness, health, and more. Insights and solutions from industry experts were provided to help individuals both new to InfoSec as well as seasoned professionals.

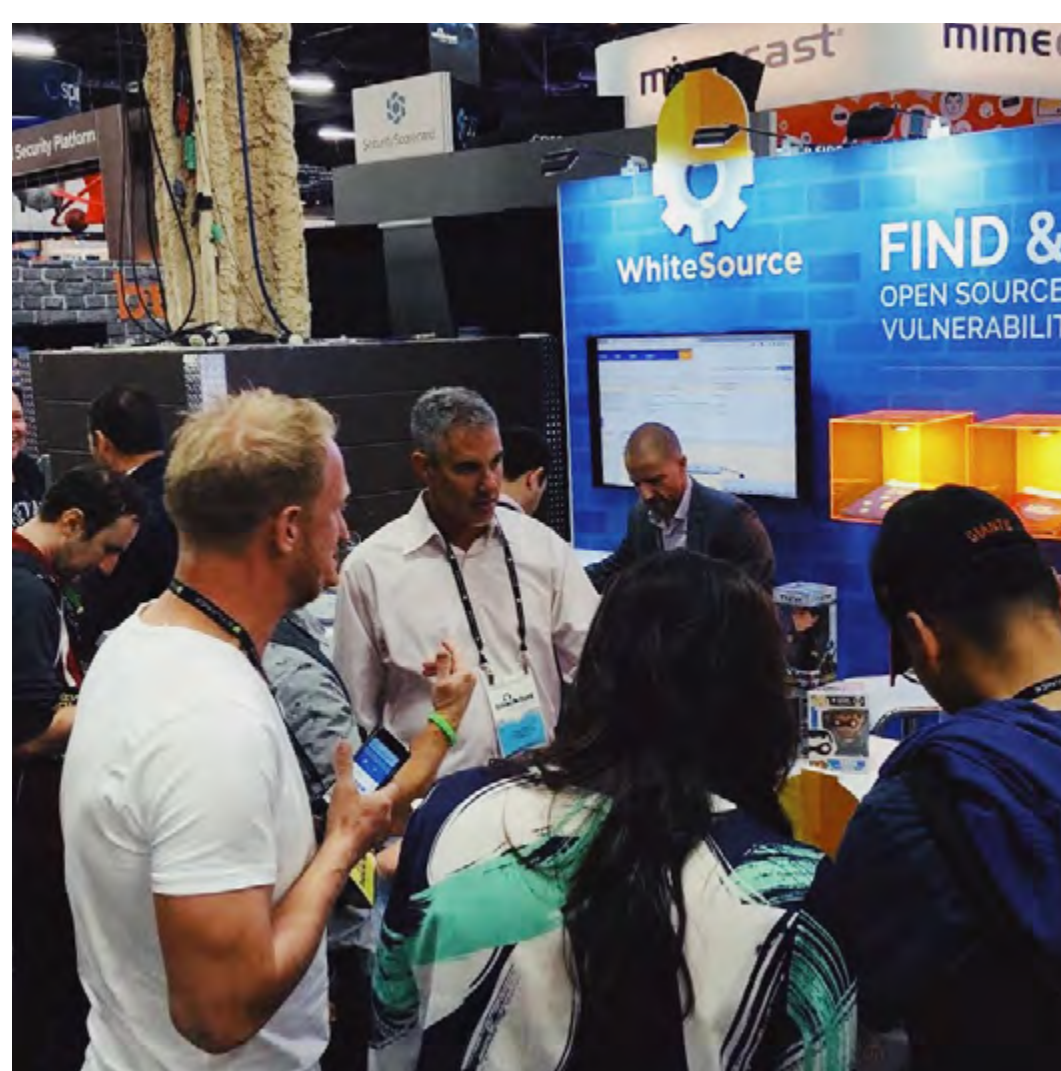
New community programs: Over the years, Black Hat has expanded its community programming to shine light on topics specific to the InfoSec community, as well as welcome a wider range of professionals to the event. This year's offerings spanned scholarship opportunities, workshops, networking, activities promoting health and wellness, partnerships with non-profit organizations and more.

Electronic Frontier Foundation support: For the fifth year, Black Hat is proudly donating \$50,000 to the EFF to continue supporting their important work in protecting civil liberties within the digital world. Black Hat has a strong partnership with the EFF to provide pro-bono legal consultations to security researchers on the legality of any research or data they plan to present at the annual shows.

Scholarships: Black Hat awarded more than 200 Academic Briefings Scholarships to deserving students from around the world. Black Hat and EWF again offered the Female Leaders Scholarship Program to minimize the gender gap among the InfoSec community and give students the opportunity to learn, network and collaborate with the world's brightest minds. Event speakers were also given two complimentary Briefings passes per talk to be given to students of their choice.

HERO corps: Black Hat will be donating all proceeds from its specialized 2018 event t-shirt to the Human Exploitation Rescue Operative (HERO) Corps, a joint project of the National Association to Protect Children.

Black Hat gallery





Qualys provides visibility of inaccessible IT assets

Qualys announced a new Out-of-Band Configuration Assessment (OCA) module that allows customers to achieve complete visibility of all known IT infrastructure by pushing vulnerability and configuration data to the Qualys Cloud Platform from systems that are otherwise difficult or impossible to assess. OCA's expanded data collection approach completes customers' global IT asset visibility by significantly broadening the types of technologies supported by the Qualys Cloud Platform.

An API-based sensor module, OCA enables customers to add metadata from unscanned assets into the Qualys Cloud Platform to gain deeper assessment of configuration, and achieve better visibility of potentially critical vulnerabilities across their full environment.

Security teams strive to minimize risk by securing all enterprise assets from cyber threats. However, a sub-set of these assets may remain at risk due to remote scanning challenges such as inaccessible locations, placement on highly secure disconnected "air gap" networks or with sensitivity to scans. Qualys OCA offers customers a simple alternative method to reduce that risk by assessing the security of these critical disconnected assets via an API that extracts asset, configuration and vulnerability data and delivers it into the Qualys Cloud Platform for inclusion in their overall security and compliance program.

"This new groundbreaking method of data extraction helps customers extend their single-pane-of-glass visibility to all assets, which is a key first step to ensuring continuous security," said Philippe Courtot, chairman and CEO, Qualys, Inc. "As a new addition to the Qualys sensor family, Offline Device Assessment gives customers the ability to broaden compliance programs to include such highly locked-down devices and those on air-gapped networks."

Qualys and IBM X-Force Red help orgs identify, fix most critical vulnerabilities

Qualys announced that IBM X-Force Red will leverage the Qualys Cloud Platform as part of its X-Force Red Vulnerability Management Services (VMS).

