[+] (IN)SECUREMagazine

12 | 2019
ISSUE 64

Reevaluating cyber threats

Could audio warnings augment your ability to fight off cyberattacks?

Unmask cybercriminals through identity attribution

Want to build a SOC? Here is what you need to know beforehand

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

EXPLORE THE HUMAN ELEMENT OF CYBERSECURITY.

What's the most important weapon in the fight against cyberthreats? New software? Faster equipment? Smarter computers? At RSA Conference, we believe it's people.

Attend RSA Conference 2020, February 24-28, and join thousands of security professionals, forward-thinking innovators and solution providers for five days of actionable learning, inspiring conversation and breakthrough ideas.

Register for RSAC 2020 before January 24 and save $900* on a Full Conference Pass.

rsaconference.com/helpnet-us20

#RSAC

FOLLOW US

*$900 discount applied to the on-site price.

Table of contents

Featured experts

BOB CARVER, Principal Cybersecurity Threat Intelligence and Analytics, Verizon
AMYN GILANI, VP of Product, 4iQ
PHILLIP MADDUX, Principal Application Security Researcher & Advisor, Signal Sciences
KEVIN O'BRIEN, CEO, GreatHorn
NIMMY REICHENBERG, Chief Strategy Officer, Siemplify
MATTHEW ROSENQUIST, Independent Cybersecurity Strategist
DANNY THOMPSON, SVP of Market and Product Strategy, APEX Analytix
ED WILLIAMS, EMEA Director of SpiderLabs, Trustwave

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

Could audio warnings augment your ability to fight off cyberattacks?

AUTHOR_ Phillip Maddux, Principal Application Security Researcher & Advisor, Signal Sciences

The security of your environment shouldn't depend on whether you're looking in the right place at the right time. While active visual means such as dashboards, emails, tickets, and chat messages are a vital part of security event monitoring, they might not get your attention if your eyes are elsewhere. Even when you're focused on the right screen, important events can easily get buried in an overload of information, delaying their processing, or allowing them to be overlooked entirely. Your website/web app needs a way to "speak up" when it's under attack.

> *Auditory delivery of security events will evolve to become a valuable complement to the tools most security teams already rely on.*

Now, imagine if potential website attacks or blocked requests announced themselves as clearly and recognizably as your phone's custom text-tone for your best friend. As you go about your busy day, you're always aware of the events you care about as they happen. Even if your attention was momentarily diverted from your screen, you'd get alerted in real time and could still respond quickly, saving valuable time.

To be clear, this passive, auditory type of event monitoring is currently only a theoretical capability, and will not replace active, visual means any time soon. Rather, auditory delivery of security events will evolve to become a valuable complement to the tools most security teams already rely on, adding a real-time, eyes-free dimension to the rich information and workflows currently in use, and targeting specific events so that only the most urgent or important ones trigger a sound.

When your SOC can hear hackers coming

Once proven, auditory monitoring promises valuable benefits for security teams. To begin with, new events and changes in event patterns will be identified more quickly. On an organizational level, auditory monitoring will help companies deal with the chronic talent shortage facing most security organizations. Passive alerts also make it possible to scale event monitoring coverage among analysts, while ensuring that nothing falls through the cracks.

> *Passive monitoring may even be delegated beyond the confines of the security operations center and its teams.*

In addition, auditory monitoring has the potential to expand cybersecurity careers for people with visual impairments. Finally, non-analysts such as senior security personnel, who don't ordinarily participate in monitoring, will be able to keep their ears open to the most critical events. In fact, passive monitoring may even be delegated beyond the confines of the security operations center and its teams, enabling operations teams, developers, and management to play an "if you hear something, say something"-type role in security.

> *In some scenarios, the sound alone might be all the information they need; for others, the nearest screen could fill in additional details.*

What would this approach look like—or sound like—in practice? Here are a few examples of how companies could leverage audible alerts for their web apps:

- SOC analysts sifting through system logs in Splunk could be alerted with a buzz if there's an increase of injection attack activity, such as XSS, SQLi, code injection, and so on.
- Managers tied up in meetings throughout the day could hear a chime from their laptop if a new round of credential stuffing attacks begins.
- DevOps teams concerned about new deployments running smoothly could hear a chirp if application errors occur.

In some scenarios, the sound alone might be all the information they need; for others, the nearest screen could fill in additional details. For added certainty, alerts could be configured to repeat periodically at intervals that correspond to their urgency, until cleared manually. However you implement it, auditory monitoring can bring an entirely new sensory realm into play that could help cut through the overload of visual information found in many IT settings.

A handful of open source projects are already experimenting with audible monitoring. Specific to cybersecurity, one project (https://github.com/foospidy/sigsci-sounds) uses sound to identify network traffic patterns such as ICMP pings and UDP/TCP port scans, and another uses sounds to identify specific events from web application firewall event logs.

Beyond the screen

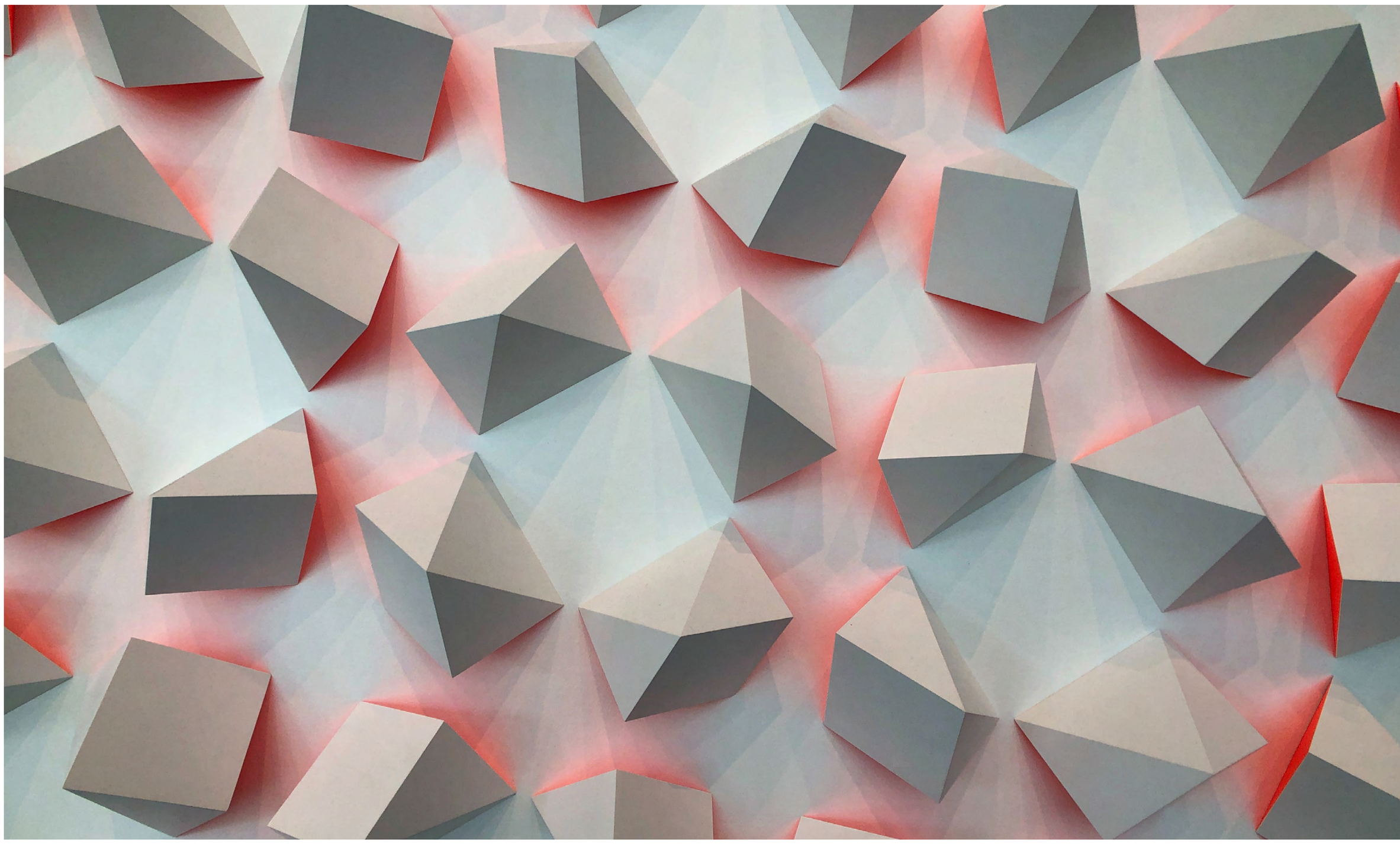
Computing has centered on visual displays for so long that screens can seem like the definitive way to present monitoring information, but this is far from true. Voice assistants and other non-visual media are transforming the way consumers interact with their apps and devices, and it's easy to imagine a future where sound-based interaction is the norm for many use cases. There will always be a need for the kind of detail, drill-down interactivity, and at-a-glance historical depth that

only a display can provide, but as technologists increasingly think beyond the pixel, there's tremendous potential for new ways to deliver timely information in auditory form. The simplest, briefest sound can be highly effective for capturing attention in situations where every minute counts, even in the hectic setting of a SOC.

> *Just as analysts can be overloaded with standard alerts, they could be overloaded with audible alerts*

If not applied appropriately, though, the auditory approach could become ineffective. Just as analysts can be overloaded with standard alerts, they could be overloaded with audible alerts. Perhaps not just overloaded, but even irritated to the point of disabling alerts altogether. To avoid this, audible alerting should be targeted for meaningful or high valued events. In addition, ensure the sounds you select are not obnoxious to your office neighbors.

For now, auditory security event monitoring remains an experimental concept to be explored, but it's worth paying close attention to the projects and pilots it spawns. As the speed and intensity of attacks continue to grow, the ability to hear your web app's "cries for help" could make all the difference.



Business email compromise (BEC) scams are a burgeoning threat for organizations and, despite rising awareness, new victims are cropping up daily.

> *The most common misconception about BEC scams is that the threat is limited to direct attacks on your own email environment*

Your supplier's BEC problem is your BEC problem

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

BEC scammers don't care what business the potential targets are in: all they care is that they have money that can be stolen – preferably lots of it – and that they have vulnerabilities they can exploit to pull off the heist.

Four major BEC fraud techniques

"The most common misconception about BEC scams is that the threat is limited to direct attacks on your own email environment, and that controls

and controls training should focus only on direct attacks," Danny Thompson, SVP of Market and Product Strategy at APEX Analytix, opined.

"Supplier email environments will get compromised and bad actors will divert supplier payments to their accounts. That makes your supplier's BEC problem, your BEC problem."

Cybercriminals have become increasingly sophisticated in their methods of carrying out BEC, he says, but four major techniques are generally at play: supplier spoofing, executive spoofing, credential harvesting, and exploitation of group user IDs or email addresses.

Supplier spoofing occurs when fraudulent bank accounts are included on emailed invoices or contained in emailed bank account change requests that appear to be from a company's supplier. **Executive spoofing** involves a fraudulent bank account change contained in an urgent change request from (ostensibly) the paying company's CEO.

Attackers that have managed to gain access to a supplier's emails and have harvested credentials for their accounts on customer websites and supplier portals can enter fraudulent bank account changes directly into the accounts.

These requests usually come from email addresses that are, at first glance, indistinguishable from legitimate ones. The latter are also likely to occur on the day before a major holiday, when the more experienced vendor master maintenance teams or supervisors are away from the office, leaving inexperienced staff with the choice of executing the request or defying the CEO.

Next: Attackers that have managed to gain access to a supplier's emails and have harvested credentials for their accounts on customer websites and supplier portals can enter fraudulent bank account changes directly into the accounts.

"**Credential harvesting** is of particular risk because many supplier information management portals lack sophisticated login controls such as multi-factor authentication," Thompson noted, and said that these well-informed fraud attempts often slip through normal accounts payable (AP) controls because of the credibility of information included in the requests.

We have seen several instances of BEC fraud where the timing of the attack certainly suggested an insider was involved.

Finally: Some companies use a generic email address to communicate with their customers – whether by email or as a login ID for their supplier information management portal.

"Disgruntled employees on their way out or soon after departure retain access to these credentials and can submit a bank account change request to their personal accounts. In these cases, everything about the request comes from a legitimate channel, making it much harder to identify and prevent," he explained.

BEC fraud by insiders

Working at a provider of supplier portal software and AP recovery audit services, Thompson is the right person to ask about whether BEC fraud is sometimes initiated or facilitated by an insider.

"We have seen several instances of BEC fraud where the timing of the attack certainly suggested

an insider was involved. These are cases where the fraudulent bank account change request coincided with the day unusually large payment was due. This often occurs when key members of the controls process are out of the office, typically just before a long holiday break," he shared.

New technology like deepfake video and especially audio has been and is sure to be used more by scammers.

"The suspects in these scenarios are: insiders in the supplying organization, third parties who have gained access to the accounts receivable (AR) or accounts payable records (either through the supplier's or the buyer's systems) or insiders in the buying or supplying organization. Over the years, we have found enough cases of insider fraud or insider/outsider conspiracies to conclude that insiders are very likely involved in BEC fraud."

While employees in procurement, AP, treasury and vendor maintenance and their counterparts in billing and AR should definitely receive regular training on scams, he says that some training should be limited to those specifically responsible for bank account change controls.

"The reason to limit some training is the risk of insider fraud. According to the Association of Certified Fraud Examiners, the majority of occupational fraud incidents originate in accounting. Of course, the more one knows about the control environment, the more likely one is to find a way around those controls. So, it is important that some controls remain a mystery to the broader procure-to-pay and order-to-cash population."

Tackling the BEC problem

When the BEC problem started gaining prominence years ago, it caught a lot of organizations by surprise.

New technology like deepfake video and especially audio has been and is sure to be used more by scammers, invalidating traditional, best-practice controls for bank account change requests such as a call-back to the supplier contact on record.

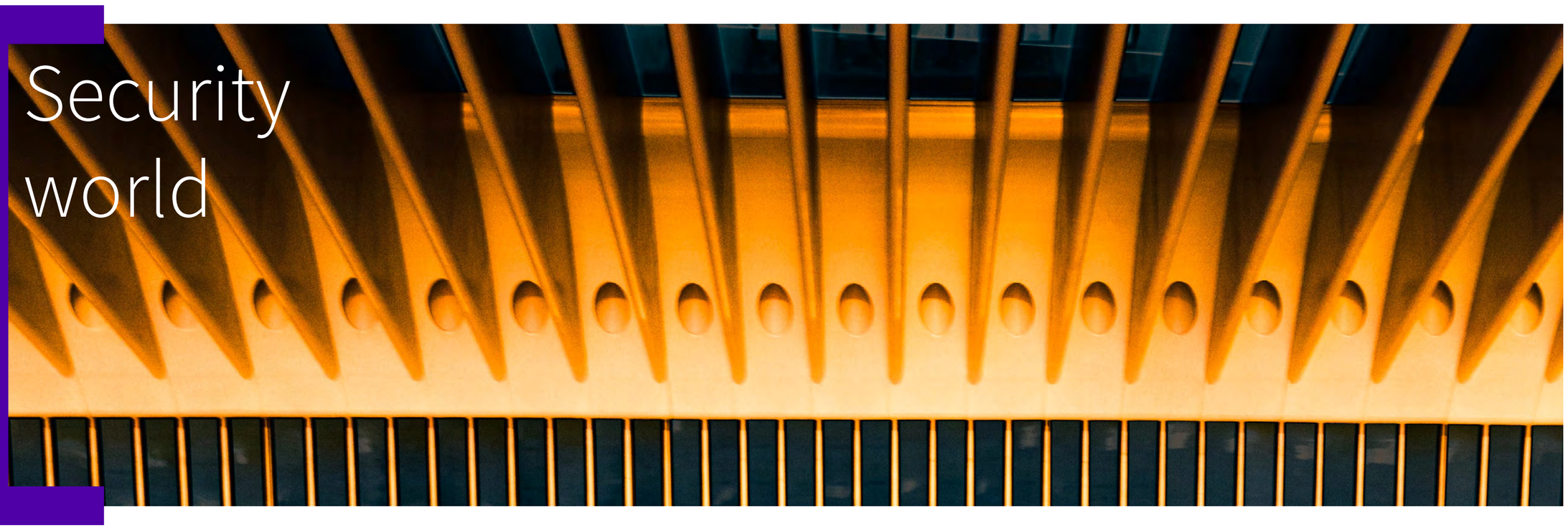
He expects more and more companies to refuse to accept bank account change requests through traditional channels (invoice, mail, phone, fax or email) and to only accept bank account changes through secure portals.

This will be followed by a rise in compromise of supplier login credentials in cases where the supplier portal software provider has failed to implement controls that match the threat, including multi-factor authentication, whitelisting/blacklisting (of email domains, IP addresses and suspicious banks), and user behavior pattern tracking to identify suspicious activity.

"My advice for the CISO of any large organization is to implement new controls that have become available, ones that are less dependent on humans, to prevent this type of BEC fraud," he noted.

"These controls include everything from online behavior pattern tracking to actual bank account ownership validation, where bank account change requests are validated in real time against the banking system to confirm that the owner of the payee bank account is the supplier. This validation process will ideally be integrated directly into the bank account change request and approval process, as the ultimate check to prevent payment fraud."

Security world



Only 47% of cybersecurity pros are prepared to deal with attacks on their IoT devices

Fewer than half (47%) of cybersecurity professionals have a plan in place to deal with attacks on their IoT devices and equipment, despite that fact that nine out of ten express concerns over future threats, according to the Neustar International Security Council (NISC) research.

These findings come at a time in which 48% of organizations admitted to experiencing a cyberattack against their IoT or connected devices and equipment in the last year alone.

Just over a quarter (27%) reported feeling “very confident” that their personnel would know how to protect against such attacks, while 38% claimed they are currently in the process of developing a plan.

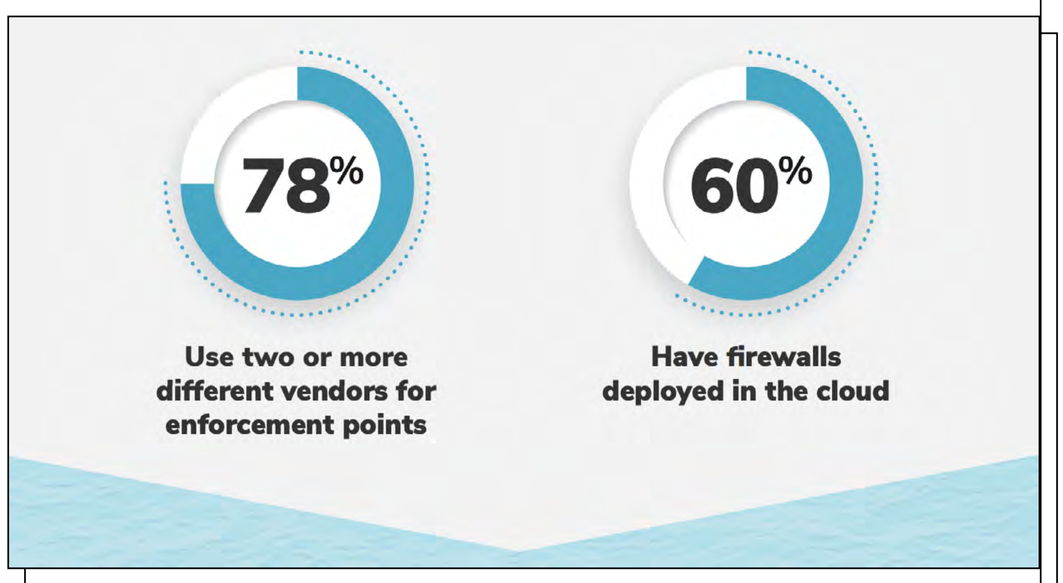
“With IoT devices and equipment now being such a fundamental part of business, organizations are continuing to connect more devices to their networks, resulting in an increased attack surface. This not only opens businesses up to more attacks, it also gives malicious actors new opportunities to breach security systems,” said Rodney Joffe, Chairman of NISC and, Security CTO at Neustar.

Top concerns for audit executives? Cyber risks and data governance

As organizations continue to collect customer and employee data, chief audit executives (CAEs) are increasingly concerned about how to govern and protect it. Gartner conducted interviews and surveys from across its global network of client organizations to identify the biggest risks facing boards, audit committees and executives in 2020.

Data governance has risen to the top spot of CAEs’ audit concerns, up from second place in last year’s report, replacing cybersecurity preparedness. Increased regulatory scrutiny has pushed governance risks, along with related data management challenges such as third-party ecosystems, cyber vulnerabilities and data privacy, as major concerns for audit departments.

Network complexity and lack of visibility contribute to misconfigurations and increased risk



Enterprises are slow to abandon manual processes, despite being short staffed, and the lack of automation, coupled with increasing network complexity risk and lack of visibility contribute to costly misconfigurations and increased risk, a FireMon report reveals.

Micro-segmentation, zero trust, containers, SDN, or cloud – it all falls under the same boardroom theme: digital transformation. Whether the goal is to be more agile, competitive or super-charge the supply chain, digital transformation is the glue driving the mission to be more responsive while closing the gap on security.

Highlighting this scenario, the report reveals that cloud adoption is up significantly – 72% of respondents are managing some form of hybrid cloud environment today, compared to the 53% cited in the 2018 report.

The mindset of the C-suite illuminated the core findings of this year's report. Citing a variety of security process challenges in the network environment leading to misconfigurations, C-level respondents shared the following feedback:

- Emails & spreadsheets drive workflow: 38% of C-level respondents said that change management processes are ad hoc, such as using email to send requests to firewall admins and spreadsheets to track network changes.
- No clear view of security posture: Only 23% had at least 80% real-time visibility into network security risks and compliance.
- Outdated communications: 35% of respondents only found out about a misconfigured firewall causing issues through urgent phone calls, emails and texts.

As more companies deploy cloud apps, they must also implement security tools

86% of enterprises have deployed cloud-based tools, but only 34% have implemented single sign-on (SSO), one of the most basic and critically important cloud security tools, according to Bitglass. The report found that the use of cloud applications has grown extensively over the past twelve months, with Salesforce and Slack increasing by 55% and 44%, respectively.

As more companies deploy cloud applications and modernize the way that their employees perform their work, they must also implement effective security tools and strategies tailored to a cloud-first environment.

IT professionals deem hybrid cloud as most secure

Enterprises plan to aggressively shift investment to hybrid cloud architectures, with respondents reporting steady and substantial hybrid deployment plans over the next five years, according to a Nutanix survey. The vast majority of 2019 survey respondents (85%) selected hybrid cloud as their ideal IT operating model.

Vanson Bourne surveyed 2,650 IT decision-makers in 24 countries around the world about where they're running their business applications today, where they plan to run them in the future, what their cloud challenges are, and how their cloud initiatives stack up against other IT projects and priorities.

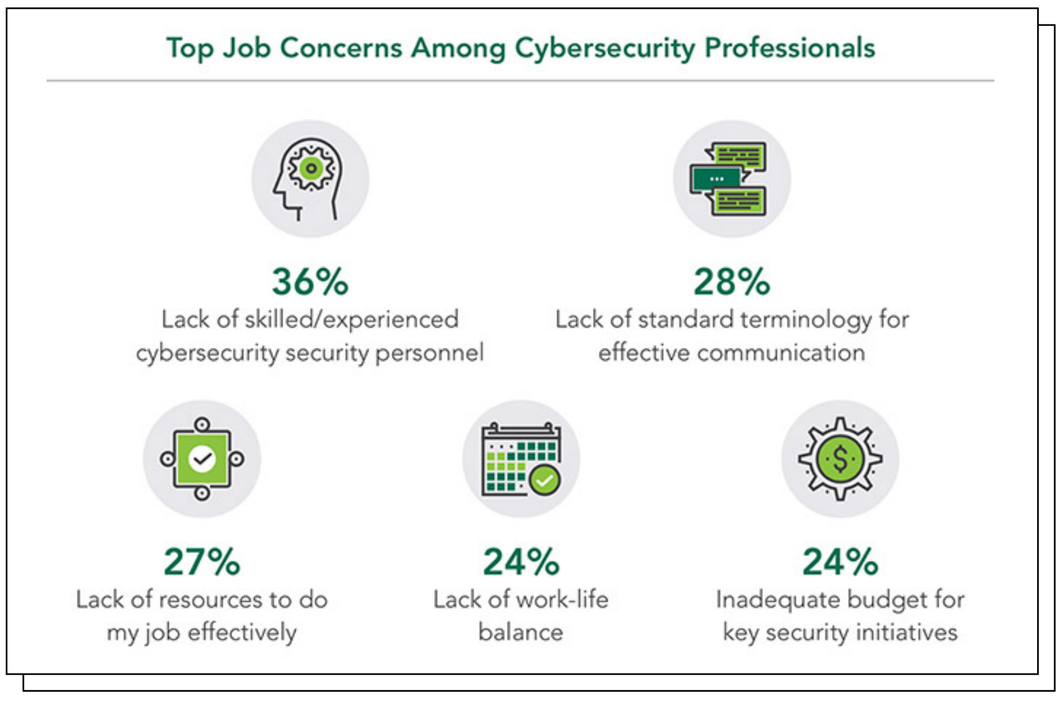
The 2019 respondent base spanned multiple industries, business sizes, and the following geographies: the Americas, EMEA, and the APJ region.
This year's report illustrated that creating and executing a cloud strategy has become a multidimensional challenge. At one time, a primary value proposition associated with the public cloud was substantial upfront capex savings. Now, enterprises have discovered that there are other considerations when selecting the best cloud for the business as well, and that one size cloud strategy doesn't fit all use cases.

Cybersecurity workforce skills gap rises to over 4 million

The estimated current cybersecurity workforce is 2.8 million professionals, while the amount of additional trained staff needed to close the skills gap is 4.07 million professionals, according to (ISC)2. The data indicates a necessary cybersecurity workforce increase of 145% globally.

Among the key findings from the study:

- 65% of organizations report a shortage of cybersecurity staff; a lack of skilled/experienced cybersecurity personnel is the top job concern among respondents (36%)
- 66% of respondents report that they are either somewhat satisfied (37%) or very satisfied (29%) in their jobs; and 65% intend to work in cybersecurity for their entire careers
- 30% of survey respondents are women; 23% of whom have security-specific job titles
- 37% are below the age of 35, and 5% are categorized as Generation Z, under 25 years old
- 62% of large organizations with more than 500 employees have a CISO; that number drops to 50% among smaller organizations
- 48% of organizations represented say their security training budgets will increase within the next year.

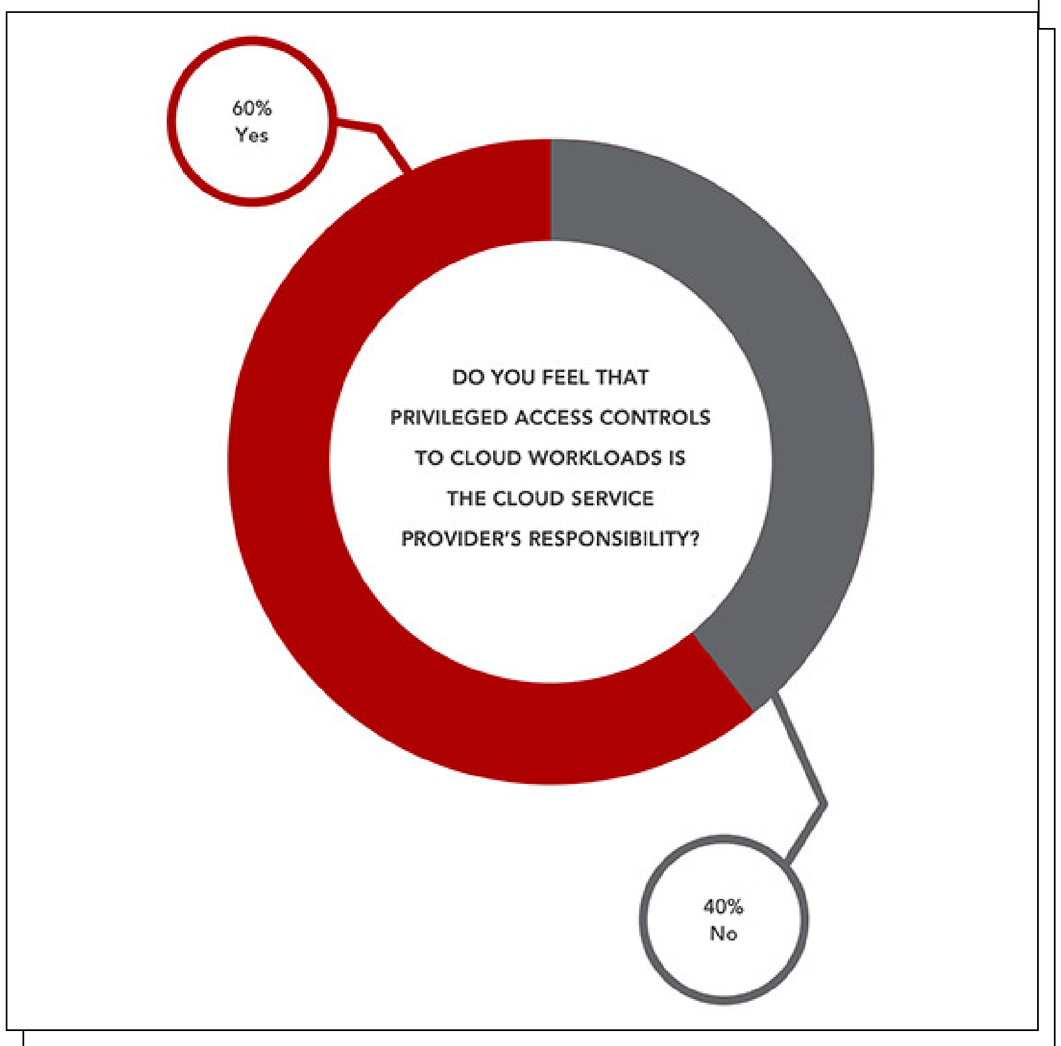


The leading challenge facing cloud migration projects is security

60% of organizations misunderstand the shared responsibility model for cloud security and incorrectly believe the cloud provider is responsible for securing privileged access, according to Centrify.

Furthermore, organizations are not employing a common security model or enforcing least privilege access to reduce risk, and the majority list security as their main challenge with cloud migrations.

The cloud's availability, accessibility, scalability, and speed of delivery make it an attractive option to deliver IT services more efficiently and affordably. However, securing multi-cloud and hybrid environments creates an unfamiliar situation, in which organizations are unsure of who is responsible for controlling privileged access.



5,183 breaches from the first nine months of 2019 exposed 7.9 billion records

According to Risk Based Security's Q3 2019 Data Breach QuickView Report, the total number of breaches was up 33.3% compared to Q3 2018, with 5,183 breaches reported in the first nine months of 2019.

Breach activity in 2019 is living up to being "the worst year on record". Although the total number of breaches is on track to break previous year records, the total number of records exposed has already surpassed the 2017 year-end total. 7.9 billion records have already been exposed and we are on track to reach as high as 8.5 billion.

"As we look over the experience of 2019, what stands out is that we are often our own worst enemy," commented Inga Goddijn, Executive Vice President at Risk Based Security. "Whether it's a phishing campaign that ultimately provides malicious actors with a toehold into systems or misconfigured databases and services that leave millions of sensitive records freely available on the internet, it seems to be human nature coupled with weak controls that contributed heavily to the number and severity of breaches we've seen this year."

Who is responsible for Active Directory security within your organization?

Over one third (36%) of IT professionals say their organizations are more vulnerable to security threats now than they were five years ago, according to a new Alsid research.

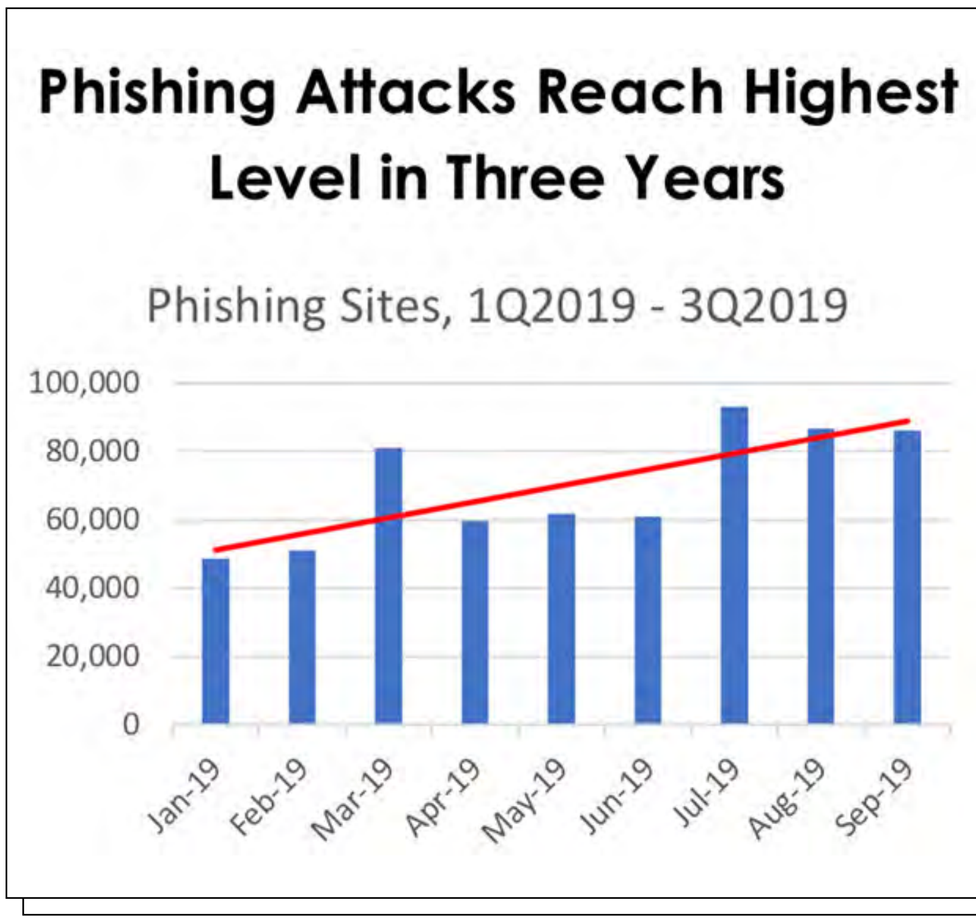
Ransomware attacks are just one of the many types of attacks that rely on compromising the Active Directory, which is sometimes forgotten as an element of an organization's IT security.

Of organizations which have an Active Directory, the survey data shows that responsibility for Active Directory security is split between functions, with 27% of those IT professionals reporting that responsibility lies with the IT team, and 19% stating that the security team holds responsibility for Active Directory security.

16% of respondents said that their organization employs an Active Directory security specialist. But 24% said that they don't know who is responsible for Active Directory security within their organization – showing that sometimes this important function can fall through the cracks between IT and security teams.

Furthermore, just one in five (21%) IT professionals said they have followed security best practices by testing a complete Active Directory restoration successfully more than once, and then incorporating the findings into their cybersecurity policy.

16% of respondents whose organizations have an Active Directory stated that Active Directory security is not treated as a priority in their organization, whereas 31% replied that AD security is a priority, but not a top priority. 26% said that Active Directory security is treated as one of the top priorities by their employer.



Phishing attacks at highest level in three years

The total number of phishing sites detected in July through September 2019 was 266,387. This was up 46 percent from the 182,465 seen in the second quarter of 2019, and almost double the 138,328 seen in Q4 2018.

"This is the worst period for phishing that the APWG has seen in three years, since the fourth quarter of 2016," said Greg Aaron, APWG Senior Research Fellow and President of Illumintel.

In addition to the increase in phishing volume, the number of brands that were attacked by phishers in Q3 was also up notably. APWG contributor MarkMonitor saw attacks against more than 400 different brands (companies) per month in Q3, versus an average of 313 per month in Q2.

Most organizations plan to increase their cybersecurity budgets in 2020

With the perpetually shifting threat landscape, most organizations (over 90%) believe that the cyber threat landscape will stay the same or worsen in 2020, according to FireEye.

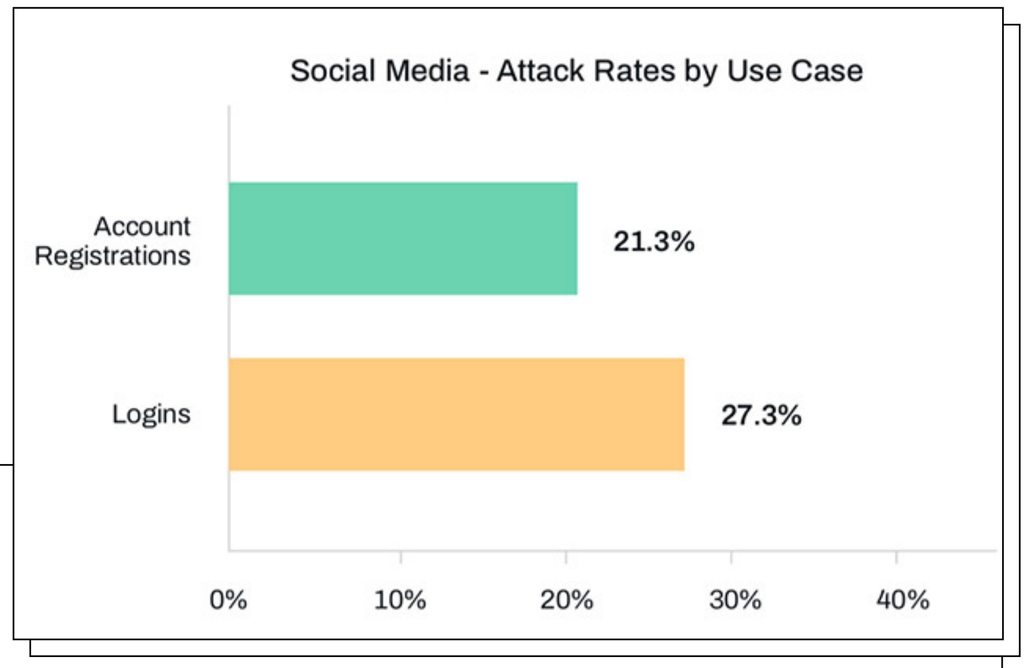
To address concerns regarding the potential loss of sensitive data, customer impact, and business operation disruptions, the vast majority (76%) of organizations plan to increase their cybersecurity budget in 2020:

- Organizations most commonly expressed plans to bump cybersecurity spending by 1-9% over 2019 allocations
- The greatest number of U.S. participants indicated budgetary increase plans of 10% or more (39%), followed by the UK (30%) and South Korea (22%)
- However, 25% of organizations in Japan and 24% in South Korea indicated plans to keep their security spend the same year over year.

Security and risk compliance: Still the most important part of IT strategy

Security practice is the number one priority for IT teams, with a clear majority (59%) reporting deficiencies in the controls that should ensure data processing and storage systems adhere to security policies, while over a quarter (27%) pointing to a lack of relevant skills as inhibiting quality assurance in the evolving Testing environment, according to Capgemini.

The report further highlights insufficient progress in test data and test environments management (TDM and TEM) as challenges continue to escalate for organizations: 60% of respondents this year said the greatest test environment roadblock they face is cost. This figure is up from 39% just two years ago.



Cybercriminals are testing exposed credentials for future account takeover attacks

Fraud increased 30% overall in Q3 2019 and bot-driven account registration fraud is up 70% as cybercriminals test stolen credentials in advance of the holiday retail season, according to Arkose Labs.

Researchers examined transactions in the financial services, e-commerce, travel, social media, gaming and entertainment industries from July 1, 2019 to Sept. 30, 2019. After analyzing over 1.3 billion transactions spanning account registrations, logins and payments, the report found that one in five account openings were fraudulent.

There has been a 30% increase in account takeover attacks in the retail industry compared to the previous quarter. Account takeover attacks are a precursor to payment fraud, as most e-commerce companies encourage consumers to create accounts and store payment details to remove friction in the path-to-purchase.

81% of all retail attacks were fraudulent payments transactions, with fraudsters targeting this sector to monetize the identity and payment credentials that have been breached en masse.

SIEM complexity and cloud visibility put companies at risk

Nearly half of companies are unable to remediate insider threats until after data loss has occurred, a Gurucul survey reveals. The study found that lack of visibility into anomalous activity, especially in the cloud, and manual SIEM workloads have increased the risk of insider threats for organizations and prevent many from detecting and stopping data exfiltration.