As part of an expanded relationship, X-Force Red will deploy the Qualys Cloud Agent and Qualys

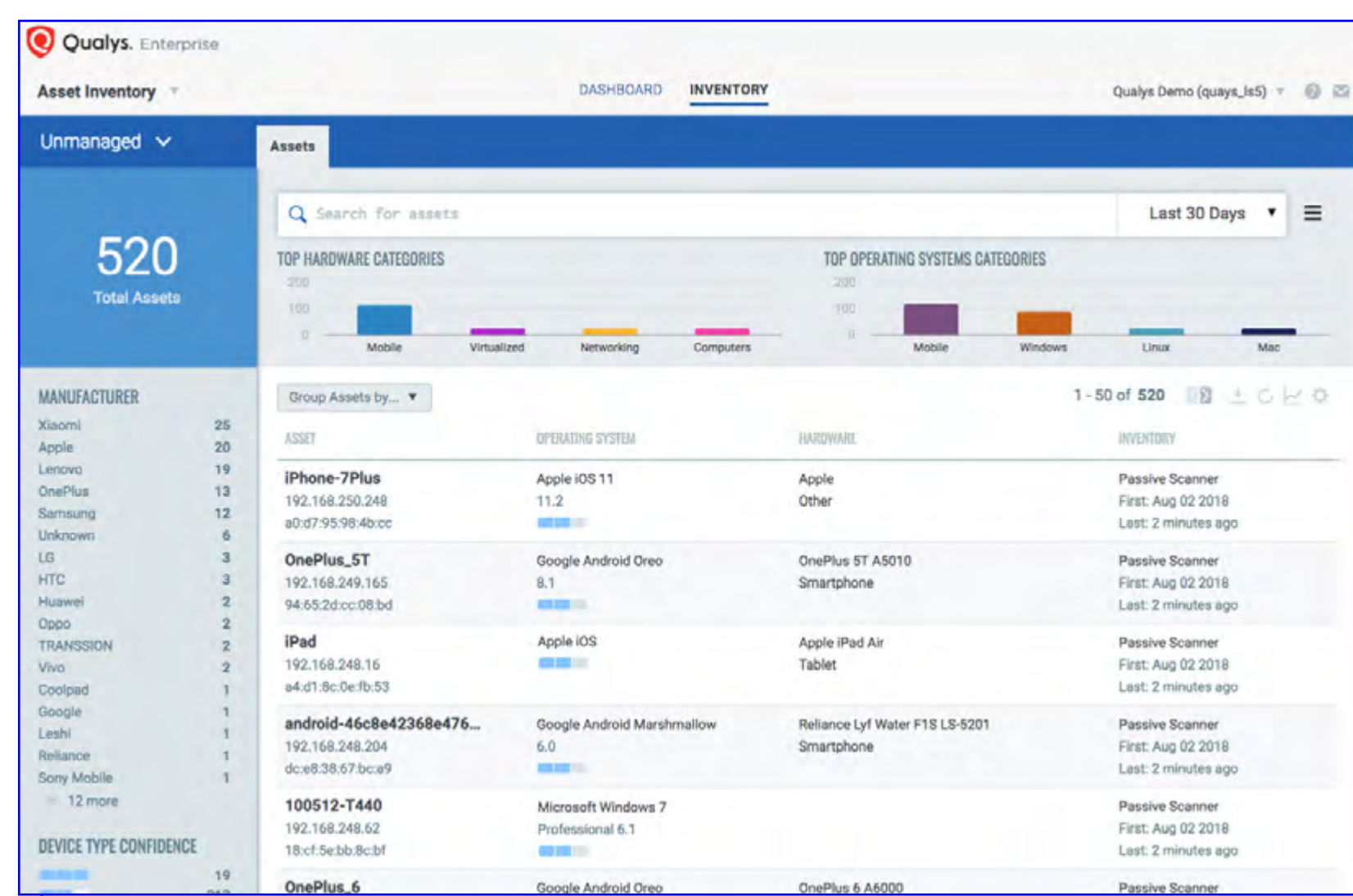
Cloud Apps into client environments across the globe, providing a programmatic vulnerability management approach that leverages the breadth of Qualys' continuous visibility and depth of the X-Force Red team's services to identify, prioritize and remediate clients' most critical vulnerabilities.

The Qualys Cloud Platform will also be leveraged by X-Force Red VMS to help extend security and compliance visibility into IoT-connected cars, network testing and application testing. X-Force Red will offer the Qualys Cloud Platform to its network of Global 2000 strategic outsourcing customers.

Qualys integrates real-time network analysis in its Cloud Platform

Qualys has introduced Passive Network Sensor (PNS), a new member of the Qualys sensor family that natively integrates network analysis functions into the Qualys Cloud Platform.

The Qualys Cloud Platform, with its active scanning, always-on agents, container and cloud sensors, provides global enterprises with unprecedented 2-second visibility of their hybrid IT infrastructure covering on-premises assets, multi-cloud environments, containers and

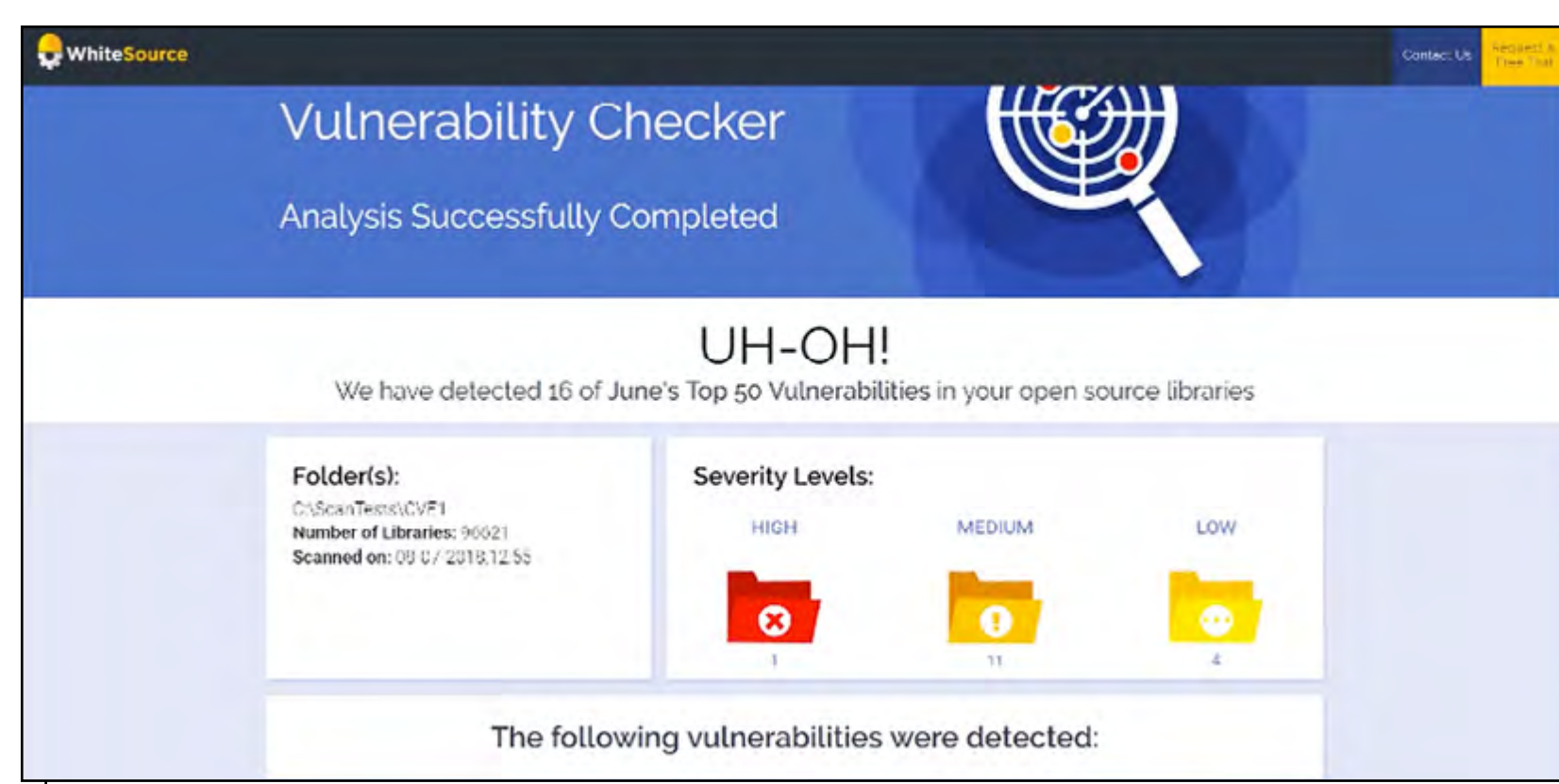


traveling workforces. The highly scalable platform performs over 3 billion device assessments annually, analyzing a trillion change events with its Kafka clusters that process billions of messages daily, and indexing over 250 billion security data points in its Elasticsearch clusters.

WhiteSource unveils free open source Vulnerability Checker

WhiteSource announced the release of its Vulnerability Checker, a free tool that provides companies with immediate, real-time alerts on the 50 most critical open source vulnerabilities published in the open source community.

The new standalone CLI tool is free to use and available for anyone to download as a desktop application directly from the WhiteSource website. Once downloaded, the Vulnerability Checker



offers users the opportunity to import and scan any library and run a quick check on the chosen development project against last month's top 50 vulnerabilities.

The Vulnerability Checker provides an alert if any open source component within the scanned library contains one or more of the top new open source security vulnerabilities enumerated in the previous month's report.

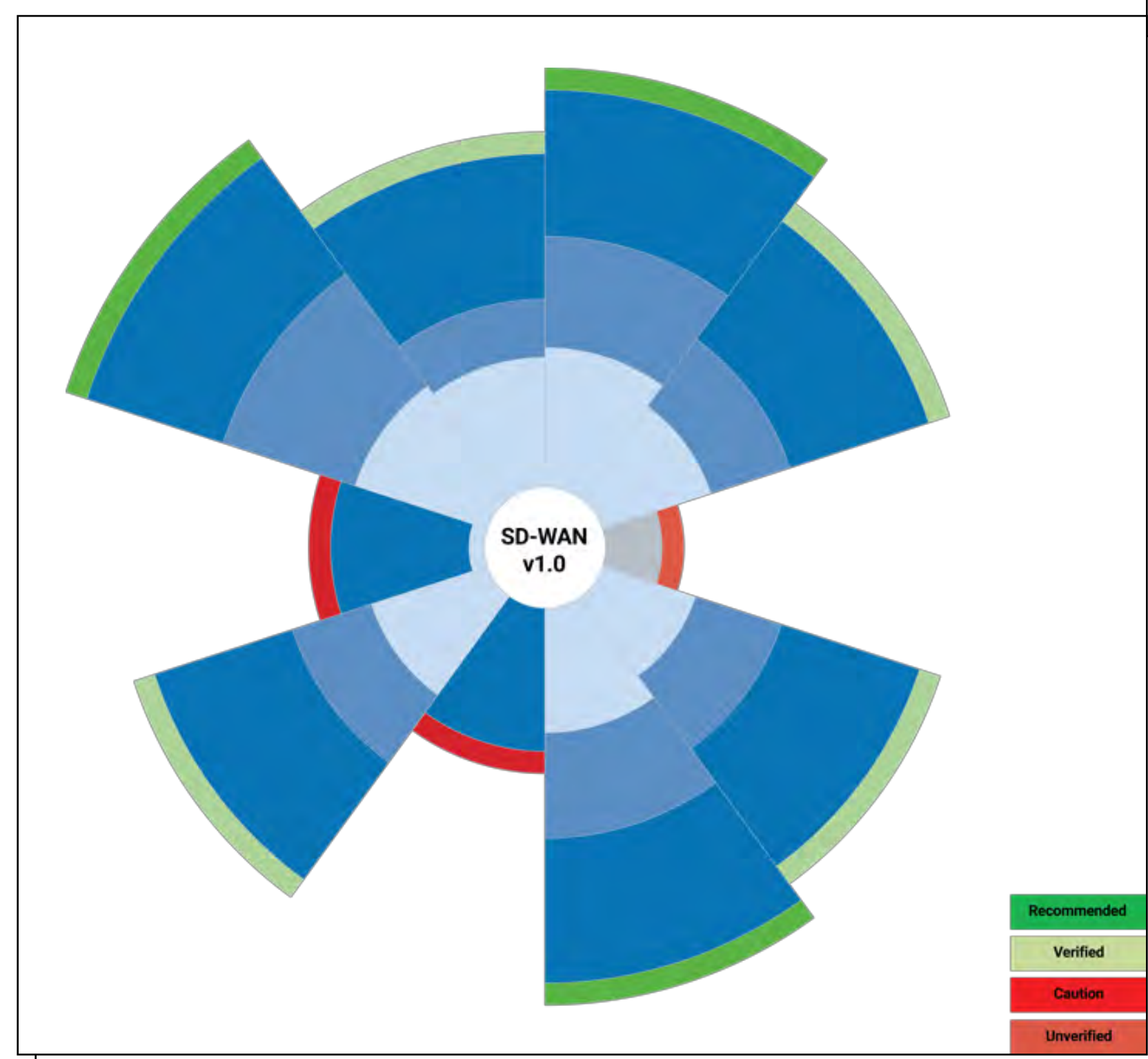
Which SD-WAN product should enterprises choose?

Adoption of Software Defined Wide Area Network (SD-WAN) has reached an inflection point and nearly every distributed business is deploying, evaluating, or planning to implement an SD-WAN as part of its IT vision. To help enterprises understand the merits of products in the market and identify the capabilities best suited to meet their use case requirements, NSS Labs announced the results of the industry's first Software Defined-Wide Area Network (SD-WAN) Group Test.

The capabilities that were assessed by NSS Labs include:

- ▣ Remote Initial Configuration
- ▣ WAN Impairment and Link Failover
- ▣ Dynamic Path Selection with SLA Measurements
- ▣ Path Conditioning and Application-Aware Steering
- ▣ Link Saturation and Congestion
- ▣ Application-Aware Traffic Steering
- ▣ Performance by Application Flows
- ▣ Raw Packet Processing Performance – UDP Throughput and UDP Latency
- ▣ Maximum Capacity
- ▣ HTTP Capacity and limits
- ▣ Application-Aware Response Time
- ▣ Security Effectiveness

While security effectiveness was not included in the final scores, it was evaluated in products offering security capabilities.



Products tested:

- ▣ Barracuda NextGen Firewall F-Series F80 v7.1.1
- ▣ Citrix Systems Inc. NetScaler SD-WAN 10.0.0.207
- ▣ Cradlepoint AER2200-600M v6.5.0
- ▣ FatPipe Networks MPVPN/SD-WAN v9.1.2
- ▣ Forcepoint NGFW 1101 vSMC 6.3.6, engine 6.3.6.19302
- ▣ Fortinet FortiGate 61E v6.0.1 GA build 5068
- ▣ Talari Networks Adaptive Private Networking (APN) Software vAPN 7.1
- ▣ Versa Networks FlexVNF v120
- ▣ VMware NSX SD-WAN by VeloCloud vEdge version 3.2

“The NSS Labs 2018 SD-WAN Group Test is the industry's first baseline assessment of these technologies. Our testing validates that this is a technology that is ready for prime time. We encourage enterprises to examine our findings for insights regarding the capabilities, performance, and cost of solutions as they continue to evolve their WAN architectures,” said Jason Brvenik, CTO at NSS Labs.