Some of the report's key findings include:

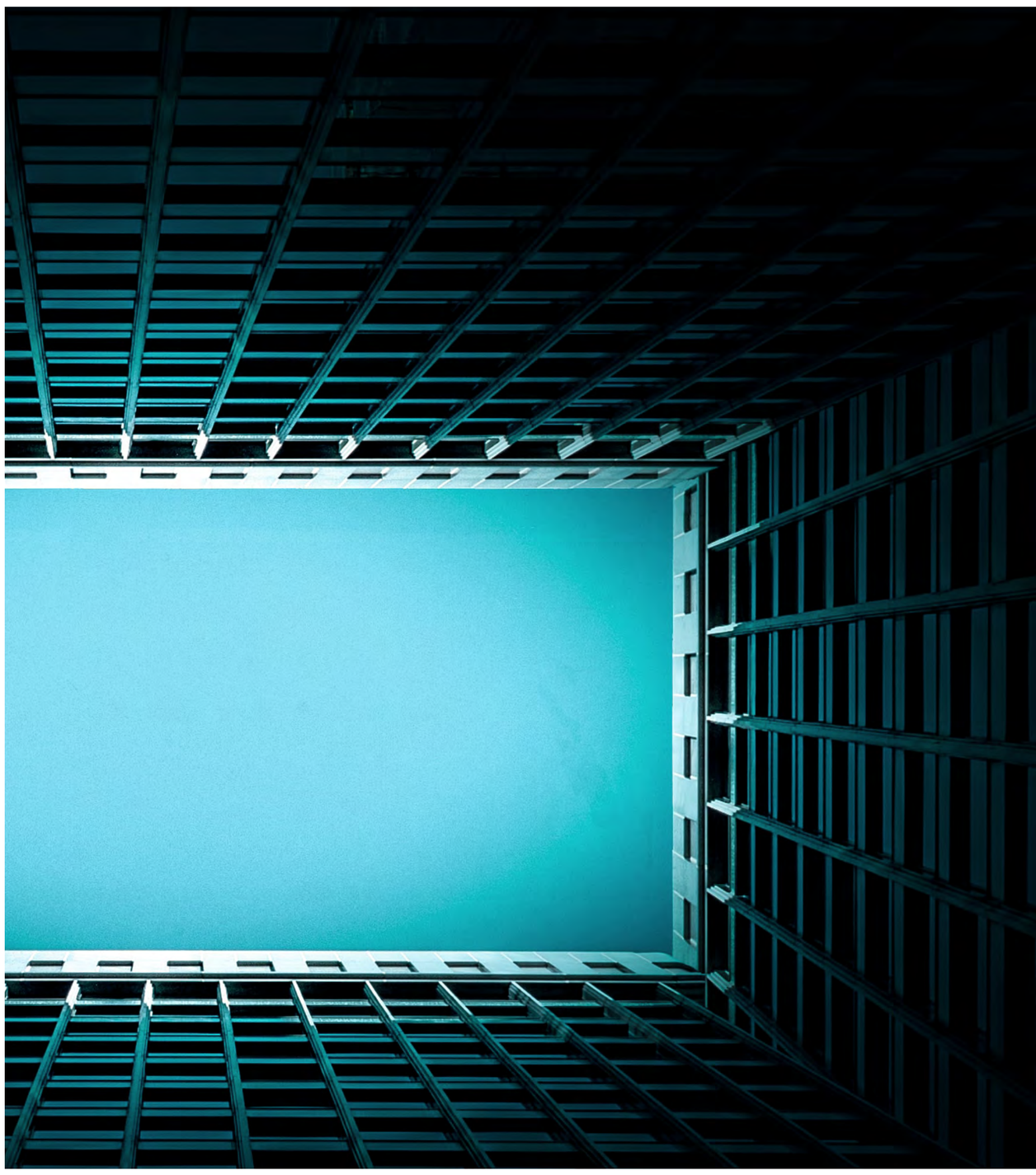
- 68% of organizations feel vulnerable to insider attacks
- 53% of organizations believe detecting insider attacks has become significantly to somewhat harder since migrating to the cloud
- 63% of organizations think that privileged IT users pose the biggest insider security risk to organizations
- Organizations cite lack of resources (31%) and too many false positive alerts (22%) as the biggest hurdles in maximizing the value of SIEM technology
- Only about one third of organizations are able to detect anomalous behavior in NetFlow/packet data (35%), service accounts (39%) and cloud resources (30%).

Microsoft to honor California's digital privacy law all through the U.S.

In the absence of a federal digital privacy law, Microsoft has decided to comply with the requirements of California's Consumer Privacy Act (CCPA) throughout the U.S.

"Under CCPA, companies must be transparent about data collection and use, and provide people with the option to prevent their personal information from being sold. Exactly what will be required under CCPA to accomplish these goals is still developing. Microsoft will continue to monitor those changes, and make the adjustments needed to provide effective transparency and control under CCPA to all people in the U.S," said Microsoft chief privacy officer Julie Brill.

She also noted that the company believes "privacy laws should be further strengthened by placing more robust accountability requirements on companies," such as minimization of data collection, more thorough explanations of why the data is collected and how it's used, and so on.



Product Showcase: SpyCloud Active Directory Guardian

Fueled by rampant employee password reuse across work and personal logins, account takeover represents a major risk to the enterprise. According to the 2019 Verizon Breach Report, the use of stolen credentials has been the number one hacking tactic for three years running. When employees reuse the same credentials across multiple logins, one data breach puts all of those accounts at risk. It's trivial for criminals to access all accounts that use those compromised credentials, leading them straight into corporate databases and more.

SpyCloud goes beyond detecting compromised passwords; it prevents account takeover from ensuing through the earliest detection possible. SpyCloud Active Directory Guardian automates the identification and mitigation of risk by continually checking on-prem Active Directory and/or Azure AD user accounts against the largest database of stolen credentials in the world. When a match is found, SpyCloud Active Directory Guardian can be configured to automatically reset the password before criminals use or sell them on underground markets. The solution enables you to be proactive in protecting your Active Directory users who reuse passwords.

SpyCloud Active Directory is a browser-based application that runs locally and easily installs in minutes. It can be custom-configured to scan automatically or on-demand.

Key Features

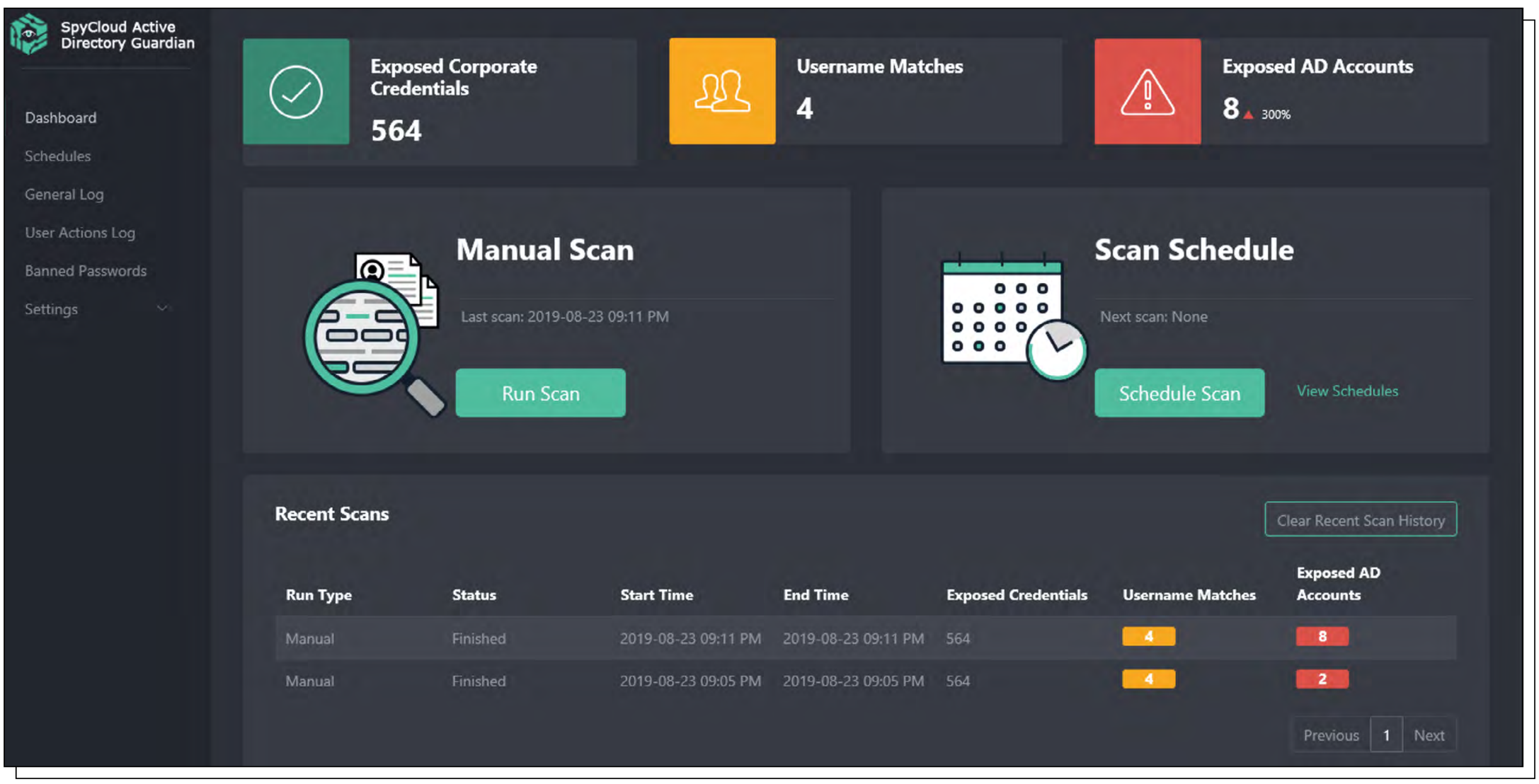
- **Automated risk detection:** Eliminates the manual, labor-intensive process of detecting compromised accounts to help companies protect their assets with fewer costs and resources.
- **Early remediation:** Gives teams the ability to remediate compromised accounts soon after the initial breach occurs – before criminals have the opportunity to cause harm.

- **Credential exposure alerts:** Alerts security teams when an Active Directory user account is matched with breach data, enabling a swift password reset.
- **Proactive password exposure checks:** Enables security teams to proactively check whether any AD user passwords have ever been exposed in a breach.
- **Built-in NIST compliance:** Helps enforce NIST guidelines across the enterprise by automatically checking AD user passwords against millions of previously-exposed and commonly-used passwords.
- **API integration:** Enables organizations to quickly integrate SpyCloud breach data into their workflows.

Automated risk detection

SpyCloud Active Directory Guardian eases the burden security teams face when trying to research, parse, normalize and match AD passwords to breach data. The automated solution rapidly and regularly compares active Windows domain users' credentials against current breach data, on-demand or on a predetermined schedule, encrypting the data for added security. Active Directory Guardian uses native Microsoft calls to pull data from the SpyCloud API and compares it locally to NTML hashes of AD passwords without logging into user accounts.

ADG DASHBOARD

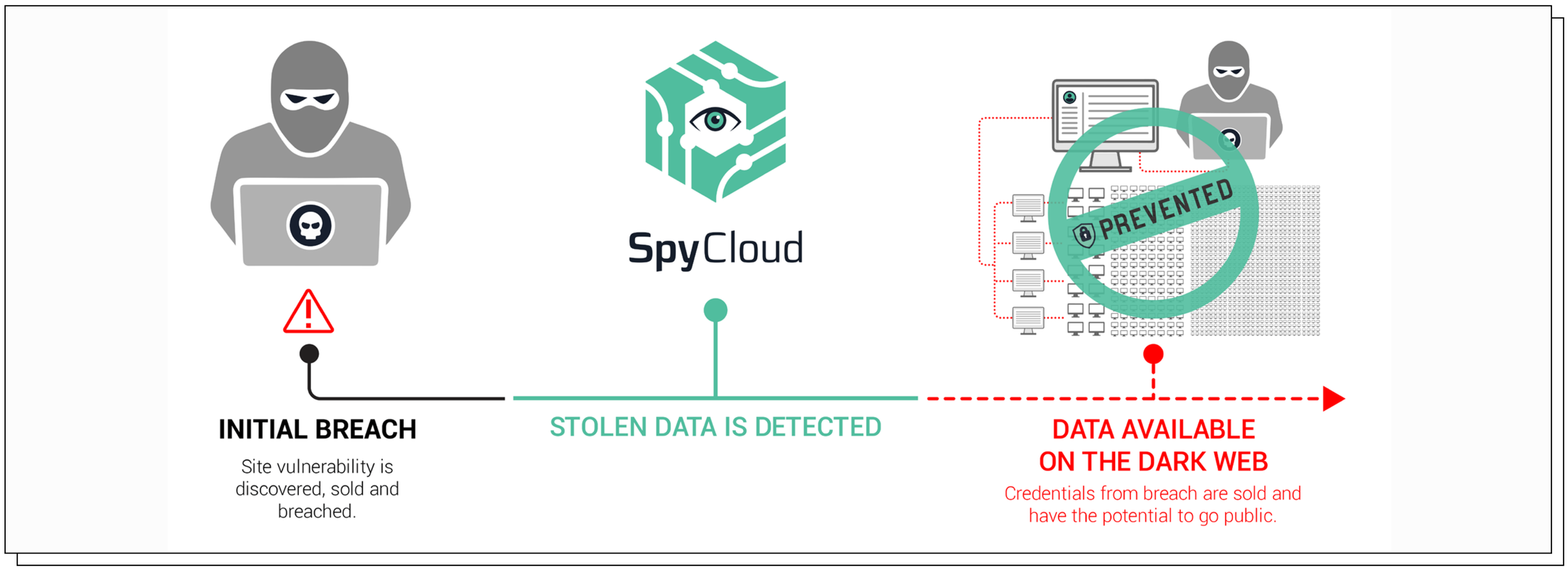


Early remediation

SpyCloud uses automated tools, proprietary tradecraft and human intelligence to find credential exposures early in the breach timeline, before stolen credentials can be used to take over accounts. Dedicated SpyCloud researchers go undercover within underground criminal communities to discover breaches automated tools can't. If a Windows domain user password (exact match or

"fuzzy" match) is found in the SpyCloud breach data, SpyCloud Active Directory Guardian can automatically force exposed users to reset their passwords. Alternatively, you can choose whether the exposure warrants an automatic reset.

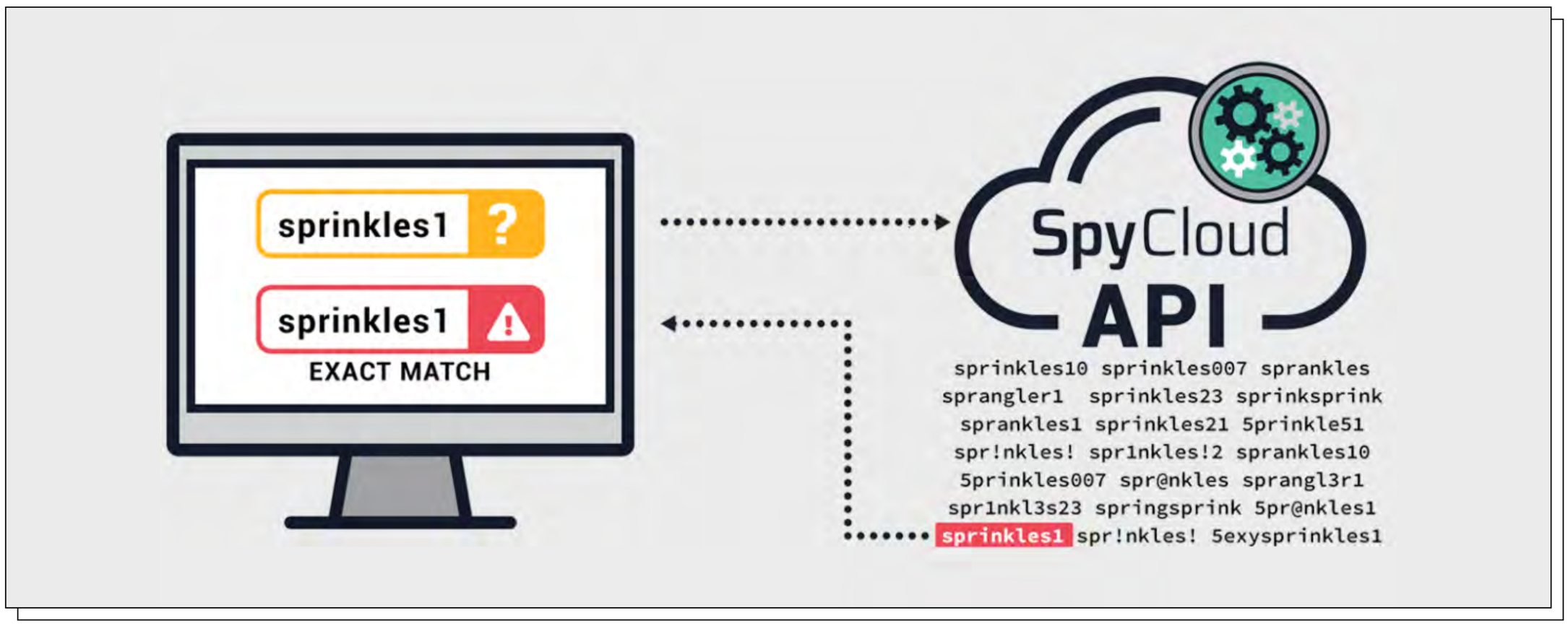
BREACH TIMELINE



Credential exposure alerts

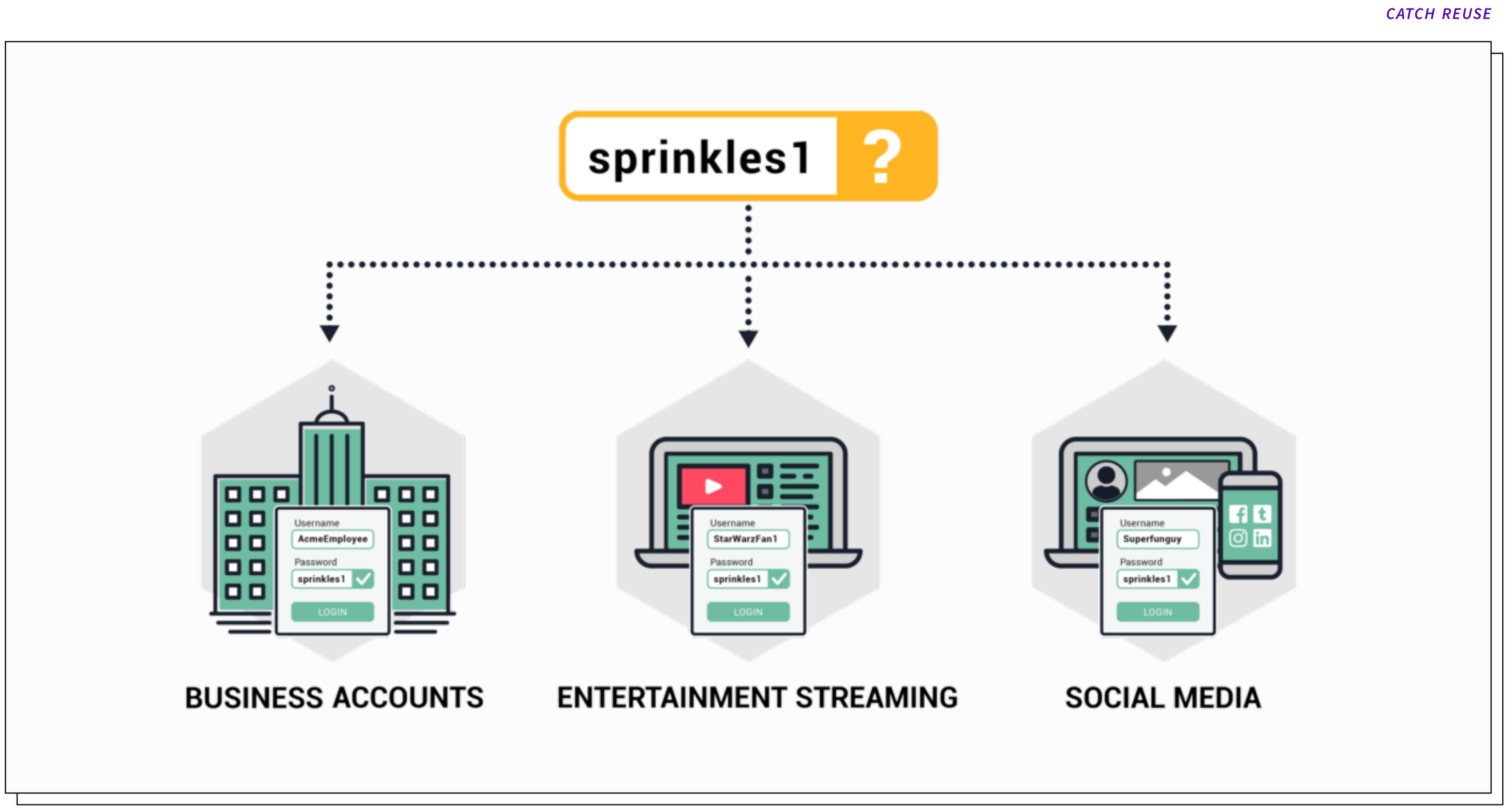
SpyCloud Active Directory Guardian automatically alerts security teams of credential exposures. Within the platform, a dashboard displays affected employee emails, exposed plaintext passwords, and guidance on the type of exposure; for example, the dashboard specifies whether the stolen credentials include an exact match for your employee's corporate password or a "fuzzy" variation. Whether you choose to run the scan on a regular basis or on-demand, instant alerts provide the necessary insight for rapid remediation.