Securely launch your IoT-related services, devices, platforms, apps

Irdeto has introduced the latest version of Cloakware Software Protection to enable any IoT connected business to take advantage of and securely launch IoT-related services, devices, platforms, applications and more.

Cloakware Software Protection is a suite of advanced cybersecurity technologies that enables

organizations to customize the protection of their software-defined business. The solution now offers more platform support, including mobile devices and other platforms on iOS, Android, Linux, MAC OS X, Windows, select RTOSs and more.

Irdeto has also expanded the solution's programming language support to include C, C++, Swift, Web Assembly, JavaScript and others. In addition, Irdeto has also announced its new Cloakware Development Center to better connect with the developers using its solutions. This ensures that any organization working with Irdeto has a trusted, strategic security partner to meet their business needs.

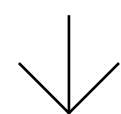
Crowdfense platform to allow researchers to safely submit, discuss and sell 0day exploits

Crowdfense announced the launch of their Vulnerability Research Platform (VRP). This web-based collaboration platform allows vulnerability researchers to safely submit, discuss and quickly sell single 0day exploits and chains of exploits.

"Through the VRP, Crowdfense experts work in real time with researchers to evaluate, test, document and refine their findings," said Andrea Zapparoli Manzoni, Director of Crowdfense. "The findings can be both within the scope of Crowdfense public Bug Bounty Program or freely proposed by researchers (for a specific set of key targets)."

Technically, the platform is organized into a streamlined set of workflows, with maximum OpSec for all participants. It is based on a zero-trust model and offers a reduced attack surface, anonymity (if desired), full E2E encryption and several other advanced security features, both client and server side.

The VRP v1.0 features include account and keys management and step-by-step workflows for the submission, technical evaluation and discussion of vulnerabilities, contracting and pricing definition, follow-up and maintenance of 0day capabilities over time.



These features were designed and refined during the past year through private betas, thanks to the support of ethical hackers, vulnerability research teams and selected brokers, with the aim of defining new best practices for the 0day market.

Vulnerability research and responsible disclosure: Advice from an industry veteran

AUTHOR_ Zeljka Zorz, Managing Editor,
(IN)SECURE Magazine



“Everything changes once you have to supervise and mentor and schedule and coordinate and keep in mind all the things others don’t. You often have to hold back your own wish to research a certain thing yourself or crack things open, because people rely on you to take a second look on their work. You kind of become the invisible ‘I’ in ‘Team,’” says Johannes Greil, Head of the SEC Consult Vulnerability Lab.

Any member of the team can propose research topics but he, as Head, has the last word on which will be undertaken.

At the beginning of every year, he puts forth a few topics that are currently relevant or may become relevant in the near future. But, also, things happen when they happen – they often stumble upon things during research and customer related consulting work, and they decide to deepen the research. After defining a budget and a timeframe for each proposal, they compare it with the others and pick

those they want to research within the next couple of weeks.

The future of vulnerability research

Greil started his internship at SEC Consult – a well-known security consultancy with offices across the world – in 2005, and worked his way up to the position of Team Lead and Head of the Vulnerability Lab.

One of the things he learned in his many years in the security field is that the more organizations spend on security from the very beginning, long before writing a single line of code, the more money they’ll save in the end.

“Unfortunately, you can wave your security budget bye-bye if marketing says a new product needs to launch yesterday, even if that might introduce a ‘slight’ security risk. In the end, business and convenience always trump security concerns,” he notes.

+ That's one of the reasons why he thinks vulnerability research will remain an exciting field of work and skilled consultants/researchers won't have to worry about finding a decent job.

"I guess we will see a lot more sophisticated automated attacks as well as the need for automated analysis tools. The number of IoT-related projects is growing fast and researchers need a way to work through those potentially vulnerable products efficiently. SEC Consult is doing its part: to improve the turnaround time of security advisories and keep good researchers focused on the deeper analysis work, we already launched a platform for automated firmware analysis, which is now also available for external testing," he shares.

"In our integrated hardware lab, we actually developed custom hardware analysis boards to help the research process. These boards make it much easier for our consultants to get low-level information out of any device (e.g., to dump flash chip contents) in a short time, as sometimes one doesn't have the time to do a deep hardware analysis."

He also foresees that, as everything is becoming more automated, human error will have a bigger impact in security research and the origin of vulnerabilities.

Advice for aspiring vulnerability researchers

His advice to security professionals who would like to specialize in vulnerability research is not to do it for fame or quick money. He's not a proponent of bug bounties, but says they can be used by researchers as an inspiration or as a test to see whether they are up to the challenge.

"Don't forget: You might invest a considerable amount of time into a bug bounty but then someone beats you to it or you just don't find anything. There is no guaranteed reward at the end," he notes.

+ Security bounties aim for quick fixes, but not solving underlying issues, and vendors use it to avoid integrating security at a technological level.

"If you're serious, an established security company might be the better choice for the long run. Being a security consultant also means to show how to fix it, and that requires a lot of expertise and training on the job."

When people apply to join the SEC Consult research teams, they usually test their reverse-engineering skills and knowledge in computer architecture and software programming, as well as how they work under pressure and whether they think outside the box. Communication skills are also important, not only to get along and work well with the team, but with vendors and other involved parties. "You are the professional, you know how it's done, but you can't blame or shame anyone," he adds.

For those that are interested in dissecting different devices on hardware level, hardware and electronics skills are vitally important.

Finally, Greil thinks that determination and having fun doing the research are among the essential traits of a successful vulnerability researcher. "If you pair all that with curiosity, a problem-solving mindset and neat communication skills, you will bloom in the infosec world."

Practicing responsible disclosure

Organized vulnerability research of the kind they do at SEC Consult comes with its own set of trials and challenges.

"Ethical and responsible hacking is not as easy as it looks, things take time and the reward is often just a (silent) patch and a non-disclosure agreement. You saved the world, but you won't get famous. Not right away, anyways," he says. Keep at it, be patient, have faith. Your time will come.

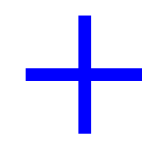
The company follows a responsible disclosure process, with two ISO standards playing a fundamental role.

“First, ISO/IEC 29147:2014 sets guidelines for the disclosure of potential vulnerabilities in products and online services. It provides methods a vendor should use to address issues related to vulnerability disclosure. Second, ISO/IEC 30111:2013 provides guidelines for how to process and resolve vulnerability information in a product or online service. Our internal responsible disclosure process then aims to provide vendors with the necessary information and timeframe needed to validate and fix a security flaw before a public advisory gets released,” he explains.

“Our biggest challenge is the coordination with the vendors as we often encounter vendors that are not aware of the impact or simply not cooperative and delay the disclosure process. Sometimes we

don’t get any answers at all or they go silent at a later stage. There are also vendors that don’t have security contacts on their website in the first place, so we need to go over different public channels which is time consuming and inefficient.”

They are constantly challenged to keep a balance between making the digital world and products more secure and protecting affected customers.



We usually give the vendor enough time to fix the issues and we only release when a patch is ready in the normal disclosure process.

“It also happens, every now and then, that a vendor stops answering and we feel obliged to release an advisory, but usually without a particular proof of concept to protect the users. We keep in mind that hackers read advisories more often than the users we intend to warn,” he concludes.

PROTECT YOUR SOFTWARE. PROTECT YOUR BUSINESS.

Your software is under attack
You must protect your ecosystem
and intellectual property

Don't be held back by security concerns

Download the latest Cloakware Report now by
scanning the QR code.

cloakware[®] by irdeto
www.irdeto.com



Managing migration mayhem: A roadmap for success

AUTHOR_ Tim Woods, VP of Technology Alliances, FireMon

New day. New threat. New technology to combat said threat. Sound familiar? The threat landscape is continually evolving and getting more sophisticated and, in an attempt to keep up, many organizations are adopting next-gen security products and services with advanced features and functionality. Next-gen firewalls are no exception - in fact, they're often a core component of security infrastructure upgrades.

But the thought of migrating from a first-gen to a next-gen firewall can strike fear in the heart of even the most seasoned security professionals.

+ Most enterprise security migrations are plagued by delays and cost overruns.

They often disrupt network services, and they can even create the very security problems they were meant to solve.



Contrary to what many believe (and have experienced), though, migrations can actually be completed relatively quickly, on-budget and without headaches. Here's a three-step roadmap to transform migration mayhem into migration success.

1_Clean up existing security policies

If you were to move into a new home, you would almost certainly get rid of your clutter before the moving truck arrived. Why move things you no longer need or use? The same principle can *and should* be applied to firewall migrations.

The number of firewall rules are growing exponentially (there are tens of thousands in some enterprises) as a result of a number of factors, including continuously evolving threats, compliance regulations, cloud computing and advanced technologies (e.g., microsegmentation and software-defined networking).



Without proper rule management and firewall hygiene, IT security teams can quickly get bogged down in a chaotic mess of rules that are outdated, unused, redundant or out-of-compliance.

In my experience, at least half of the access rules associated with legacy firewalls are no longer used or needed.

That said, the first step to a successful migration is to clean up your existing rule base, so you're only moving those rules that continue to serve a legitimate business purpose. This process entails four key phases:

Eliminate technical mistakes — Technical errors in firewall policies are rules that can be identified as ineffective or incorrect, or those that do not serve a business purpose. Common examples of technical mistakes include hidden, shadowed, redundant and overlapping rules. For example, an access request is sent to the IT department and a security professional places a corresponding rule on the firewall without knowing that the access requested is already provided or blocked elsewhere within the policy.

Technical mistakes creep into access policies over time and can cause network problems, result in security breaches and delay migration projects, so eliminating these types of errors prior to migration should be a priority.

Remove unused access — There may be some rules within your rule base that are compliant, written precisely, and provide or block the right access, but just aren't being used. In many cases of unused access, the original business purpose that mandated the creation of the rule is no longer relevant or valid, rendering the rule stagnant.

Removing unused access within your firewall is just as important as eliminating technical mistakes, as they can cause policy confusion, security issues and network hiccups. To determine rule and object usage, analyze and correlate the active policy against the network traffic pattern. Doing this over a sustained period (30, 60 or 90 days, for example) will show you definitively which rules are used and which are not.

Refine overly permissive rules — Once you've completed the first two phases of the cleanup process, the next step is to review the resulting ruleset to identify rules that permit overly permissive

access. Excessive access is often the result of poorly defined business requirements.

In other words, the business team says they need access to a certain system with a quick turnaround time, but they don't provide the security team with the business intent behind the request. In an effort to meet the imposed deadline, the security team writes a rule that provides broad network access (e.g., the use of "ANY"), with the intent of applying tighter controls once the business team provides the missing context. However, many times, the rule is never refined and broad access remains unchanged, leaving the organization open to tremendous risk.

To avoid transferring this risk over to your new firewall platform, review your ruleset and refine broad access to include only what's necessary to meet the needs of the business.

Continuously monitor policies — Policy cleanup and rule review requires significant time and effort, but it ensures that a more relevant, accurate ruleset will be migrated to the new firewall.

It also reduces errors and risk, minimizes complexity, and helps you maintain a better security and compliance posture.

Once the cleanup is complete, it's all about maintenance. It's important to continuously monitor your policies to avoid recreating the firewall mess you just organized. Compliance drift almost never happens immediately after a migration. It happens slowly, over time and often without notice. Continuous monitoring will help you keep your fingers on the pulse of the network, constantly validate (or invalidate) rules and policies, and maximize your new technology investments.

2_Secure support from the executive team

Hopefully, by now, you have a better understanding of what the policy cleanup process should entail. But before you begin, make sure you have the support of your management team. The reason this is so important is because, though you'll perform the cleanup project in the safest way possible, there is always a chance that someone's access may be shut off accidentally, or a rule may be eliminated when it's actually still needed – and this can cause serious business disruptions.

If your executive team is briefed on the cleanup initiative and understands that the benefits of better security hygiene around firewall policies far outweigh the risks associated with accidental rule or access removal, then they will continue to be supportive throughout the process. Assure management that though there may be a few flat tires along the way, you'll plug the holes immediately and get back on the right track. After all, the final destination is well worth any obstacles that may cross your path.

3_Align people, processes and technology

Now that the prep work is done, we can get into specifics around the migration itself, and a successful outcome requires the right combination of people, processes and technology.

▣ **People** — The migration team should consist of people who are knowledgeable about the existing legacy firewall platform and current policies as well as those who are experts on the target next-gen firewall platform and the desired policy outcomes. The former group possesses knowledge around why rules were created, the business intent or justification and other historical information that is important in policy cleanup and maintenance processes. The latter can chart a successful path to migration and help

the security team take full advantage of the next-gen firewall's advanced features and functionality.

▣ **Processes** — It takes clear, prescriptive processes to both untangle the complexity you undoubtedly have on your legacy firewalls and then maintain the desired security state once you've migrated to the next-gen firewall. Set goals for each phase of the migration journey and determine processes that will help you achieve them. Most importantly, institute consistent procedures to document firewall policies and rules. Clearly state the intent behind the rule, the business justification for it and who requested it. Doing so will help you maintain proper firewall hygiene, along with a better security and compliance posture.

▣ **Technology** — With a highly knowledgeable staff that can dedicate extended cycles to the steps recommended above, much of the discussed migration efforts should be achievable. However, technology does exist that can significantly accelerate the entire process. Security automation technology streamlines the process of identifying technical mistakes, unused rules and broad access rules. It provides actionable real-time data, so you can establish a consistent cadence for documenting and tracking all current and future access of a now streamlined ruleset. It rapidly accelerates the migration process while significantly reducing effort, cost and risk.

Empower your team

Perhaps most importantly, empower all parties involved in the migration project – from the security team, to business owners and management, to consultants – by providing them with the knowledge, resources and processes required to achieve a successful outcome. With everyone on board, working collectively toward your established goals using the steps outlined in this roadmap, your team will be well on its way to transforming migration mayhem into a migration process that is simple, seamless, secure and speedy from start to finish.



When No Starch Press founder Bill Pollock decided that his new venture would go for quality instead of quantity, he made the right choice.

“We haven’t had a down year in at least the last 23. This year who knows? I hope we’ll be up but I’m not guessing,” he told (IN)SECURE Magazine.


The current situation in IT publishing

Unsatisfied with the poor quality of many published titles, Pollock had been wanting to start his own publishing company since 1987. He finally did so in 1994 and has been lovingly tending it ever since.

Over the last few decades many of the titles No Starch Press published have achieved cult status, and the company became a widely respected name in the hacking and infosec community.