EXACT MATCH



Proactive password exposure checks

SpyCloud uses proprietary methods to crack recovered passwords at scale, providing them to customers in plaintext. Plaintext passwords make the data more actionable because matches are easy to identify. You can proactively check your AD passwords against this database of plaintext passwords to see whether an employee has reused their AD password, even in combination with different usernames, and if those passwords have ever been exposed in a breach.



Built-in NIST compliance

SpyCloud helps you enforce the latest recommended NIST guidelines automatically. With Active Directory Guardian, you can check for passwords that fail to meet guidelines and put the organization at risk by looking for a match within SpyCloud's entire database of stolen credentials. If a user chooses a weak or compromised password, the system flags the account and enables security teams to take immediate action.

API integration

You can leverage SpyCloud's API to rapidly integrate SpyCloud data into your SIEM or user account management tools, enabling you to feed employee breach data into your workflows.

Interested in a free trial? Give Active Directory Guardian a try today: https://spycloud.com/pages/active-directory-protect/

Unmask cybercriminals through identity attribution

AUTHOR_ Amyn Gilani, VP of Product, 4iQ

Organized crime has grown more complex since the turn of the century. Coinciding with the rise of the digital world, cybercriminals have leveraged the proliferation of technology to broaden their reach with a more sophisticated network-structured model, effectively globalizing their operations in cyberspace and ultimately devastating companies and consumers alike. The faster you act, the quicker you will be able to disrupt the adversary and prevent future attacks, directly yielding greater financial savings and identity protection. Part of taking action, however, requires knowing who the bad actor is in the first place - in other words, attributing and uncovering the identities of cyber adversaries.

A modern approach to crime fighting must mirror the technological and organizational sophistication of our cybercriminal nemeses.

In the past, organized crime groups utilized a "boots on the ground" approach to attack, involving the coordination of more traditional hierarchical structures and on-location activity. More recently, such an approach has fallen out in favor of smaller, nimbler, more loosely structured crime rings that use advanced technology to widen their capabilities. Cybercriminals can hack into corporate databases and steal sensitive information from anywhere in the world. Taking out the "mob boss" to cripple their infrastructure and operations is a dated strategy—a modern approach to crime fighting must mirror the technological and organizational sophistication of our cybercriminal nemeses, and, as a result, security analysts are starting to shift their views on identity attribution.

Back in 2007, I was deployed to Iraq as a U.S. Air Force intelligence analyst, assigned to the Joint Special Operations Command (JSOC) Task Force with the objective of disrupting terrorist activities by targeting and capturing Al-Qaeda senior leadership. We were in constant pursuit of adversaries who endangered the very fabric of our democracy, seeking to discover and uncover the identities of enemy forces' leadership, weapons smugglers, and financiers. To achieve the Task Force's objectives, we used a myriad of sophisticated resources, including signals intelligence (SIGINT), human intelligence (HUMINT), and state-of-the-art drones.

The Task Force was successful in slowing down insurgent forces, due in large part to the accurate intelligence and positive identification (PID) of adversaries. In our governed rules of engagement, PID means that a hostile has been reasonably identified as a member of the target group or a confirmed imminent threat to our team. Drones, sky cameras, and many eyes and ears on the ground all worked together towards finding and finishing positively identified adversaries.

Adding a deeper layer of complexity to our mission was the necessity for confirming that a "precision strike" from a drone missile actually hit the intended mark. Occasionally, militant groups would falsely announce the death of their leaders or senior operatives in an attempt to throw us off track. Verifying a successful, targeted kill requires on-the-ground confirmation by U.S. personnel, generally through substantiating physical evidence or aerial photographs. Additionally, SIGINT and social media monitoring aided in confirmation efforts.

> *A growing number of private intel teams are now slowly transitioning to a more tactical approach by making intelligence more identity-driven.*

The same thinking can be applied to unmasking cybercriminals. While intelligence units at commercial organizations may not have access to the same sophisticated resources that were at the Task Force's disposal, a growing number of private intel teams are now slowly transitioning to a more tactical approach by making intelligence more identity-driven. Although threat actors have become increasingly adept at obfuscating their identities and attack vectors, identity intelligence and attribution analysis experts are at the forefront of developing effective countermeasures and proactive defenses.

Uncertainty in attribution and plausible deniability have historically weighed in cybercriminals' favor, but bad actors are people too and their personal histories present opportunities for intelligence specialists. Many cybercriminals leave their own historical breadcrumb trails, through data breaches or leaks and across the surface, social, deep, and dark web, ultimately leading security forces to their identities. While this data is transient in underground communities, a few organizations

have collected breached and leaked information from open sources to fuel cybercriminal investigations. New capabilities and tools leverage breached data, open source intelligence (OSINT), proprietary information, and other data sources, making identity attribution not only possible, but reliable and able to be validated in a timely, efficient, and effective manner.

By taking advantage of breached data, quickly acting on available intelligence, performing active defense, and attributing the real identity of adversaries and understanding their attack methods, cybercrime intelligence teams can now effectively neutralize and disrupt offensive cyber operations (OCO) and their infrastructure.

From my personal experience working in a security operations center (SOC), many security operators and traditional threat intelligence analysts are taught to fix—in a pre-defined cycle of detect, respond, remediate, and repeat—what is five feet in front of them. On the one hand, SOCs have been useful because they consolidated and correlated security alerts from so many tools into a single system. Yet the constant influx of new tool and threat feeds tend to produce an unreasonable flood of security alerts every day. Arduous tasks such as blocking indicators of compromise, flagging suspicious beaconing and removing phishing emails from employees' inboxes are necessary, but strictly reactive and time consuming. Mitigating one security incident could take hours, if not days; identifying activity that could indicate a security risk and ensuring that they were correctly handled—analyzed, defended, investigated, and reported—would yield an end result that was not likely to efficiently determine the identity of the attackers.

Yet, today, after a breach makes headlines in the news, the first question on everyone's minds is: "who did it?" By taking advantage of breached data, quickly acting on available intelligence, performing active defense, and attributing the real identity of adversaries and understanding their attack methods, cybercrime intelligence teams can now effectively neutralize and disrupt offensive cyber operations (OCO) and their infrastructure.
The Capital One breach that was disclosed in late July was compelling not only because of how massive it was but also because the bad actor, Paige Thompson, was so careless in disguising her identity following the incident. More often than not, as previously stated, cybercriminals will attempt to obfuscate their identities. Thompson, however, chose to draw attention to herself by boasting about the crime on social media, which I believe is not listed under "Best practices" in the cybercriminal rulebook. Thompson did not try to disguise her identity, to the bemusement of the cyber world, and was subsequently identified and arrested with the help of the FBI. However, most cybercriminals don't present themselves on silver platters in quite the way Thompson did.

By uncovering the identity of cybercriminals attacking your organization, you can take a variety of actions identified in the following five-step approach to disrupt the adversary and prevent future attacks:

1_Make the data obsolete: Resetting the passwords of employee and customer accounts, to prevent takeovers, will reduce the value of exfiltrated data on the black market and make data buyers and traders lose confidence in the seller. The dark web economy relies (to a surprising degree) on trust.

2_Move quickly: The more swiftly you can take action on the discovered compromised data, the better. This will lead to less disruption and financial

losses for your organization. Every minute counts when your organization's data is exposed. Time to actionable intelligence is key.

3_Report it: Quickly file suspicious activity reports (SARs) and inform law enforcement. Call the DHS's National Cybersecurity and Communications Integration Center (NCCIC) or an established contact from the local FBI cyber unit. If you haven't connected with one already, you should. If you have a high degree of confidence in your attribution investigation, law enforcement can help indict the person and disrupt their campaign, and possibly unveil and prosecute their entire fraud ring.

4_Identify threat vectors: Analyze when and where. At what point was the data compromised? Was it due to a risky merchant? Was it a poorly administered/configured database in the cloud? Was it a weak link in your supply chain? Patch up weaknesses and holes and be sure to vet your partners' and vendors' security postures, as they may represent possible avenues of attack as well.

5_Collaborate: Given the interconnected nature of our networks, collaboration has become a crucial tool in the arsenal of law-abiding organizations. If you come across leaked or exposed data from another company, be proactive and inform them so they can quickly notify customers, reset passwords, and perform necessary remediation. Collaborating will allow organizations to learn more about the adversarial network and how this group or person operates. For anti-phishing, contribute to the Anti-Phishing Working Group (APWG). For identity attribution support, invest in a credible identity intelligence monitoring service.

What does the impact of identity attribution and disruption look like? By consistently executing on these five elements, an organization can disrupt cybercriminal operations so effectively that when exfiltrated data becomes available on nefarious forums, the criminals already know that they won't be able to take advantage of it. Your stolen information won't sell because you've developed the reputation that your data will devalue as soon as it hits a dark web marketplace.

> *For law enforcement, attribution is crucial for prosecution and building a case. For corporations, attribution means identifying bad actors in order to assess the risk that an individual or entity poses, allowing the corporation to construct a competitive counter strategy.*

Not only is attribution for disruption applicable to military task forces, it can be effectively beneficial to financial services, retailers, cryptocurrency markets, social media platforms, as well as intelligence and law enforcement units. For law enforcement, attribution is crucial for prosecution and building a case. For corporations, attribution means identifying bad actors in order to assess the risk that an individual or entity poses, allowing the corporation to construct a competitive counter strategy.

With a few keystrokes from a connected device anywhere in the world, cybercriminals can hack into databases and steal troves of sensitive information. Security operation leaders need to understand that there is always a real person behind an attack, so shifting to catch the culprit and their cohorts rather than playing the repetitive game of defensive whack-a-mole will be essential moving forward.

Phishing attacks are a complex problem that requires layered solutions

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

Most cyberattacks start with a social engineering attempt and, most often than not, it takes the form of a phishing email.

It's easy to understand the popularity of this attack vector: phishing campaigns are relatively inexpensive (money- and time-wise), yet successful. Attackers don't need to create/buy technical exploits that might or might not work – instead, they exploit what they can always count on: users' emotions, fears, desires, and the fact that, despite knowing better, it only takes a moment of inattention to make a mistake.

> *The reality is that people are always soft targets, and social engineering and phishing attacks are outpacing legacy technologies and training-only solutions.*

"Cybercriminals play on users' expectations of trust in email communications and the human instinct to click on malicious links, give away credentials or even install malware and ransomware on endpoint devices - despite training and warnings to the contrary. The reality is that people are always soft targets, and social engineering and phishing attacks are outpacing legacy technologies and training-only solutions," said Kevin O'Brien, CEO at GreatHorn.

That's not to say that security training doesn't have a role to play.

"In the fight against phishing, consistency is often a business's best preventative. Since an organization's employees typically serve as the first line of defense, arming workers with a thorough background on relevant threat types and generic preventive measures can provide demonstrable value," he noted.

"But, while interactive, most phishing awareness training or 'Spot the phish' phishing simulation exercises are rarely tailored, making them ineffective when it comes to spotting real-life phishing attempts."

> *Once trust is established, it's easier to convince people to interact with malicious links and attachments.*

Effective oldies and emerging phishing approaches

While brand impersonation is the "gold standard" method for effecting credential theft, O'Brien says they are seeing new and innovative phishing attacks emerge almost every day.

"Phishers frequently exploit global brands like Microsoft, Dropbox, and DocuSign in their scams because the brands' good reputation lulls victims into a false sense of security," he explained.

"Once trust is established, it's easier to convince people to interact with malicious links and attachments. And because the URLs for these brands are hosted on seemingly legitimate websites, they can more easily evade many common email security tools."

Microsoft has been phishers' favorite brand to impersonate for quite a while, as compromised Office 365 accounts allow attackers to launch insider attacks targeting anyone in the organization in just one step.

"We also recently identified a set of widespread credential theft attacks that directly impersonate – of all things – cybersecurity companies themselves," he shared.

"Legacy email security companies require that their customers publish – via DNS entries – that they are using their services. The attackers spoofed some of the less well-known aspects of the email specifications, such as the return path and received headers, to appear as though they were coming from well-known email security companies."

Another type of approach they've recently seen in customer environments is the "Note to self" attack: the attackers spoof the user's email display name, put "Note to self" in the subject line and drop a link or attachment into the email.

Even if targets are not in the habit of mailing themselves notes, such an email often piques their interest and occasionally tricks them into doing things that they know they should not do under other circumstances. And, according to O'Brian, this approach is particularly successful at duping mobile users because the email is rendered differently on a mobile phone than on a computer.

A note on BEC scams

Email campaigns aimed at stealing login credentials are prevalent and can fuel even more dangerous and disastrous attacks such as business email compromise (BEC) scams.

FBI's Internet Crime Complaint Center (IC3) shared in April that BEC scams, along with email account compromise (EAC) scams, have brought about nearly $1.3 billion in losses last year.

"IC3 recently released new data regarding business email compromise, showing that the damages have reached over $26 billion. Moreover, the FBI says that these scams are continuing to grow every year, with a 100% increase in the identified global exposed losses between May 2018 and July 2019," O'Brien noted, and pointed out that the losses are certainly much higher.

"The FBI only investigates claims over a certain dollar amount, so there are many cases not reported. Also, these numbers are also only hard losses – the cost of IP theft, fines, consumer protection, etc. aren't included in these estimates."

BEC scammers are constantly trying new approaches to evade security tools that organizations have in place. As Armorblox CEO Dhananjay Sampath recently pointed out, they've evolved from sending a single email with malware or a phishing link to using multiple emails and social engineering methods, such as mentioning out-of-office responses, injecting personal information such as details of a real estate purchase or using workflow information.

O'Brian expects the evolution to continue in the coming years and attackers to shift from simple financial extraction attacks to incorporating additional types of attack.

Security awareness and phishing training for employees is a great idea but should not be the only thing they rely on because users make mistakes and are inconsistent.

He also anticipates improved execution and targeting by attackers impersonating brands, as well as a continuing rise of ransomware aimed at organizations.

Advice for CISOs

O'Brien advises CISOs and IT leaders to keep telling themselves that there is no silver bullet for the phishing problem and to tackle it holistically. Security awareness and phishing training for employees is a great idea but should not be the only thing they rely on because users make mistakes and are inconsistent.

"Consider this: a little over 10% of Americans don't use seatbelts, and 80% of them admit that when they're in the back of an Uber or a Lyft or driving a short distance, they often don't buckle up. They know it's safer to do it, and they still don't do it. The situation with security awareness training isn't that much different and that's why you can't ever train the problem away completely," he opined.

Detection technology will also never be able to identify and stop all phishing attacks, and that's why, instead of just looking to block "bad things", companies need to focus on identify suspicious ones and give users the tools to make better decisions about them.

"User training and business processes need to be reinforced with in-the-moment education to warn people what to do when. And we need integrated IR tools to remove things that get through – because things will get through," he said.

CISOs and IT leaders must accept that just implementing the best "set it and forget it" tools is not the right answer when it comes to phishing (or any other threat, really). They should cultivate a security-first culture by embracing a dynamic and continuous approach to risk assessment, prioritization, and remediation.

"Companies are facing increasingly asymmetric threats from sophisticated and well-funded adversaries and they must use the leverage that we have to outpace them," he concluded.

"As with any asymmetric struggle, it is in better technique and more rapid innovation where organizations can find advantage. That's where my focus has been and will continue to be."

Industry news

Jumio launches Jumio Go, a real-time, automated identity verification solution

Jumio is the first automated identity verification solution to integrate NIST/iBeta-certified liveness detection via FaceTec ZoOm which serves as a powerful chilling effect on would-be cybercriminals hoping to impersonate legitimate users.

Powered by AI, Jumio Go provides enterprises with a real-time, secure and reliable way to verify remote users, ensuring the person enrolling or logging in is who they claim to be online. Across a number of important use cases (e.g., renting e-scooters), verification speed is critical. Key benefits include:

- **Unrivaled speed:** Employs state-of-the-art AI, OCR and biometrics to deliver our fastest identity verification solution ever.
- **Data driven AI:** Exploits the power of massive production data sets, which include over 200 million historic identity verifications, and machine learning to spot patterns and better detect when an ID has been manipulated or altered.
- **Certified liveness detection:** Detects and deters advanced spoofing attacks (including deepfakes) with FaceTec's embedded NIST-certified liveness detection.
- **Global coverage:** Supports more than 500 ID types across the globe, helping enterprises scale to serve an increasingly international customer base.
- **Omnichannel support:** Supports a wide range of customer implementations, including mobile SDK (iOS & Android), mobile web, desktop and cloud API service options.

Jetico releases BestCrypt Volume Encryption - Enterprise Edition for Mac

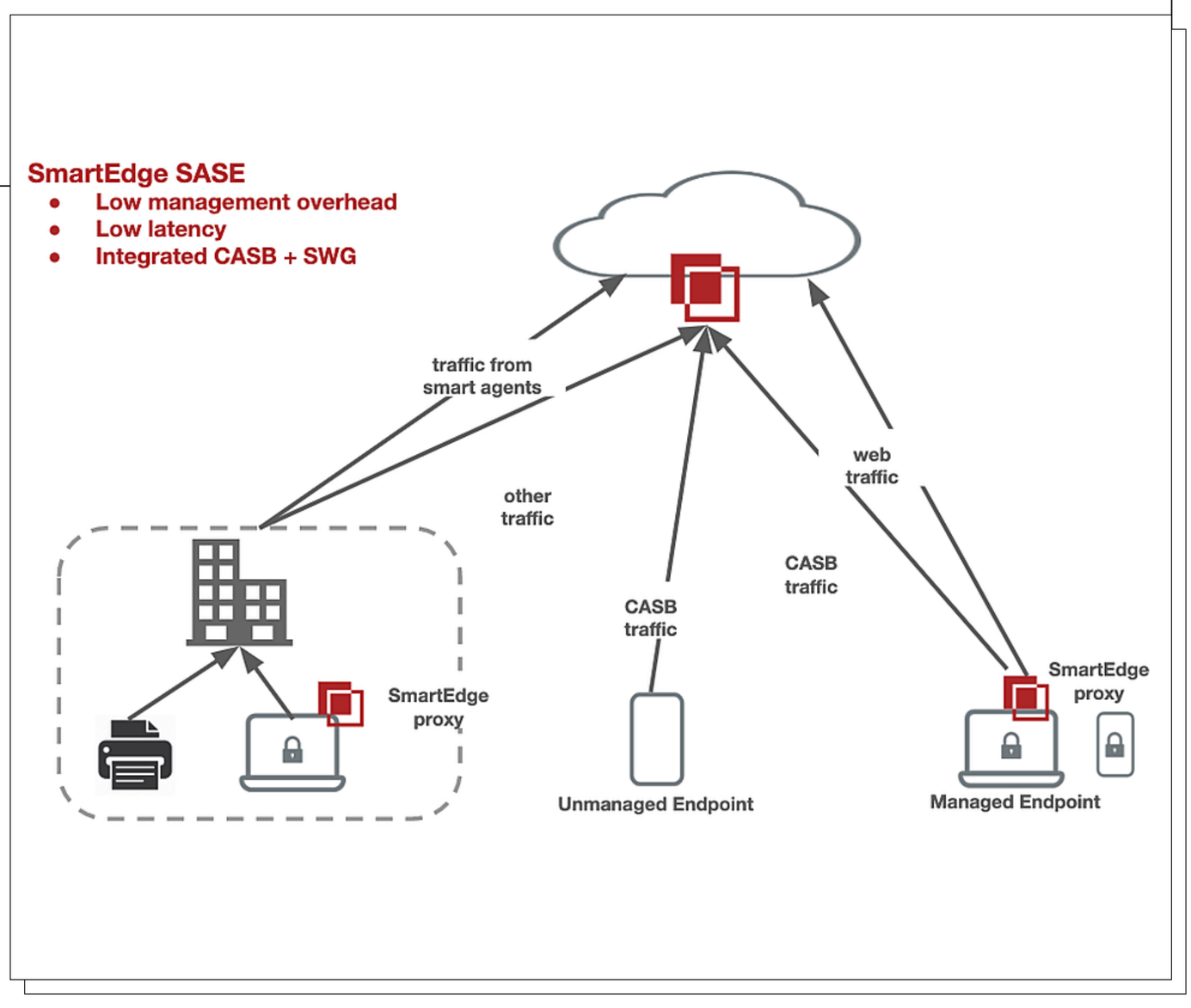
Expanding on many years of Windows support, Jetico delivers the world's only OS agnostic tool to encrypt Mac hard drive data with central management, both in cloud or on-premise.