For the love of a good IT book: The No Starch Press story

AUTHOR_ Zeljka Zorz, Managing Editor, (IN) SECURE Magazine



When Pollock first started in this business, IT books were “big, fat, and fluffy” and many were simply rewrites of manuals. But over the years and with the advent of self-publishing, many interesting titles and amazing writers popped up in the tech field, making it easy for Pollock to find them.

The thing he doesn’t like about today’s IT book business is the over-publishing. “As average unit sales have trended down, major publishers responded by printing more titles and doing less with each of them. One publisher I’m aware of is releasing around 600 ‘books’ each year. In comparison, we’ve published fifteen books in total last year and should reach just over 30 this year.”

Another thing that differentiates No Starch from many of their competitors is that they don’t do print on demand.

“We often print 5,000 copies or more of a title at a time. Each time we print though we’re taking on that additional inventory risk but we take that risk because our focus is on crafting the best product; making the best book. We still think offset printing is the way to do that,” he says.

Choosing a new title

In general, the company does not publish a book unless they love it. Also, they avoid topics that change rapidly.

“We don’t publish very much on tools because tools change too quickly and we don’t like to rush,” he says. “We look for interesting, exciting topics by passionate authors, and we edit them extremely carefully. Think of us as the craft kitchen that is always working to make the new, delicious favorite.”

He bemoans the disappearance of the art of editing from much of IT/tech book publishing, but says

that they are fighting against it: they are expanding their editorial group with people who can actually edit and who are given enough time to do it right.

Pollock also uses his time at hacker cons and knowledge of the infosec community and current topics to try to determine what their readers will most enjoy.

All the editors participate in the discussion of whether they will accept a new project and Pollock gauges their responses before a final decision is made.

“Do I see excitement in their replies? Or are they waffling? Do we like the topic or are we bored by it? Will our readers like the book even if we don’t? Does someone want to edit it? Do we like the author (that matters – publishing can be like a marriage)? These are all things we take into consideration when choosing the next project,” he explains.

Plans for the future

Pollock’s looking to change the way that work flows through the editorial process.

“We’ve been a bit too loose over the years and that doesn’t work well when you’re working with a major distributor like Penguin Random House. Our challenge is to change our process internally without sacrificing quality.”

There are also other changes in the pipeline. As they plan to publish more, they need to build their editorial group to support that effort.

“We’ve grown a lot over the last few years and I never scaled our infrastructure. I’ve also learned in the last few months that we’ve been missing some key organizational pieces and a couple of key positions, like someone to handle HR and benefits,” he shares.

“I’m looking to hire a people manager right now because that can’t be me. Even if I had time to do it, I simply have too much on my plate already and I’m too intense.”

He still edits some of No Starch Press’s hacking/security/tech titles and, about a year ago, he launched the No Starch Press Foundation, which aims to educate the public about hacking and to create safe places for the hacking community.

He’s also toying with the idea of getting into video training, but he’s looking for someone to help lead that initiative.



Advice from the editor

Pollock compares editing tech books to solving a puzzle, and he loves to dig into a book to try to make sense of the author’s discourse. But, naturally, there are also things he doesn’t like.

“Bullets, em-dashes (too many of them), sub-bullets (never), numbered headings (we publish books not manuals), ellipses (I delete them), using too many asides (try to integrate them), icons (ugh). I like books to read like books,” he notes.

He also advises tech book authors to define new terms when they first mention them; not to kill their readers with forward or backward references, analogies or metaphors; not to overwhelm them with code; and to keep their explanations (and book) long enough to cover the subject and short enough to keep them interesting.

“Say what you mean, clear your visuals, don’t write to arbitrary page counts, and please don’t send a chapter in unless you think it’s finished,” he urges.

For those IT professionals who have decided to write a technical book but have yet to begin he has the following pointers: “Choose a topic that you’re passionate about. Keep your reader in mind. Don’t go too narrow unless you really don’t care if your book will sell. And, finally, listen to advice but don’t always follow it.”

Events

HITBSecConf 2018 – Beijing

October 29 - November 2, 2018

Kempinski Hotel Beijing, Beijing, China

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

Held in collaboration with JD Security, the event kicks off with 3-days of hands-on technical trainings followed by a 2-day multi-track conference. There will also be a team based Capture the Flag competition with an AI focus, plus a technology exhibition with areas dedicated to makerspaces, hackerspaces, AI and blockchain-related technologies.

HITBSecConf 2018 – Dubai

November 25-28, 2018

Grand Hyatt Dubai, United Arab Emirates

<http://helpnet.pro/hitb2018dxb>

Featuring a 2-day technical training courses, a 2-day multi-track conference, a Capture the Flag competition, technology exhibition with a focus area on AI and blockchain related tech, space for makers and hackerspaces, a car hacking and hardware related village plus a CommSec track - a free-to-attend track of 30- and 60-minute talks.

Insider Threat Symposium 2018

October 15-16, 2018

The Mary M Gates Learning Center, Alexandria, USA

<http://insiderthreat.dsigroup.org>

The event features key members of the IC, DoD, federal agencies, and discussion sessions focused on data analytics, machine learning, and building successful insider threat programs. The symposium provides an open and collaborative forum to generally understand the requirements and support necessary to combat, prevent, and detect insider threats.



Systems Security
Certified Practitioner

An (ISC)[®] Certification

THE FUTURE BELONGS TO THOSE WHO PREPARE FOR IT TODAY.

Achieve more in your IT career
with these 9 tips.

Get the eBook



Overcoming the threat of ransomware with zero-day recovery

AUTHOR_Alex Fagioli, CEO, Tectrade

Mix zero-day exploits together with ransomware and you get a cyberthreat that very few organizations are equipped to deal with. Yet by bringing IT support and cyber security teams closer together, a zero-day recovery architecture provides options for how to respond and remain operational in the immediate aftermath of an attack.

2017 is widely considered to have been the worst year in data breach history; however, with increasingly intelligent cyber criminals coming up with new methods daily, the number of cyberattacks accompanied by ransomware is expected to increase even more in the coming years. The number of zero-day attacks is expected to increase from one-per-week in 2015 to one-per-day by 2021. Evidence also points to more persistent and targeted ransomware attacks taking their place alongside the “garden-variety” strains that are relatively easy to intercept and defeat.