For added convenience, BestCrypt Volume Encryption – Enterprise Edition can also run in the cloud, empowering admins to control all disk encryption activities from anywhere without needing to configure and maintain a dedicated server.

Bitglass SmartEdge architecture ensures high performance and no latency

Bitglass announced its SmartEdge architecture, delivering a Secure Access Service Edge (SASE) solution that simultaneously circumvents the management overhead and performance bottlenecks of competing solutions. With SmartEdge, endpoints carry their own on-device Secure Web Gateway (SWG), locally terminating SSL and inspecting all network activity for blocking threats and data leakage.

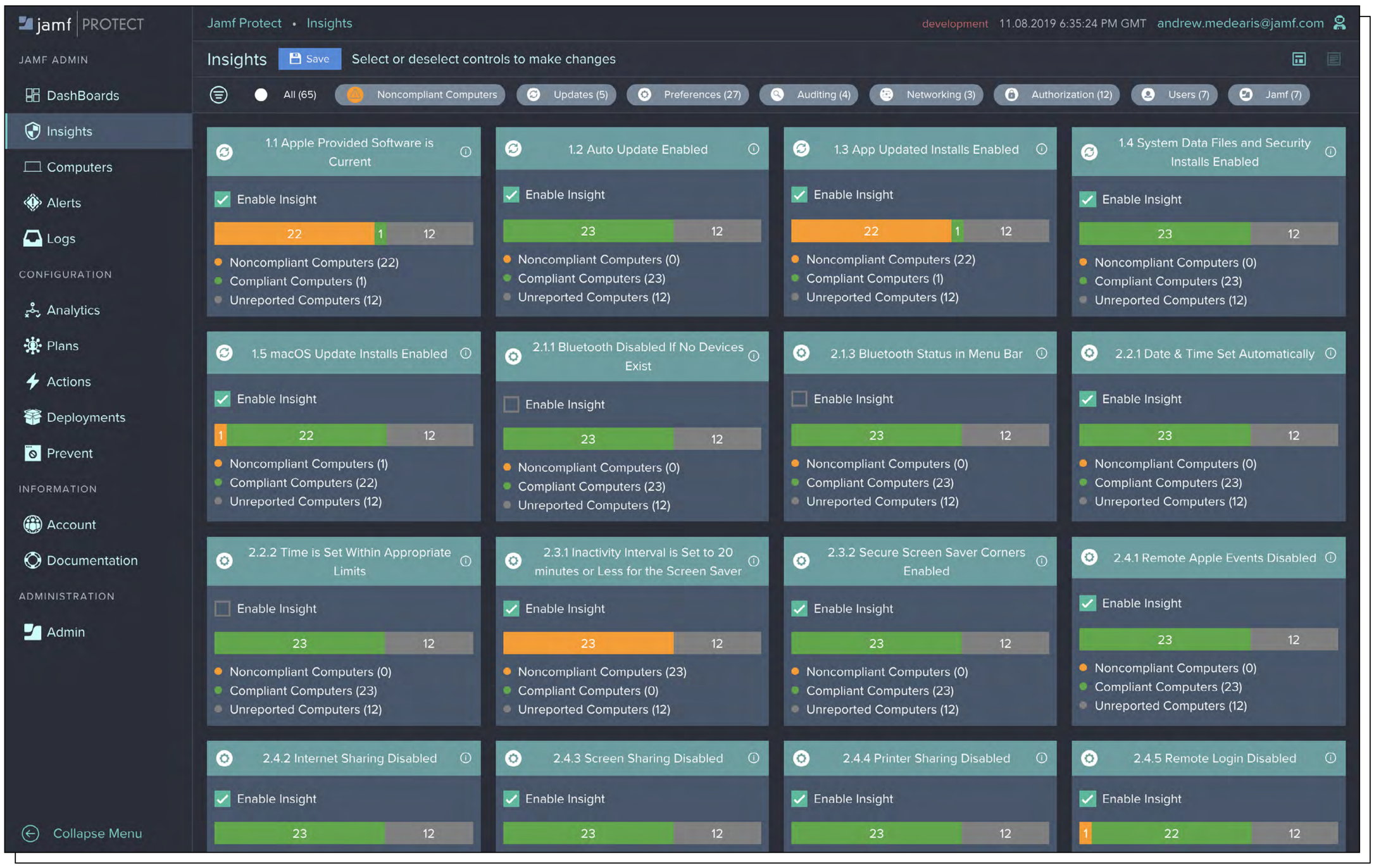
This architecture eliminates the extra network hop inherent in legacy SWG architectures, ensuring high performance and no latency. This cloud security solution delivers comprehensive SWG, Cloud Access Security Broker (CASB), and Zero-Trust Network Access (ZTNA) services in a combined solution managed from the cloud.



HITRUST CSF 9.3 adds CCPA, SCIDSA, and NIST SP 800-171 authoritative sources

HITRUST CSF now incorporates and harmonizes 44 authoritative sources, most recently adding one new data privacy-related and two new security-related authoritative sources, as well as updating six existing sources as compared to the previous release.

- California Consumer Privacy Act (CCPA) 1798 – requiring qualifying organizations to protect consumer data in specific ways as well as that consumers be able to opt-out sharing of their dana
- South Carolina Insurance Data Security Act 2018 (SCIDSA) 4655 – requiring qualifying organizations to have a comprehensive information security program and to report cybersecurity events
- NIST SP 800-171 R2 (DFARS) – providing guidance on protecting controlled unclassified information in nonfederal systems and organizations
- Updating various authoritative sources to latest versions: AICPA 2017, CIS CSC 7.1, ISO 27799:2016, CMS/ ARS v3.1, IRS Publication 1075 2016, and NIST Cybersecurity Framework 1.1.

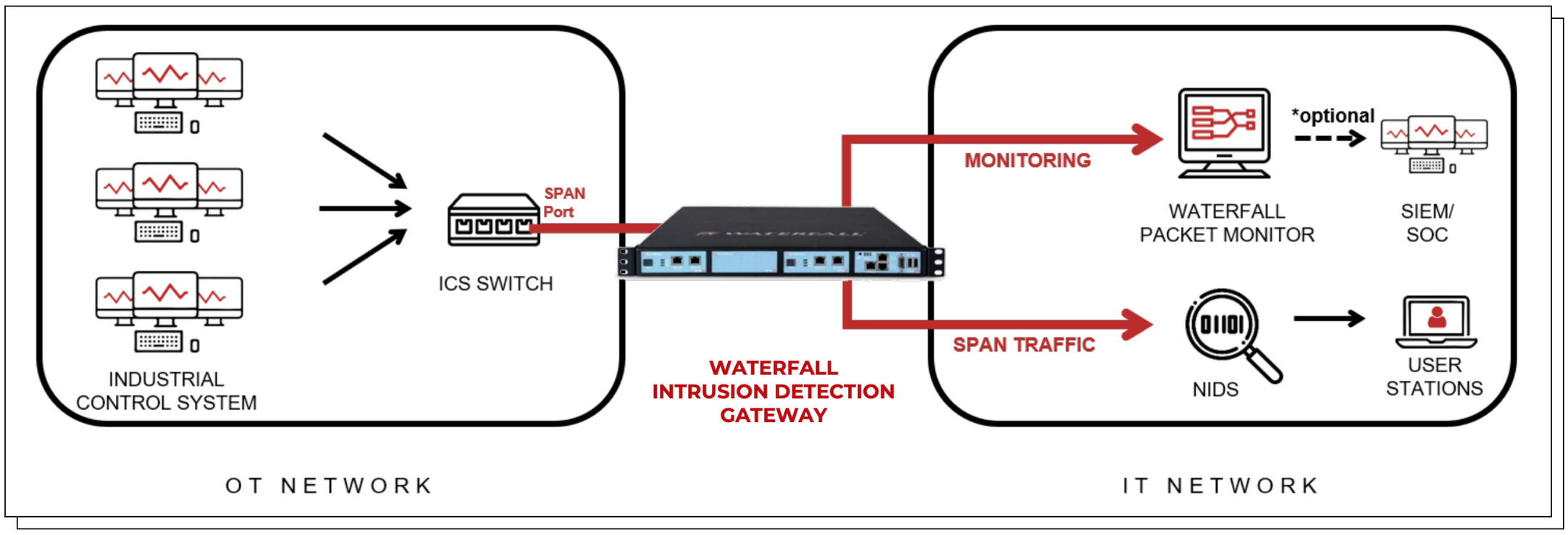


Jamf unveils Jamf Protect, an enterprise Mac endpoint protection solution

Jamf Protect leverages native Apple security tools and on-device analysis of macOS activity to create customized telemetry that gives enterprise security teams visibility into their macOS fleet and the ability to respond and block identified threats.

Jamf Protect ensures enterprise security while upholding the Apple experience end users crave, along with the ability to:

- **Gain native tool visibility** – Gain and extend visibility into macOS built-in security tools like XProtect and Gatekeeper for awareness and improved reporting, compliance and security posture.
- **Attain on-device activity analysis** – Receive real-time alerts to analyze activity on the device and choose whether to proactively block, isolate or remediate threats.
- **Secure data control** – Collect granular control over what data is collected and where it is sent, including directly into your existing SIEM.
- **Champion end-user experience** – Through Jamf Protect's kextless agent and minimal use of device resources, preserve an end-user experience that keeps employees productive and happy.
- **Support from day-one** – Using Apple's newly-released Endpoint Security Framework, teams can support the latest and most secure macOS experience from the first day a new operating system is available.
- **Audit against CIS benchmarks** – Understand and increase your security posture fleetwide with the ability to measure against CIS benchmarks.



Waterfall for IDS: Hardware-enforced security between OT networks and IDS sensors

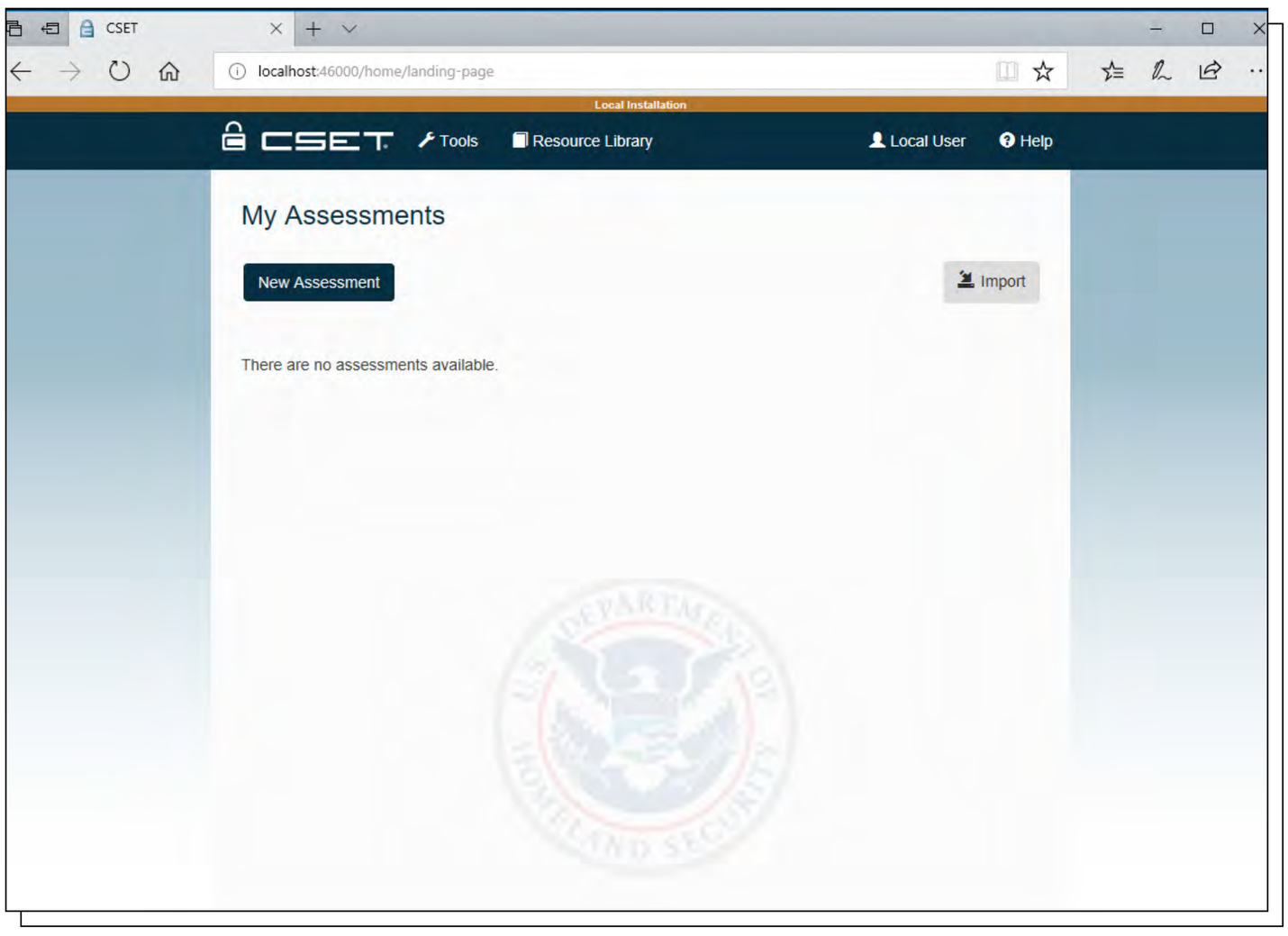
Waterfall Security Solutions, the OT security company, announced the release of their new product Waterfall for Intrusion Detection Systems (IDS), which enables intrusion detection sensors to monitor OT and ICS networks from IT networks without risk to the monitored networks.

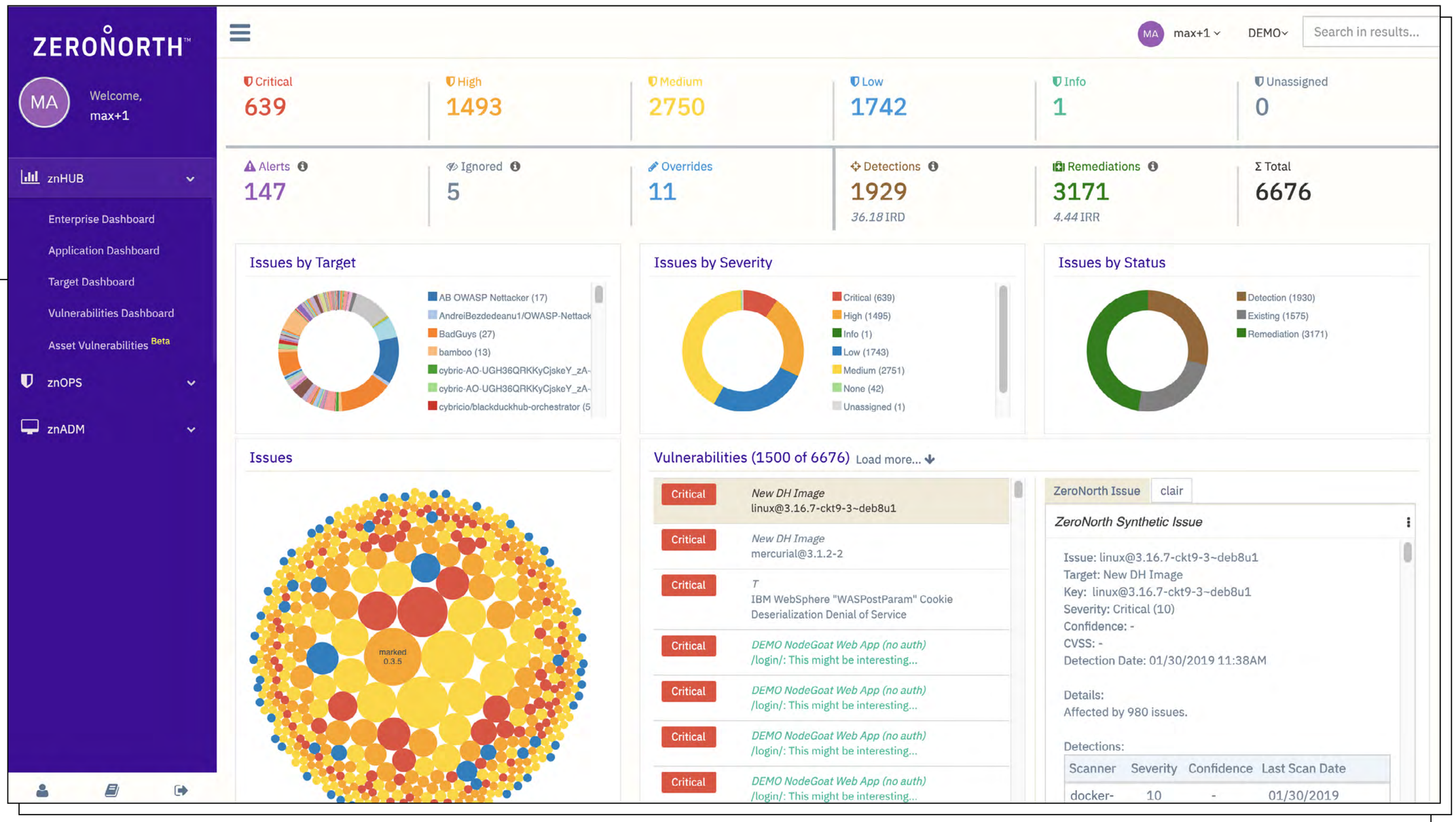
Waterfall for IDS provides hardware-enforced security that deploys transparently between OT networks and IDS sensors. Hardware-enforced security enables the OT sensors to be deployed confidently on IT networks where those sensors can be conveniently adjusted and updated by central security analysts.

“Extending intrusion detection systems into OT networks is a priority for most industrial enterprises,” said Lior Frenkel, CEO and Co-Founder of Waterfall Security Solutions. “Waterfall for IDS is an example Waterfall’s continued commitment to invest in and produce products and technologies that are vital to the security of modern, industrial enterprises.”

Cyber Security Evaluation Tool 9.2 released

The Cybersecurity and Infrastructure Security Agency (CISA) has released version 9.2 of its Cyber Security Evaluation Tool (CSET). CSET is a desktop software tool that guides asset owners and operators through a consistent process for evaluating control system networks as part of a comprehensive cybersecurity assessment that uses recognized government and industry standards and recommendations.





ZeroNorth's platform enhancements drive security into DevOps

ZeroNorth announced new platform capabilities that enable customers to more effectively build security into the SDLC and evaluate, prioritize and respond to risk based on business context. These enhancements are driven by new integrations with software pipeline and enterprise security platforms, and advanced filtering and analytics capabilities.

The ZeroNorth platform enables organizations to embrace critical digital transformation initiatives, such as DevOps, the cloud and microservices, without leaving security behind.

By orchestrating the many different scanning tools organizations rely on, the ZeroNorth platform reduces the resources required to implement a vulnerability management program. ZeroNorth also provides consistent data that enables organizations to proactively manage risk.

Moogsoft unveils all-in-one AIOps and observability solution for DevOps teams

Moogsoft Express is a new AIOps Cloud offering with native observability capabilities that helps DevOps and site reliability engineering (SRE) teams deliver continuous service assurance throughout the continuous integration/continuous delivery cycle. Moogsoft Express is built on Moogsoft's AIOps platform. This SaaS solution features intelligent noise-reduction, alert correlation, and native observability capabilities, including metrics collection and anomaly detection.

It also offers out-of-the-box workflows and integrations with notification and alerting tools, helping DevOps teams resolve incidents quicker and meet service level agreements (SLAs) with their customers.

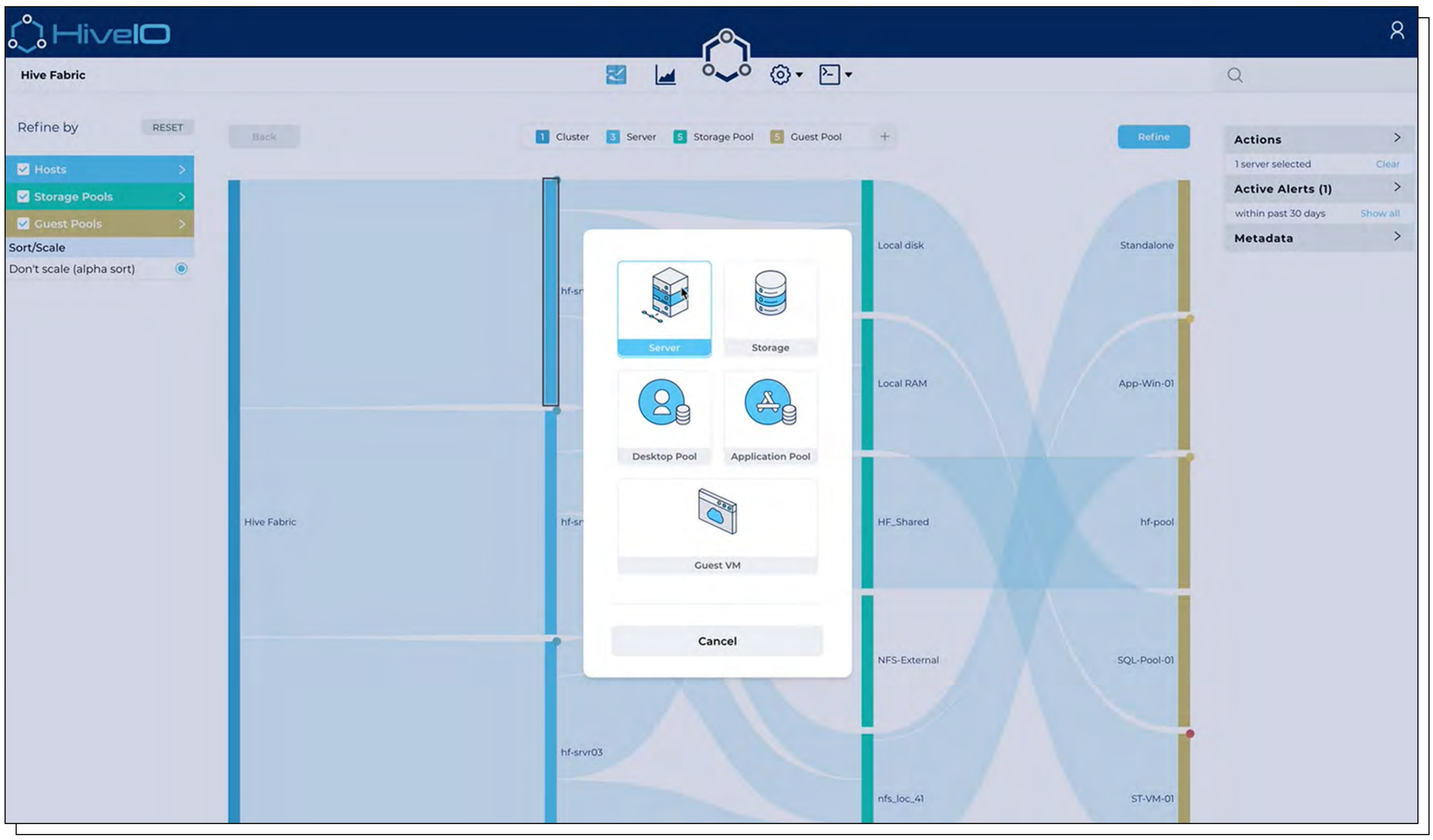
HiveIO Hive Fabric 7.4: Deploy virtualization technology without vendor complexity

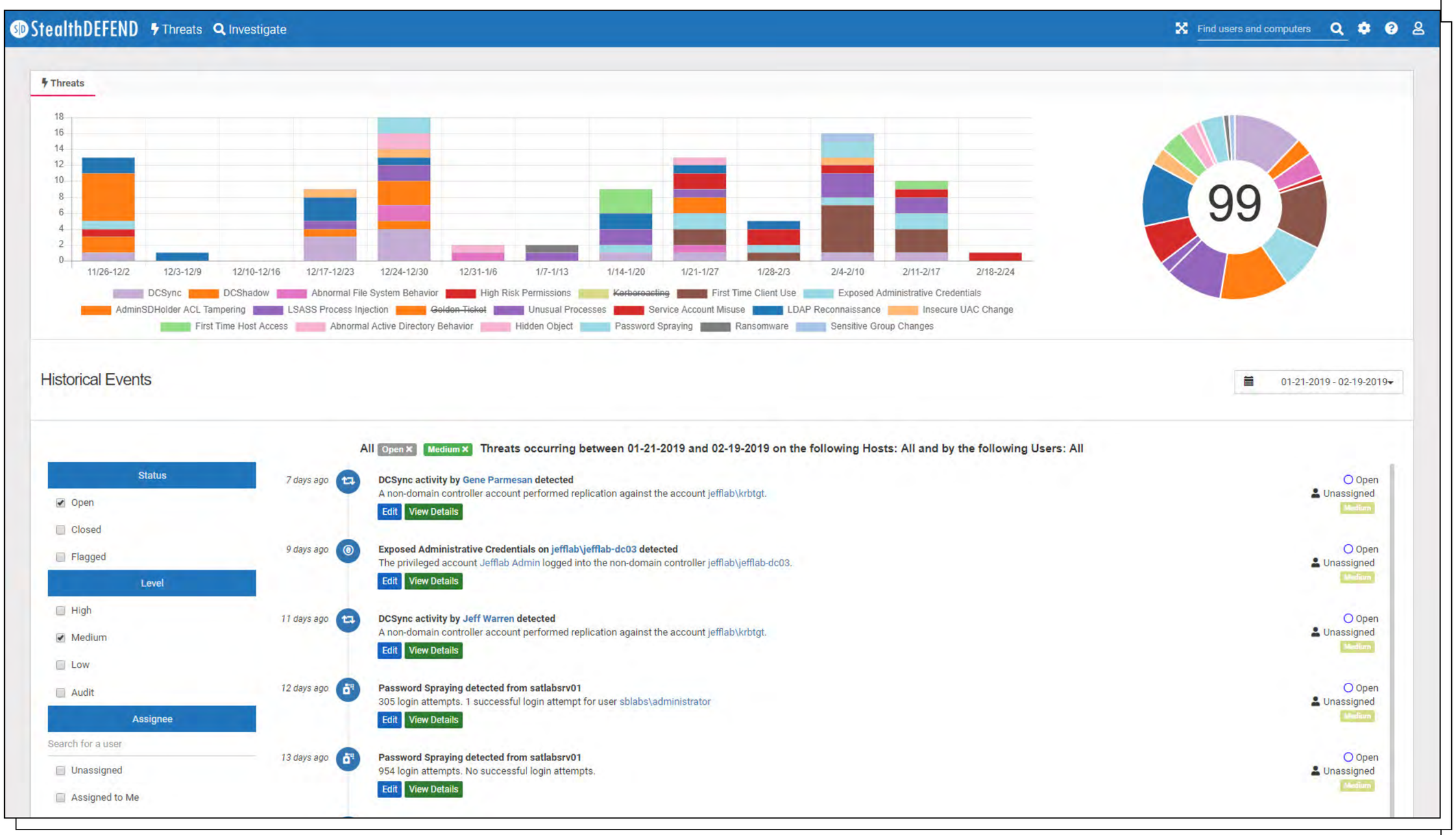
HiveIO released version 7.4 of Hive Fabric, an Artificial Intelligence (AI) ready solution that enables organizations to deploy virtualization technology without vendor complexity or the need for specialists. New features include:

Security enhancements: Security vulnerabilities are a top concern for IT leaders. Users can now apply an optional layer of security to the desktop broker by enabling two-factor authentication (2FA). This requires end-users to use both a password and second form of validation to access a desktop. The new authentication includes a wide variety of third-party 2FA and multi-factor authentication (MFA) support, including Microsoft Azure MFA and RADIUS enabling solutions like Imprivata.

Hive Fabric Gateway: With the new Gateway Mode, users can place a server or virtual machine (VM) running Hive Fabric in a demilitarized zone. This enhances the security of an environment through the separation of roles and responsibilities for each server. By assigning the Gateway role to a Hive Fabric server, it automatically configures itself and minimizes the functionality it provides in the cluster. Additionally, Gateway Mode reduces the number of internet-facing components for added security.

One-click cluster-wide upgrade: Administrative activities should be as simple as possible. Now, administrators can upload an update or new version, and automatically apply this to the entire cluster with a single click.





STEALTHbits releases StealthDEFEND 2.2, its real-time threat detection and response platform

Attackers continue to advance their techniques to infiltrate organizations, exploiting vulnerabilities in Active Directory and the structured and unstructured data that contain the sensitive information they want. Organizations concerned about data breaches and the rising costs to remediate them need advanced solutions to not only quickly identify, but automatically respond to an ever-increasing barrage of attacks and breaches.

With the enhancements delivered in StealthDEFEND 2.2, security professionals can now identify forged Kerberos Privileged Attribute Certificates (PAC) and detect when the Ntds.dit file – Active Directory's database – is being tampered with.

Both of these attack vectors are very difficult to detect via native means, potentially draining resources with no guarantee of detection. StealthDEFEND makes it simple to detect these threats and mitigate the risk these threats pose with less resources. Equally as important as the ability to detect these threats is the ability to automate the appropriate responses to contain them.

Sysdig Secure 3.0 provides enterprises with threat prevention at runtime

Sysdig Secure 3.0 provides enterprises with threat prevention at runtime using Kubernetes-native Pod Security Policies (PSP). PSPs are controls in Kubernetes that define the security conditions pods must follow in order to run.

Sysdig Secure 3.0 also includes the first incident response and audit tool for Kubernetes, giving enterprises the ability to reconstruct historical system activity. Enabling these capabilities are three new features: Kubernetes Policy Advisor, Falco Tuning, and Activity Audit.

This release focuses on securing Kubernetes environments throughout the entire lifespan – detecting vulnerabilities and misconfigurations during the build phase, blocking threats without impacting performance during the run phase, and enabling incident response, forensics, and audit.

The time and expertise needed to manually configure security policies often result in costly misconfigurations. With the Kubernetes Policy Advisor, Sysdig Secure auto-generates Pod Security Policies (PSP) to significantly decrease the time spent configuring security. Strict security policies reduce risk, but can also break applications. Sysdig validates policies through simulations, enabling teams to adjust misconfigurations before shifting to production.

Winning the security fight: Tips for organizations and CISOs

AUTHOR_Zeljka Zorz, Managing Editor, (IN) SECURE Magazine

For large organizations looking to build a robust cybersecurity strategy, failure to get the fundamentals in place practically guarantees a disaster.

If you ask Matthew Rosenquist, a former Cybersecurity Strategist for Intel (now independent), overcoming denial of risk, employing the right cybersecurity leader, and defining clear goals are the three most critical objectives for avoiding a negative outcome.

Getting things right

Every organization, large or small, begins with a belief they are not at significant risk. This denial is dangerous and can persist even when attacks occur, he says.

This denial must be addressed with facts and critical thinking and, once leadership accepts

the need for cybersecurity and the responsibility for addressing related risks, they must find and employ a good cybersecurity leader.

> *Being successful in cybersecurity is not accomplished by luck or by mistake.*

Rosenquist warns against employing experts from unrelated domains.

"Far too often organizations believe cybersecurity leadership is a simple project management or technical role and that just about anyone could be successful in it. I have seen excellent human resources, marketing, engineering, and finance managers be given the role, which eventually resulted in calamity," he shared.

Even worse: they might bring in staff they trust but are not competent, creating a closed group of novices that will flounder without even knowing they are failing.

> *Without clear goals there is also no way to gauge, justify, or prioritize security.*

"Being successful in cybersecurity is not accomplished by luck or by mistake," he remarked. "It takes contextual knowledge, special skills, experience, passion, and the relentless pursuit of understanding and mitigating risks in order to build the right foundations for success. A leader must use all of their proficiencies to be able to communicate risks, develop plans, articulate value, motivate team members, drive operation excellence, and to foster goodwill across the organization. In cybersecurity, the absence of quality leadership guarantees crises."

(The good news is that most large companies have overcome denial of risk and many are including cybersecurity skill sets into the C-suite and even the board of directors.)

Finally, it is essential that every security organization has clear strategic goals to satisfy stakeholders' expectations. Only with clear goals that the top organizational rung agreed upon can a long-term plan be developed – one that will be resistant to distractions and deliver sustainable value.

"Without clear goals there is also no way to gauge, justify, or prioritize security, therefore expectations will never be met and the program will eventually be viewed as a failure," he pointed out.

> *Unlike the straightforward operational challenges of information technology (IT), cybersecurity is forced to constantly change in order to meet and counter the persistence and innovation of the attackers.*

CISOs' challenges

Chief information security officers (CISOs) have their work cut out for them.

In order to be effective, they must:

- Understand, manage, and communicate the complex set of shifting cyber risks that exert pressure on the enterprise
- Garner support from the C-suite and the board levels as well as middle management, and influence the actions of every employee and vendor
- Address and stay in lockstep with the technology and process shifts implemented across the organization to secure potential vulnerabilities.

"Unlike the straightforward operational challenges of information technology (IT), cybersecurity is forced to constantly change in order to meet and counter the persistence and innovation of the attackers," Rosenquist noted.

"It is not just about addressing the weaknesses of yesterday or the issues of today, but also the new attacks that tomorrow will bring. The CISO's goal is to continually achieve optimal balance between the risks, costs, and usability factors for cybersecurity."

Constantly managing cyber risk

Eliminating all risks an organization may face would be astronomically expensive and extremely burdensome – the CISO's role is, therefore, to manage cyber risk through prioritization.
To decide what is most important to a risk management initiative, the goals must be defined, exposures identified, and possible avenues for control explored.

The organization's risk appetite is defined through an executives-and-board discussion. It should be expressed in both qualitative and quantitative terms for clarity and metrics tracking, he notes.

> *It's important for CISOs to realize what the board is there to do and tie cybersecurity to their objectives.*

"For example, it may include conditions like 'no data breaches involving sensitive customer information', compliance to all regulatory requirements, and less-than 4 hours downtime per quarter due to cyber-attacks. The list can be as extensive as desired but must also accompany estimations for costs, friction to system usability, and impacts on employee productivity," he explained.

Once defined, these targets become the overall goal for the cybersecurity program and based on those goals the CISO can identify what is most important to secure, what technology constitutes the digital ecosystem, what controls are already in place and what controls should be put in place.

The answer to the questions of what is most important to secure and how should also be influenced by the CISO's understanding the opposition.

"If you know the goals, methods, and capabilities of the attacker archetypes that constitute the primary threat to the security goals, it is possible to identify the most valuable avenues for investment to intercept the likely attacks," he concluded.

Garnering support from the board and the C-suite

It's important for CISOs to realize what the board is there to do and tie cybersecurity to their objectives.

"Be clear and speak in plain terms, don't try to overwhelm them with technical or security terminology, don't use FUD, be open and pragmatic," he advised.

"Use industry data as benchmarks and always frame challenges in respect to the overall goals. Be as clear as possible and consistent with the framework of your metrics over time. Give your insights and recommendations and back it up with logical reasoning. You are their expert. Be ready to help them understand when asked."

Boards, he explained, are about strategic positioning and success. They do not focus on minutia, even if it is interesting to the CISO.
Most boards want to hear the high-level issues, have an opportunity to ask questions, want to

understand if compliance is being met, and how the security posture compares to peers. If issues are being solved, they want progress reports and to know if anything else is needed.

At the same time, the CISO must be able to communicate the value proposition in terms of the executive management's business goals. Here it's less about strategy and more about the goals of the individual executives.

"All the profit centers want to know how security can be a competitive advantage or protect the reputation with their accounts. For example, Sales and Marketing may be most interested in keeping their customer lists and revenue targets confidential. Legal may be most concerned with regulatory compliance and data breaches. IT is always concerned with downtime and malware cleanup. The CISO must understand the requirements, be a team player, and convey the benefit to foster necessary support," he noted.

Integrating new tech

For every new technology that is implemented in the organization, it's important to evaluate the unintended risk consequences and adapt as necessary.

Hacking tools and methods are constantly being developed and security teams must be vigilant in maintaining awareness and proactively land risk mitigation capabilities across the prevention, detection, and response cycles.

New security tools represent both an opportunity and a risk, Rosenquist pointed out. "In many cases, better tools can reduce the risks, costs, or friction of usability and productivity. These may be worthwhile to consider adopting. Alternatively, if peer organizations shift to better tools ahead of you, this makes you a comparatively easier target, which may earn the attention of attackers seeking an easy victim."

Of course, not all security products are worth the money.

"The security industry is cutthroat and still full of misdirection, fear-mongering, snake oil peddling, and immature products. It really is a 'buyer beware' market," he added, and advised CISOs to look beyond the marketing noise when evaluating the latest offerings.

They should:

- Listen to promotional materials with a high degree of skepticism
- Dive into the methodology behind metrics
- Verify claims
- Tap industry experts for opinions
- Reach out to peers who have firsthand knowledge of the product's effectiveness.

Finally, he noted, for those solutions that look promising, CISOs should evaluate the products in-house to prove real usefulness and align results to the organization's risk goals to determine the value.

His prediction for the coming years is that more and more security solutions will be embracing AI to better manage risks.

"Specifically, AI will be leveraged to handle the scale of more threats in autonomous ways, provide adaptive controls based upon unscripted 'learned' criteria, allow for faster detection of malicious activities across silos, self-develop customized responses, and provide better prediction insights all at a lower cost."

A NEW PRESCRIPTION FOR SECURITY AND IT'S FREE.

Introducing Qualys Global IT Asset Inventory®

☠ WARNING! SIDE EFFECTS MAY INCLUDE

Actually knowing what's on your global hybrid-IT environment (on prem, endpoints, clouds & mobile)

Improving your security and compliance posture

Better decision making using enriched asset data

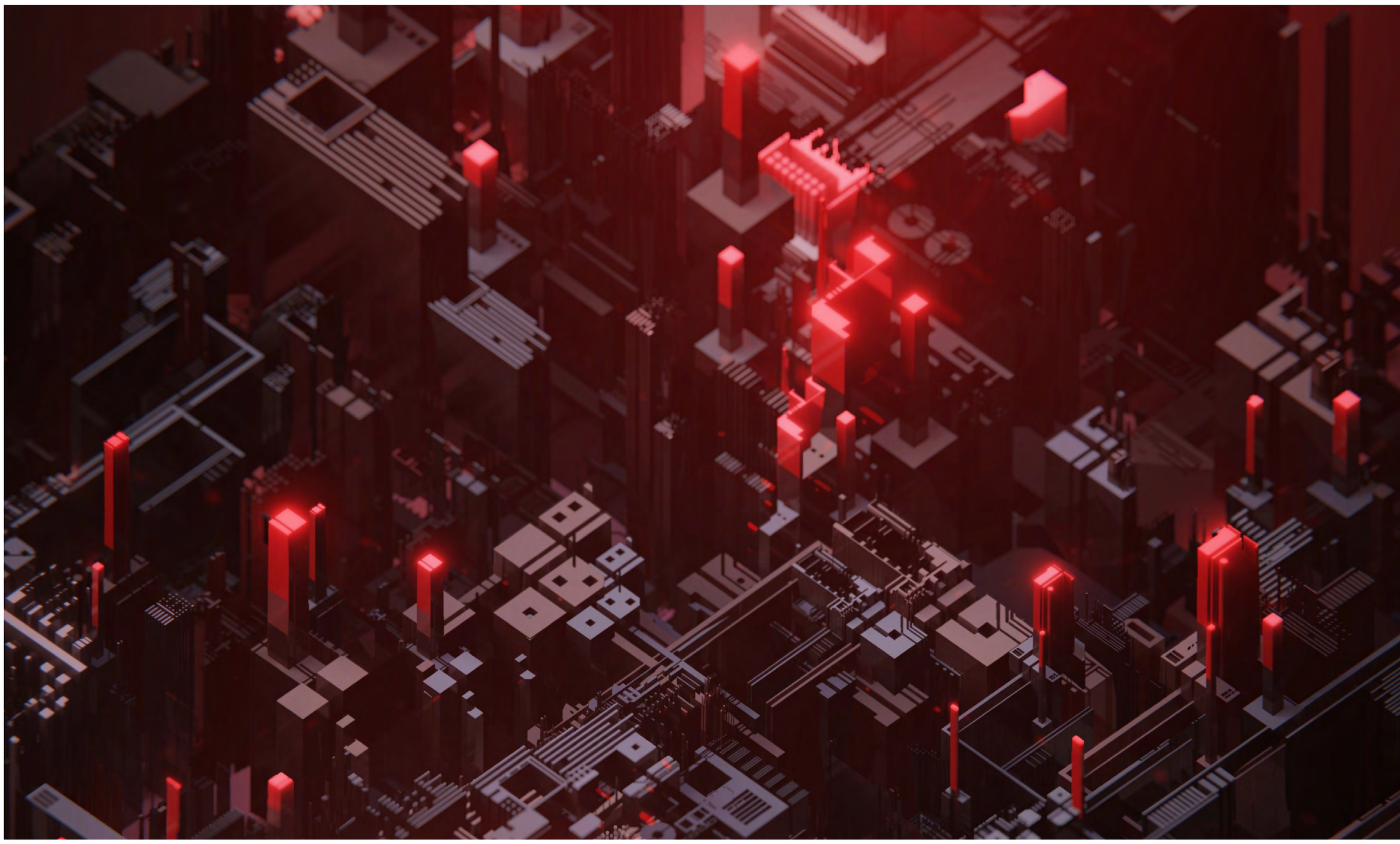
Easily finding what you need via automated classification

Finally having clean, uniform data for a single source of truth

Getting that promotion you always wanted

QUALYS.COM /INVENTORY

Qualys®



Want to build a SOC? Here is what you need to know beforehand

AUTHOR_ Nimmy Reichenberg, Chief Strategy Officer, Siemplify

How can you create a cybersecurity hub within your organization?