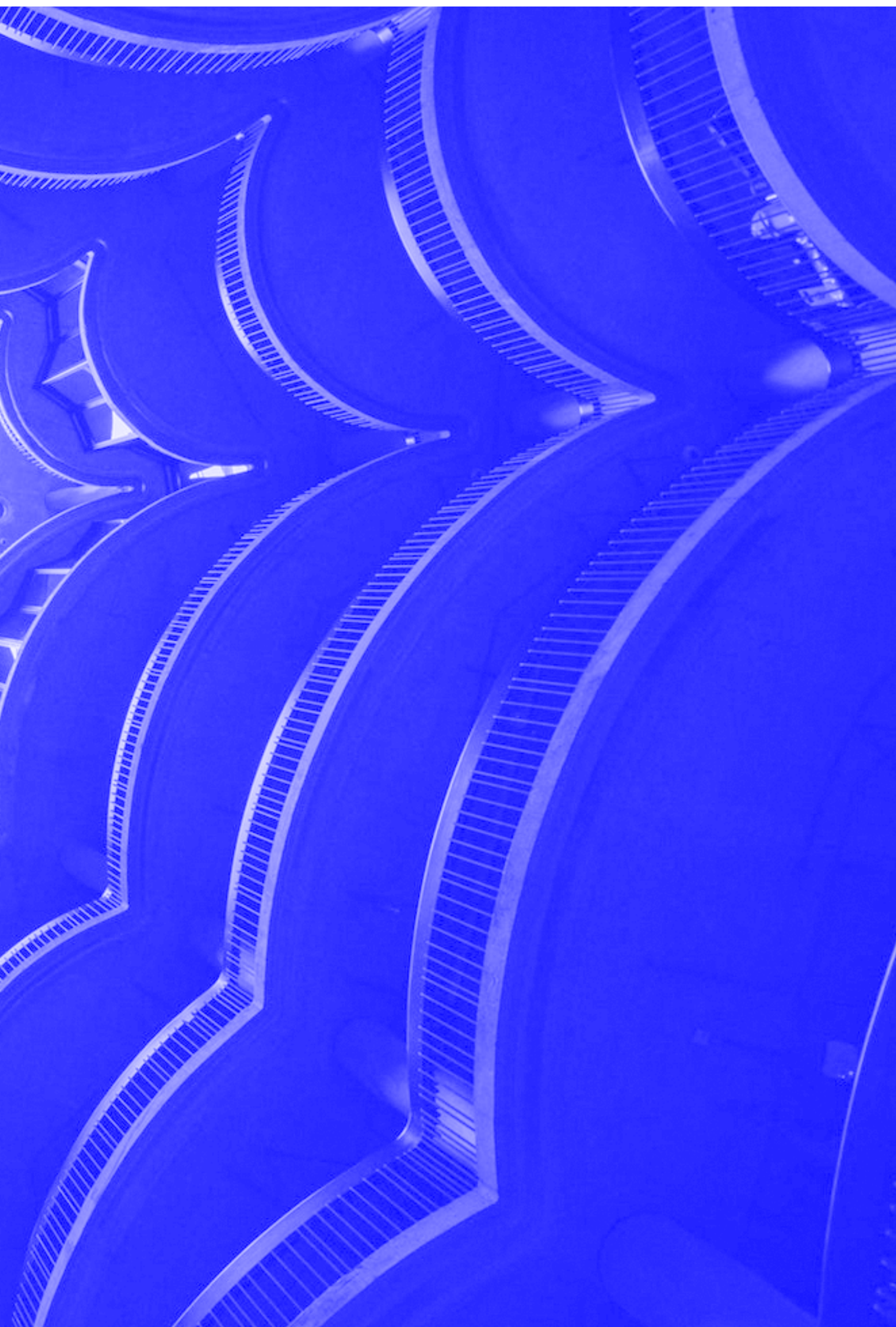
To take just one example: new research from Sophos and Neutrino estimates the SamSam ransomware has already made its handlers over £4.5 million. It is unusual in that the victims are carefully chosen, and the attacks carried out by a skilled team or individual with the resources, time and motivation to keep probing for a weak point.

+ With the attack surface growing by over 111 billion new lines of code every year, it's no surprise that a determined enough hacker will find a zero-day hole that offers a route into the network.

A plan B must therefore be put in place for what happens when all pre-prepared defences fail.

Zero-day attacks

Zero-day attacks exploit unknown vulnerabilities, meaning there is no signature to detect, let alone



defend against. So how can we protect ourselves against the unknown? The simple answer is: we can't. Just like trying to remain healthy, it makes sense to take sensible precautions that minimize the chances of getting ill. However, as any medical professional can advise, the focus must quickly switch to promoting a fast recovery as soon as the infection has taken hold.

Apart from being bad for business, ransomware attacks have the ability to put actual lives in danger. The most famous example of this is the WannaCry ransomware attack on the NHS, which was forced to cancel thousands of potentially lifesaving operations and medical appointments. Although no patient data was found to be compromised or stolen, the downtime and loss of data left 81 British hospitals affected, with emergency services being pulled and hospital facilities across the

country being brought down on top of the cancelled appointments. What cases such as this have taught us is that operations cannot continue without access to data. Being able to recover stolen data should therefore be the biggest priority for any organization, regardless of their sector or function.

Furthermore, in most cases it is the length of this recovery window that has the greatest impact on the level of damage caused by ransomware. Cyber insurance can be purchased to cover the initial costs of a breach and arguably, with the reporting of breaches now an everyday occurrence, the extent of the reputational damage is lesser than it would have been in previous years. It doesn't matter whether the main form of damage is expected to be financial or operational. If the recovery period can be minimized, then an incident that could have resulted in complete organizational paralysis can quickly be downgraded to little more than a minor irritant.

Shifting focus from defense to recovery

In the majority of organizations, the primary barrier to adopting a zero-day recovery architecture is organizational rather than technical. Responsibility for backup and recovery will sit with an IT support

team that is siloed from those responsible for security. Security professionals will do all they can to improve resilience, incorporating the likes of network segmentation, application control, advanced AV and user education to spot phishing attempts. Meanwhile, the IT support team likely already knows or suspects its backup and recovery processes are suboptimal, but lacks the budget to do anything about it. As a result, the organization is left with no option to quickly and confidently roll back to an uncompromised version of mission-critical data.

This needs to change, as the only real way for organizations to combat the threat of ransomware is to incorporate a quick recovery system into their security strategy. By shifting the focus on data recovery - the last line of defense against cyber-attacks - the threat of an attack would become lesser and, should the worst happen, organizations will be back up and running again with minimum disruption.

Enabling a zero-day recovery architecture

The process starts with IT support and security coming together to work out a set of policies that will define the architecture relevant to their organization. An on-going skills shortage means most IT teams are short-staffed and under tremendous pressure to drive digital transformation, inevitably leading to security gaps. Greater collaboration and the incorporation of security best practices into daily IT operations can deliver great benefits.

+ The policies that IT and security define may dictate that when an attack hits, a particular workload must be capable of being brought back into the server within 20 minutes.

For example, the e-commerce platform for an online retailer or the patient records system for a healthcare provider.

Meanwhile, for cost efficiency purposes it may be decided that other workloads are less of a priority and a much more generous recovery time objective can be set. In many cases, this optimization process pays for itself by reducing overall storage costs.

Next, it's time to build and test the back-up and recovery architecture. As demonstrated by TSB's recent IT disaster, with legacy systems it is very difficult to understand which systems are co-dependent or impact on the performance of another. For example, it would be pointless to be able to restore the e-commerce facility within minutes if it required the Active Directory to function, and that was assigned a recovery period of 48 hours. If there are faults, it is far better they be discovered now than in the immediate aftermath of a cyber-attack.

+ A proper zero-day recovery system has the potential of saving organizations a fortune, by minimizing down time and thus financial and operational losses.

However, the system needs to be set up before the breach occurs, as the components required cannot be added in after the fact. By combining effective cyber defences with a quick recovery system for crucial data, organizations can defeat system damaging cyber-attacks such as ransomware before they get a chance to disrupt the business.

Infosec and the future: Dr. Giovanni Vigna on lessons learned over 25 years

AUTHOR_ Zeljka Zorz, Managing Editor,
(IN)SECURE Magazine

When I asked Dr. Giovanni Vigna what are some of the most important lessons he has learned during the 25+ years he spent working in computer security, his answer was simple: always learn by doing and always innovate.

+ “Reading about security is never enough. Getting one’s hands ‘dirty’ by actually writing code or setting up systems is the only way to really appreciate how difficult it is to create reliable, effective attack/defense systems,” he says.