There is no arguing the fact that networks are continually growing in complexity and the cyberattack surface is constantly expanding. A critical step in building a stronger security posture and a more robust data protection strategy is a 24x7 facility whose mission is to monitor, detect, investigate and resolve active threats. When the inevitable attack happens, timely identification, reaction and collaboration is everything, and a business with a well-functioning security operations center (SOC) will be quicker and more coordinated in their response than one without.

According to Ernst & Young's Global Information Security Survey 2018-19, the average cost of a data breach is $3.62 million, yet more than

half of companies report they have no program (or an obsolete one) for one or more of the following areas: threat intelligence, vulnerability identification, breach detection, incidence response, data protection and identity and access management – disciplines which all originate or are closely tied to the SOC.

If you're a mid-to-large enterprise, you should be thinking about building an internal SOC.

A Siemplify study, The Road to Security Operations Maturity, conducted by the Cyentia Institute, found that "the majority of (security operations) programs are just starting their maturity journey or are midway through it. Only 16% claim to have reached peak maturity."

How can you create a cybersecurity hub within your organization? Here is a primer to designing, building and maintaining a successful SOC.

What is a SOC?

SOCs act as the front line to your cybersecurity efforts. SANS defines SOCs as "a combination of people, processes and technologies protecting the information systems of an organization through proactive design and configuration."

That means design and configuration must be carefully considered across each of these axes: staff, technology and the processes and workflows used for both, plus the intricacies of how these all work together for optimal performance.

A round-the-clock team is needed, since cyber attackers don't follow a 9-to-5 schedule.

A SOC is typically housed in a single location on-site, although some organizations have multiple distributed SOCs for global coverage.

What does the SOC do?

Within the SOC, the team's job is to (with the help of technology and repeatable processes) monitor the state of the IT systems across the organization, detect any incoming threats and internal security events, and mitigate the effects of any security incidents that occur.

Which businesses need an on-site SOC?

If you're a mid-to-large enterprise, you should be thinking about building an internal SOC. You likely already have a security team, but you may not have pooled resources to make them as effective as possible.

Smaller organizations with particularly sensitive or valuable data that need safeguarding should also consider an on-premises SOC, but the option exists to outsource security operations functions to a managed security services provider (MSSP). Some larger companies also choose to delegate all or a portion of their security operations needs to an MSSP.

Who should staff your SOC?

Your team should be made up of a mix of people, including experienced analysts, engineers and managers. A round-the-clock team is needed, since cyber attackers don't follow a 9-to-5 schedule. The number of employees needed for each shift will depend on your company's size; however, make sure that there is always at least one manager on hand, as well as experience across both engineering and analyst roles. How resources are allocated at different times of the day will be dependent on multiple factors. It's up to you to

decide the mix of experience and roles each person on the team fulfills, while still ensuring adequate staffing at all times.

Your SOC should be one of, if not the most, secure rooms in your facility.

For risk management purposes, it's a good idea to have an MSSP on call to augment your team in case of staff illness or large incidents. This amplified staff component will also need to be well-versed in how your systems are configured if they're to be on-site.

What equipment does a SOC need?

In terms of hardware – aside from the obvious multi-screen workstations for the team – you should have a wall of monitors set up to provide an overview of the current state of systems and recent historical data. This way, your SOC staff has an overview of all system information, always available at a glance.

Your SOC should be one of, if not the most, secure rooms in your facility. This means there have to be physical barrier systems, such as swipe card access, biometrics and PIN code access, to guard entrances to it. For best practices on physical security, you can reference *ISO 27001 - Annex A.11: Physical & Environmental Security.*

What technology is needed?

A comprehensive combination of tools is needed to provide full security coverage of your information systems. The essential components of any SOC include a security information and event management (SIEM) system, an incident tracking and management system, a threat intelligence platform, packet capture and analysis tools and automation tools.

Combined, these will help deliver:

- Network monitoring
- Endpoint management
- Asset discovery
- Threat intelligence
- Behavioral monitoring
- Data loss prevention
- Ticketing systems
- Policy compliance
- Incident response
- And more

However, generating meaningful alerts for your analysts is only the beginning. SOCs need to define the processes by which they handle the various alerts from initial triage through investigation, containment and response. Furthermore, to avoid alert overload and analyst burnout, these processes should be automated as much as possible. For these reasons, both new and existing SOCs are increasingly implementing a security orchestration, automation and response (SOAR) platform.

The processes and workflows that your SOC follows need to be optimized because manual checklists can introduce human error.

SOAR solutions help build and automate consistent response processes (commonly referred to as "playbooks" or "runbooks") that bring together individual security tools, allowing SOC teams to orchestrate and manage them more efficiently from a single platform. In addition, SOAR helps to mitigate alert overload by helping teams automatically close false positives and zero in on threats that truly need analyst attention.

What processes/workflows need to be followed in a SOC?

The processes and workflows that your SOC follows need to be optimized because manual checklists can introduce human error.

Incident response playbooks are fundamental to the work of the SOC. They are needed to cover common use cases, like phishing or malware events, in a repeatable manner. Playbooks are typically coded for automation and can include recipes like creating tickets on actionable events, notifying teams after incidents, and more.

The aim of the majority of playbooks is to automate tedious Tier 1 tasks (detecting and identifying events) that would usually be done by analysts. This means you have more resources to dedicate to Tier 2 (mitigating attacks) and Tier 3 tasks (optimizing operations).

How to attract internal support for a SOC

Wondering how to sell the idea of a SOC to organizational stakeholders? Start by conveying, in understandable terms, the serious and evolving nature of the threat landscape with facts and figures. Consider the following:

- A total of 16,555 new vulnerabilities were discovered in 2018, as opposed to 6,447 in 2016 (Source: CVE Details).
- Web attacks are up 56%, and supply chain attacks up 48% from 2017 to 2018 (Source: Symantec).
- Regulatory compliance (made manageable by orchestration) is more important than ever with ever-changing data privacy legislation, including GDPR and HIPAA.
- Penetration testing that evaluates the weaknesses of your IT environment will surely turn up findings that make you second guess your ability to stave off attacks and breaches.

The basic idea behind stakeholder buy-in is to convince others that cyberthreats are on the rise and always evolving, a particularly scary thought when fueled by the prospect of artificial intelligence. The value of business data, reputation and potentially ongoing viability of a company is at stake when it comes to significant and/or ongoing security incidents. The better organized you are to fight these threats, both now and in the future, the better chance you have to protect systems, hence the need for a SOC.

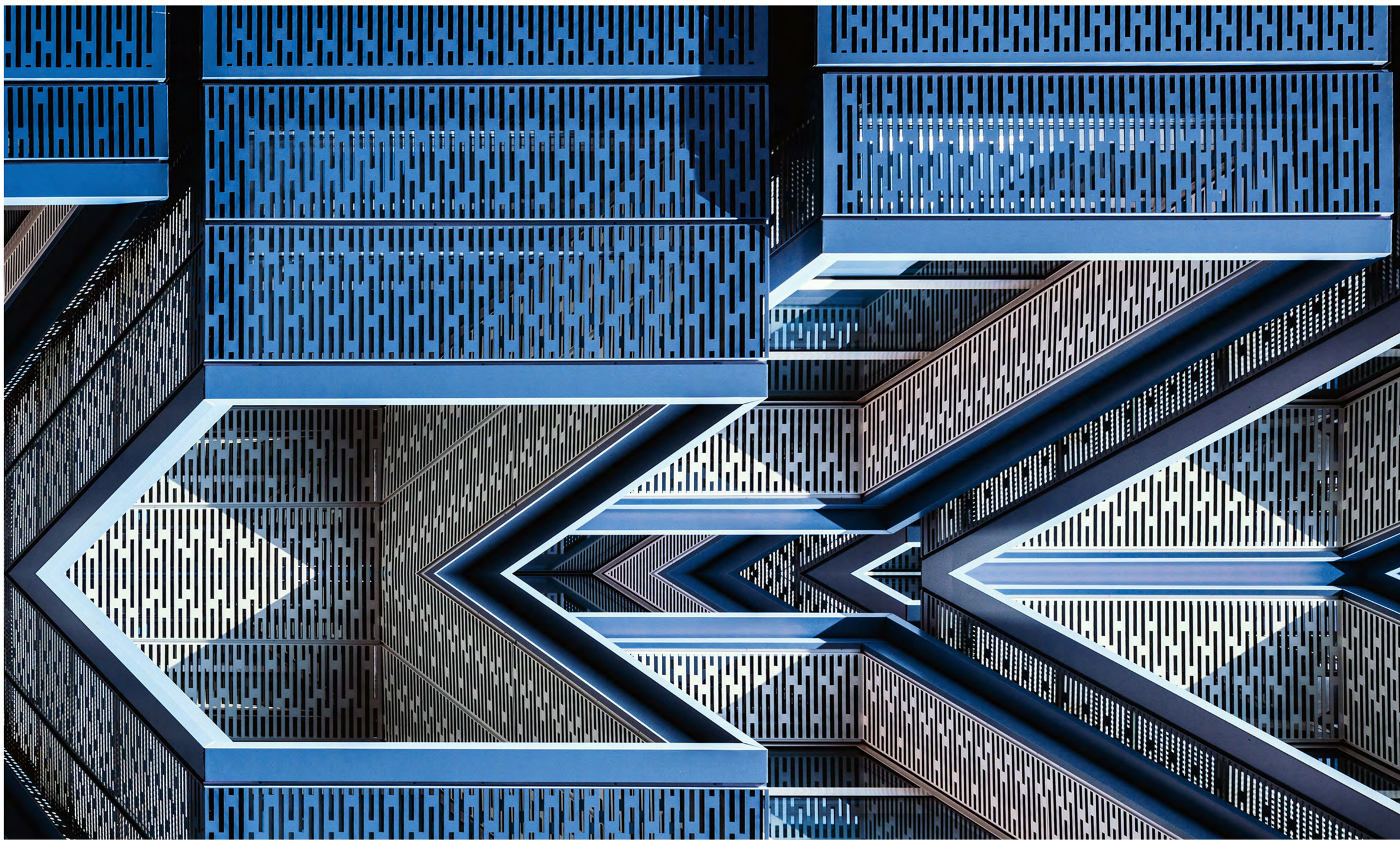
Going down the MSSP route

If you decide to use an MSSP for your SOC, you have to evaluate whether it can meet your needs. They should fit the requirements outlined above for a SOC (and then some!), as they're offering services to multiple clients.

Your service-level agreement should cover round-the-clock monitoring and an always open line (preferably multiple lines) of communication.
The MSSP should be experienced in protecting organizations of your size and network complexity, plus have advanced threat monitoring capabilities that are easily demonstrable to you. You should receive daily reports, plus more comprehensive weekly and monthly reports, as well as any relevant threat information as it comes to hand.

Next steps

Your next steps should be to develop a formal plan and budget strategy, highlighting the increasing threat that cyberattacks and malicious insiders pose to business information. Be sure to include how you plan to orchestrate all of your detection tools and automate alert and case handling from a single platform. Doing so will lead to a more efficient and effective SOC, and happier analysts.



You are using Active Directory (AD) every day, every hour, every minute when you log into your device, open your emails, access an application, or share a file.

But, guess what, it’s also used by hackers on a daily basis. Simply put, when attackers take control of your AD, they inherit godlike powers over your IT. Sweet.

Product showcase: Alsid for AD

Analyzing attack vectors: How attack pathways are born

Active Directory itself is a robust product that suffered few zero-day vulnerabilities in its history. However, Active Directory implementations inevitably become weak. Every change in business architecture, each M&A operation, every server that you add will alter your AD topology. Give it a year, and any AD will grow into a beast you can’t comprehend anymore.

Past that point, it becomes impossible to understand the possible ripple effects of the changes made to your AD. Some have a significant impact on your security posture, and you just won't know about it.

AD security tactics that don't work

First: SIEM-based monitoring. Identifying AD risks with SIEMs inescapably requires writing dedicated rules, which often generate an overwhelming flood of false positives. Not even mentioning that the most effective attacks, such as DCShadow, simply don't leave any logs behind.

Now: basic hygiene. Admittedly mandatory to any effective defense, maintaining proper hygiene for AD is a challenge, to say the least. Every simple task requires a custom script to run constantly. Chain all checks together, and you'll have a system that just doesn't work IRL.

Finally, the handful of dedicated AD solutions that automate correlation and hygiene processes all require locally-installed agents and elevated rights, which makes them impractical for any sensible AD admin.

Alsid for AD: A new approach to Active Directory security

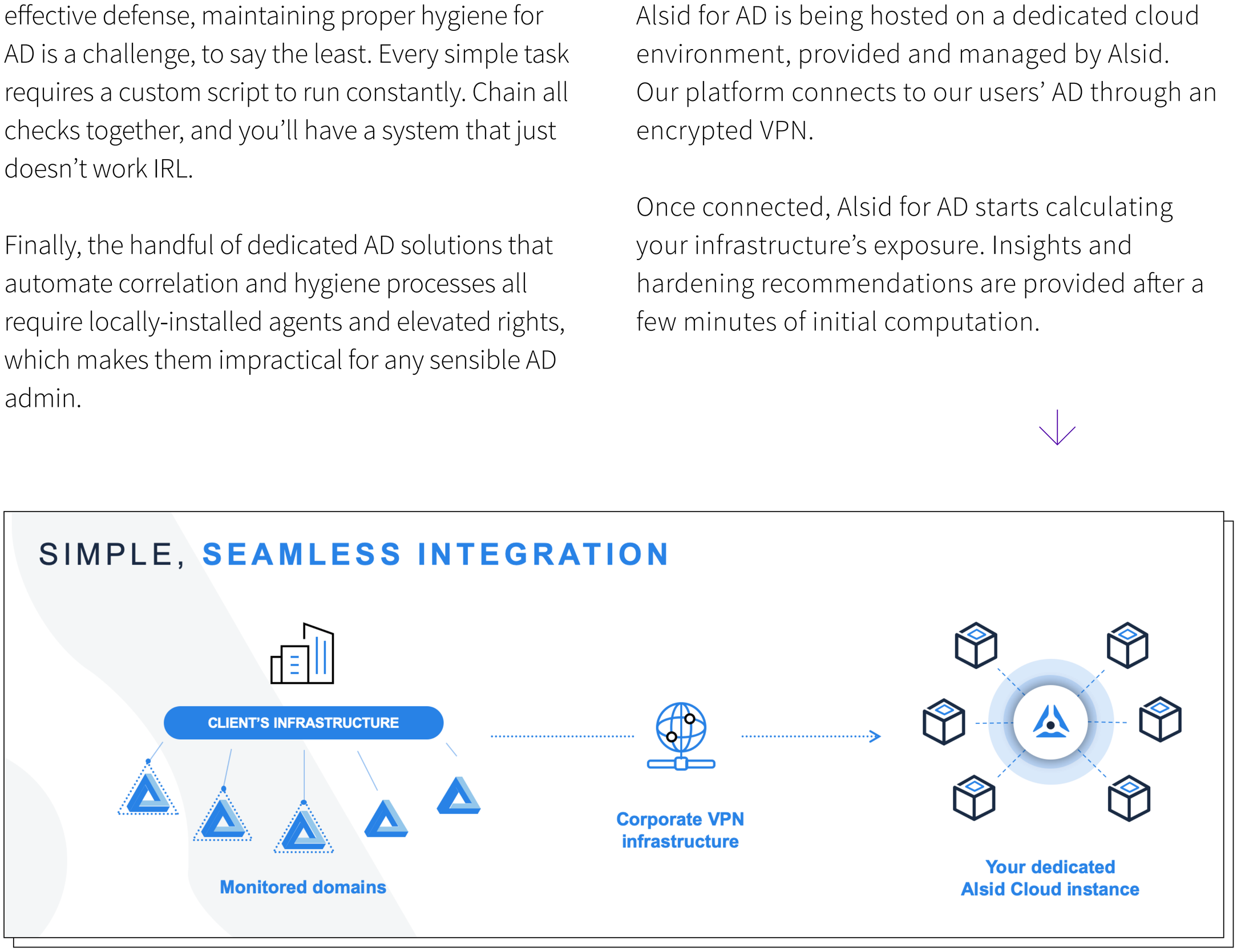
Our approach is security focused, targeting attacks patterns and providing AD-specific insights and controls for hardening your Active Directory, detecting breaches in real time, and accelerating AD forensic investigations.

From a user experience standpoint, Alsid for AD is agent-less, makes zero change to the Domain Controller and requires no privilege at all.

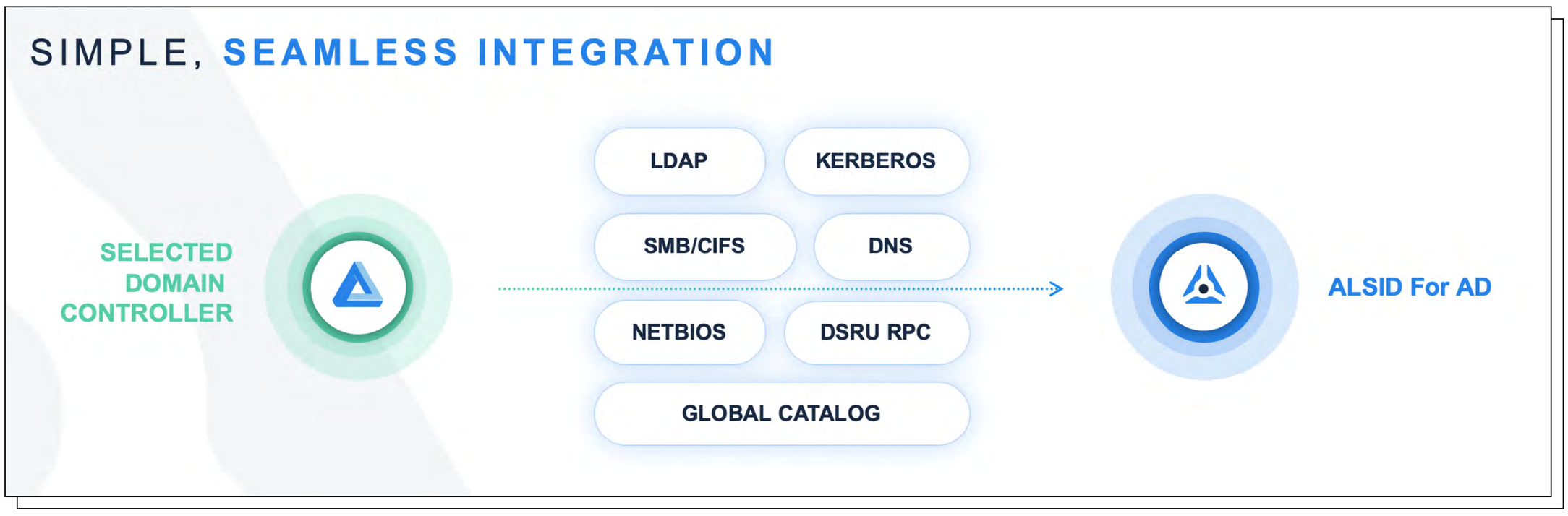
Setting up Alsid for AD

Alsid for AD is being hosted on a dedicated cloud environment, provided and managed by Alsid. Our platform connects to our users' AD through an encrypted VPN.