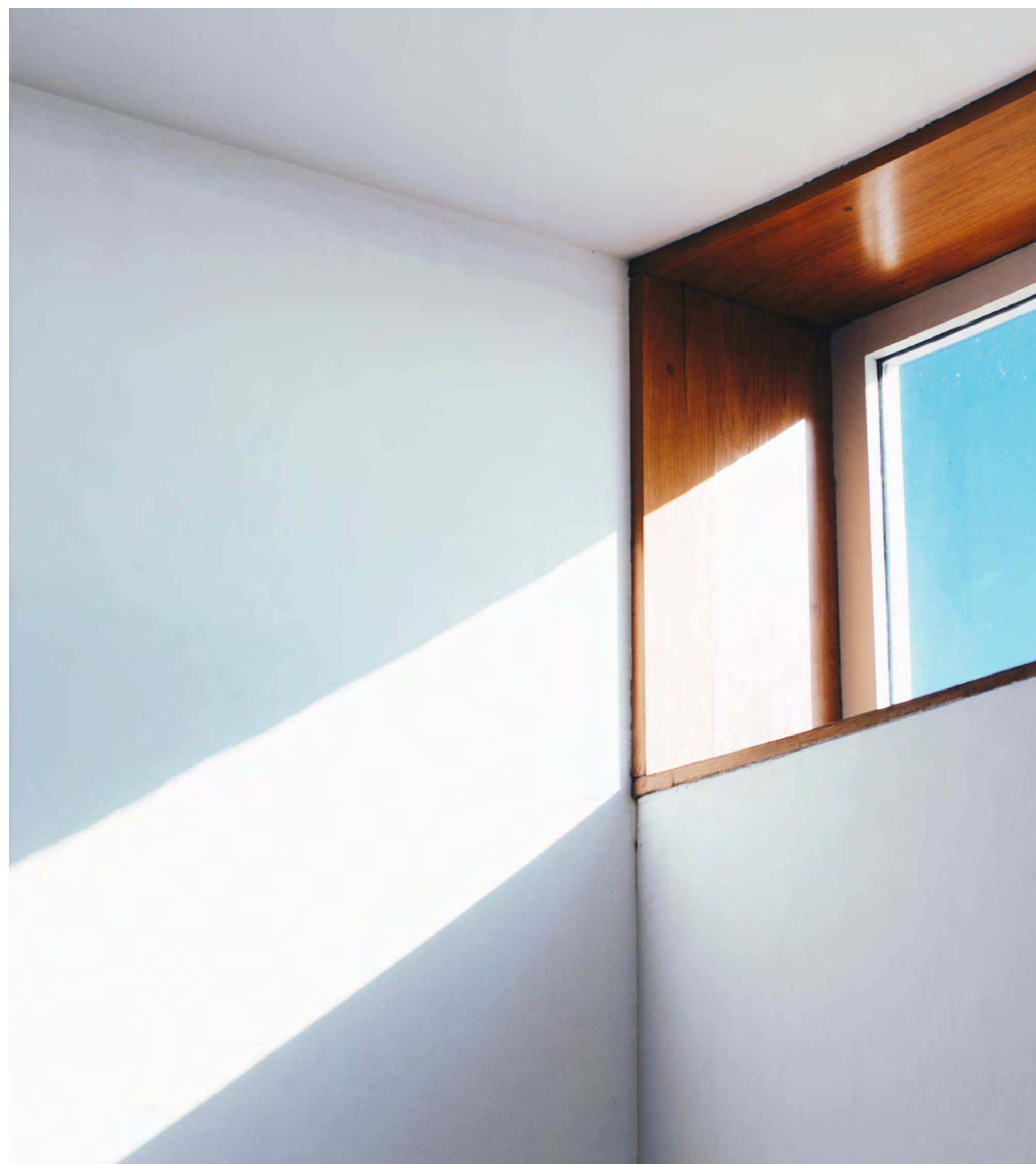
Learn by doing

One of the ways to learn by doing is to participate in CTF competitions, and Dr. Vigna knows a lot about that. He has founded and has been running the Shellphish hacker group, as well as organizing one of the world’s largest attack-defense hacking competitions for many years now.

Founding Shellphish was a natural consequence of participating in these competitions, he tells me, and since its inception in 2005, it has become the team that has participated in more DEF CON CTFs competitions than any other team in the world. The International Capture The Flag (iCTF) competition he started in 2003 is also the longest running educational attack/defense CTF competition in the world.

“My experience in organizing and participating in many CTF competitions has taught me that students and researchers love to be challenged. This drive to win results in better preparation and more commitment to achieve,” he says.

“In fact, these competitions are very similar to an athletic events, in which the event performance is important but the actual training that precedes it is crucial. Preparing for a CTF by designing and implementing attack and defense tools is the most



important learning phase, in which a student/researcher actually learns and tests the capability of different tools and techniques. The actual competition then puts the acquired knowledge to the test, but it's the preparation that contributes the most to the improvement of security skills."

These competitions are a great way to train and recruit students and employees.

"In a competitive environment, students and researchers tend to go well-beyond the call of duty, coming up with interesting, creative attack/defense solutions. In addition, doing this under severe time pressure can really shape one's view of security and improve the appreciation for team work," he adds.

Always innovate

Dr. Vigna's background in academia (he's been a Professor of Computer Science at the University of California in Santa Barbara since 2000) and security research forced him to always think about what's "novel".

The security field moves at a fast pace, so trying new approaches is the only way to move forward. And there is always a way to make a security mechanism or technique faster or more effective. He transferred this approach to Lastline, where he serves as the company's CTO.

"At Lastline we have a very in-depth view of what the active threats are. This inspires us to find novel approaches to combat them, since it's obvious that current approaches are not effective. So, even though Lastline and the university are two different worlds, they share many aspects," he adds.

Infosec and the future

There are many new and not-so-new technologies that are being tried out in the computer and

information security field, and Dr. Vigna is very excited about new ways of doing security analysis.

"So far, the model has been to have a human analyst explore a problem (e.g., finding a vulnerability in a piece of software) by using various tools and composing their results. I think that in the future it will be an automated system that drives the discovery process and uses humans as 'tools,' asking the human analyst for help when certain tasks cannot be solved automatically," he says.

"It's a sort of Copernican revolution of how we do things. While the research is at its infancy, the prospects are great since an automated approach can scale better than humans (and, no, we will not become slaves of the machines)."

Another thing that will shape the way in which we do security is machine learning.

"As we are able to collect more data, we can extract more meaning and automate more tasks, by using machine learning in the right way," he notes.

"However, in this case, 'right' is the keyword. Doing machine learning in an adversarial environment (i.e., when the data from which you are trying to learn is "fighting back") is not your standard machine learning gig. We will need to innovate the machine learning field in order to be able to learn, classify, cluster threats in the presence of an opponent that is well-aware of the techniques that are being used."

It will not be easy, he says. "The emerging threats understand which machine learning techniques are being used, what models have been learned, and use this knowledge to fly 'under the radar.' It might not be common now, but it will be the battlefield in five-ten years," he predicts.

PROTECT YOUR PEOPLE. SECURE YOUR ENTERPRISE.



How are you
protecting your
workforce?

mobile chat

collaboration tools

instant messaging

social media

cloud applications

Embrace new technologies
and drive business forward
Without Fear.

Real-time threat detection, risk remediation,
proactive defense, and automated archiving
for all your social media and digital channels.



SafeGuardCyber

www.safeguardcyber.com