Once connected, Alsid for AD starts calculating your infrastructure's exposure. Insights and hardening recommendations are provided after a few minutes of initial computation.



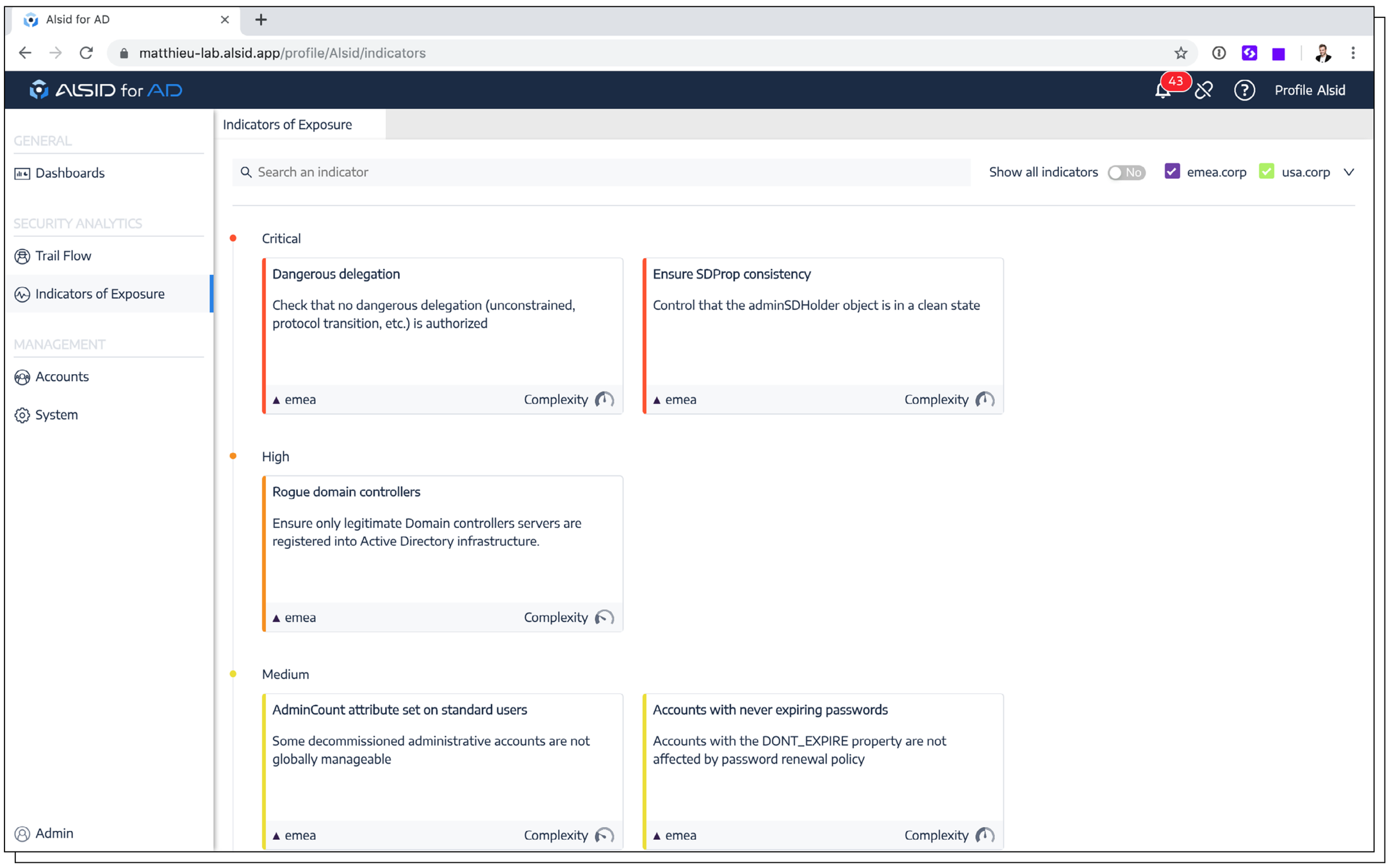
SIMPLE ARCHITECTURE DESIGN



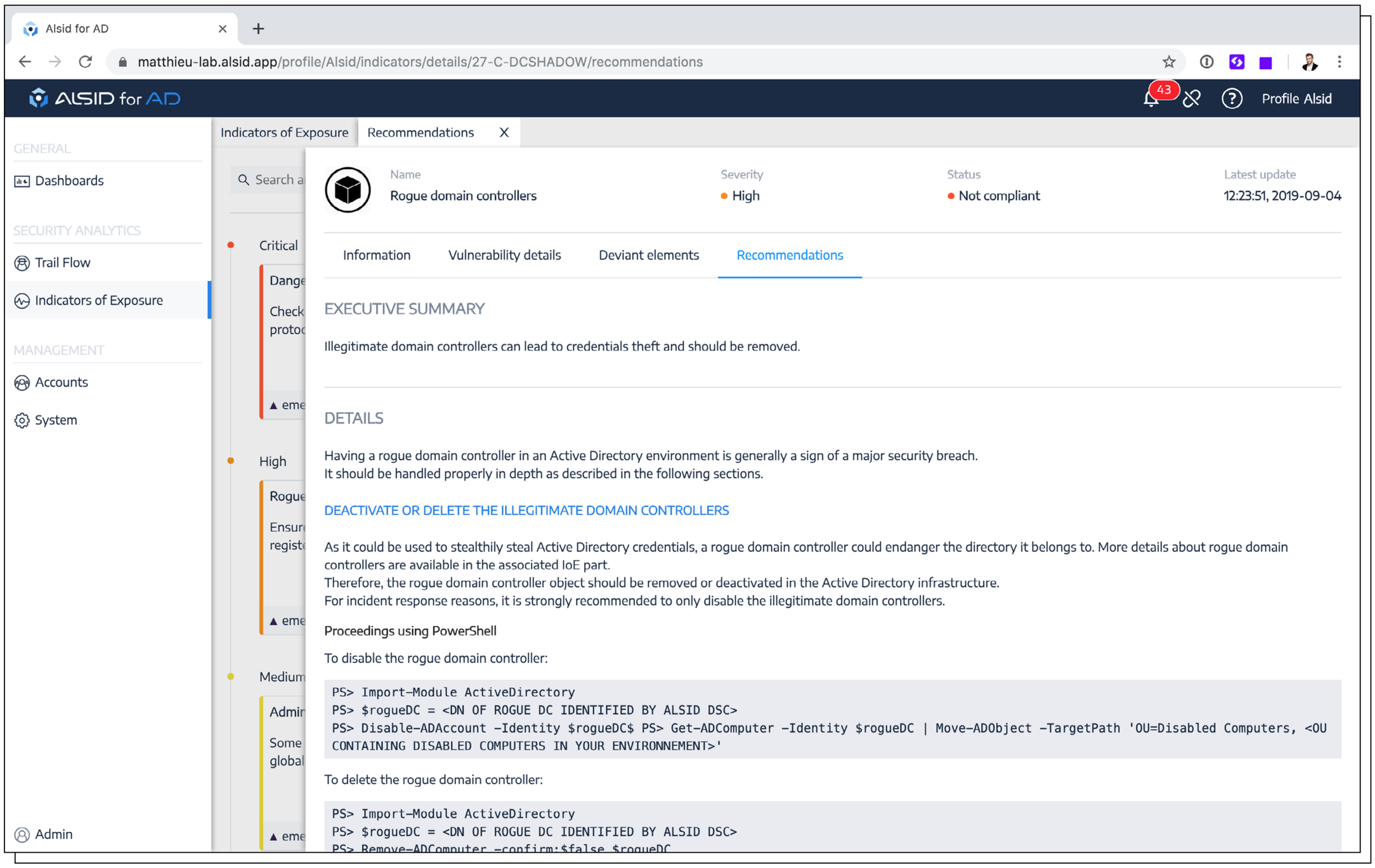
ALSID RELIES ON STANDARD PROTOCOLS ONLY

All sensible defense strategies start by reducing threat exposure. Dwarfing the adversary's ability to exploit openings is a critical step… that's easier said than done for Active Directory, considering its size and complexity.

Alsid for AD constantly scans your AD to find existing misconfigurations and weaknesses. Those Indicators of Exposure (IoE) provide descriptions, threat scores, estimations of remediation costs, and step-by-step mitigation plans. A comprehensive list of IoE is provided at https://alsid.com/indicator-exposures-reference



LIVE INDICATORS OF EXPOSURE



DETAILED REMEDIATION PLANS

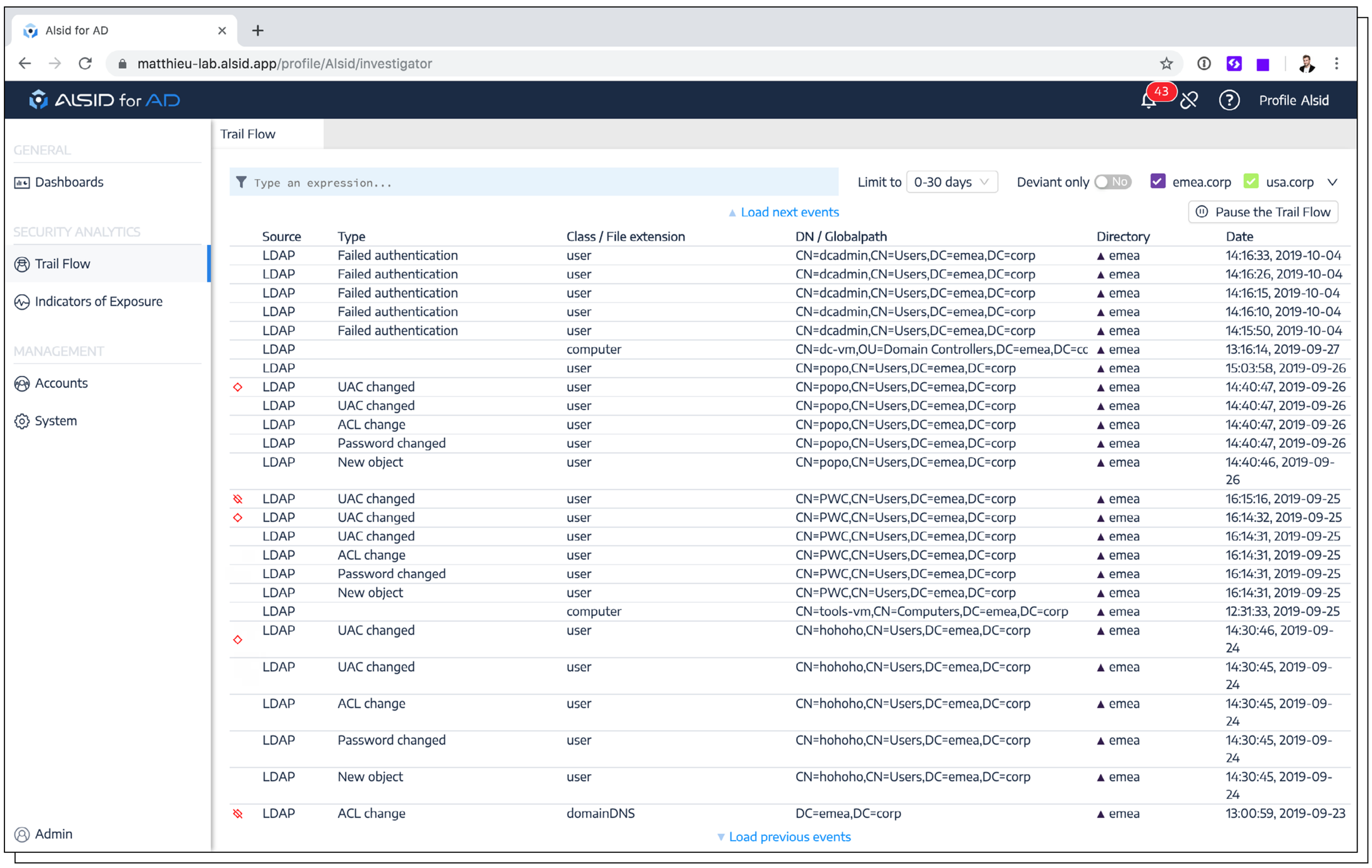
Most solutions available today are either impractical or, at best, detect attacks after they've succeeded, which effectively defeats the purpose of any sensible defense.

Alsid for AD capabilities

Alsid for AD combines 3 unique characteristics:

- **True real-time monitoring** – Our AD-native platform does not rely on Windows logs and provides insights in true real-time. Considering the vast amount of damage a rogue admin can do in only a few minutes, real-time is not an option… but remains unseen in other solutions.
- **AD-native intelligence** – Alsid maintains an always up-to-date intelligence database of attack patterns. Our research team constantly enriches our platform's detection engine accordingly, making it market's gold standard when it comes to attack coverage.

- **Before-compromise detection** – AD-targeted attacks are chains of several events that, together, eventually lead to a breach. Alsid for AD, very uniquely, detects each of these events independently, so our platform will alert its users before the eventual breach happens. So, our users can remediate to attacks before they succeed.



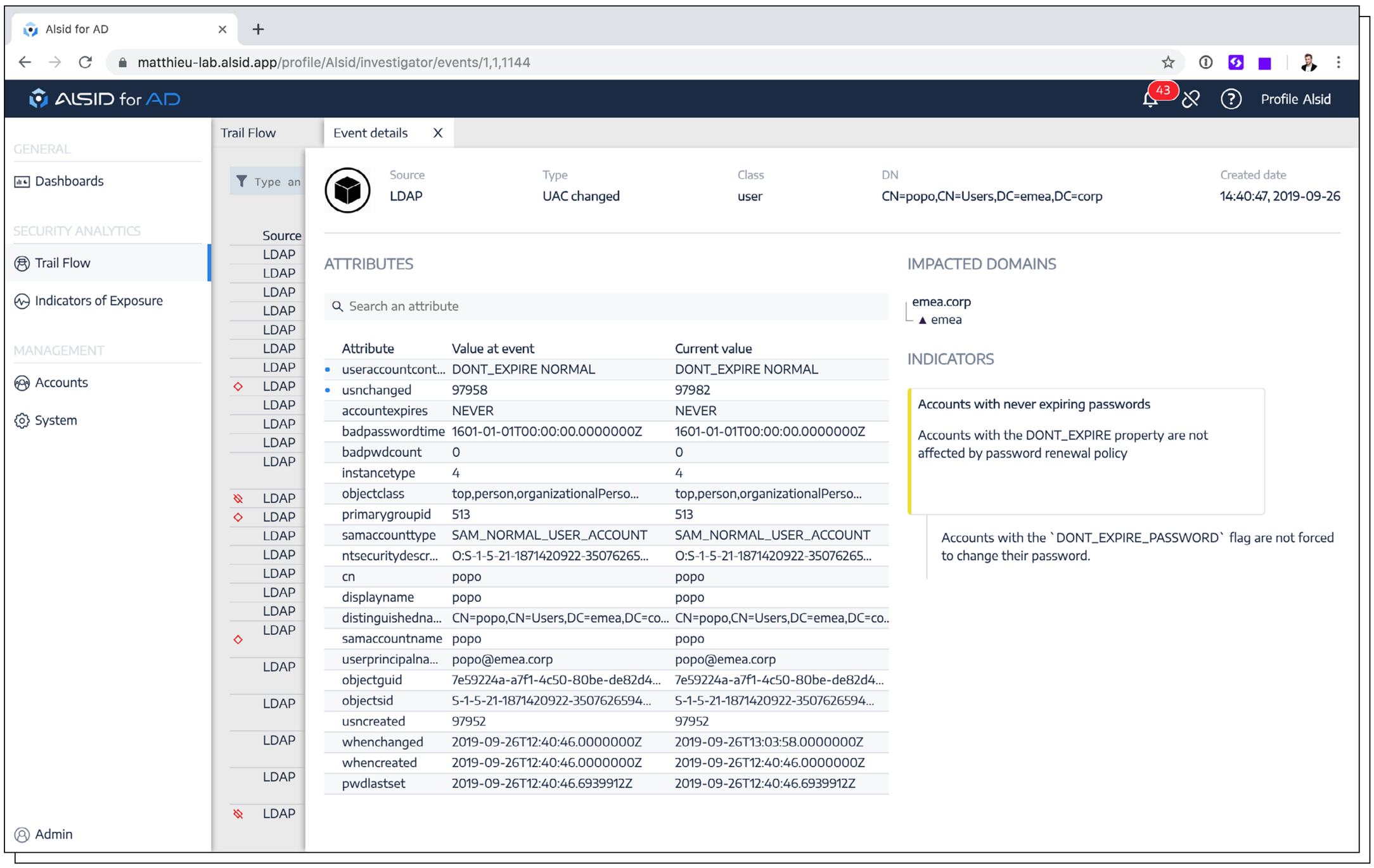
REAL-TIME DETECTION AND ALERTING

Responding to breaches: How to investigate and hunt

After a breach, incident responders investigate the attack to inform remediation. For AD, most practitioners use Microsoft Event logs, an extremely inefficient task considering the huge volume of (mostly irrelevant) data they find there. Alsid for AD keeps a complete history of all security-meaningful events. Using our advanced query system, investigators drill down into these events

with a speed and accuracy only a true AD-native technology permits.

Furthermore, Alsid for AD integrates seamlessly with orchestrators, so users can remediate to breaches at machine speed.



AD-NATIVE INVESTIGATION CAPABILITIES

Conclusion

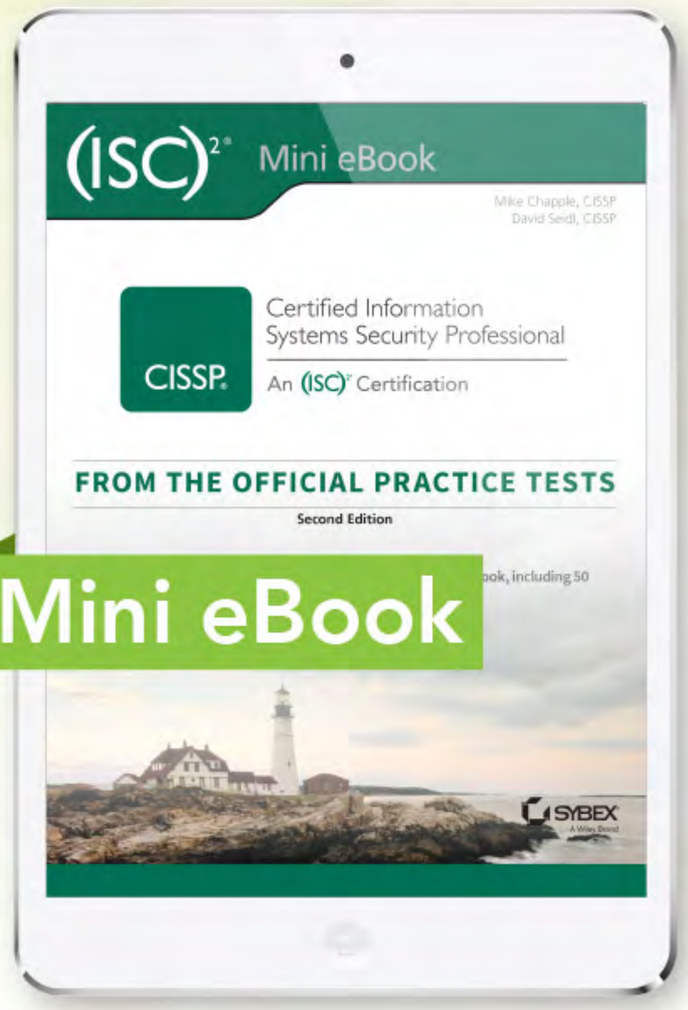
AD-related attacks are now common-place. Reports show repeatedly that AD admin and security folks struggle to deal with AD-related threat.

This is our battlefield. Don’t take our word for it: give Alsid a test-run and start improving your infrastructure’s resilience: https://alsid.com/alsid-solution

ELEVATE
YOUR **CAREER** WITH
(ISC)² CERTIFICATIONS

Organizations around the globe rely on CISSP- and CCSP-certified pros to ensure evolving cybersecurity and cloud security needs are met. Find out if you're ready to tackle growing security challenges – and raise your game with these in-demand credentials.

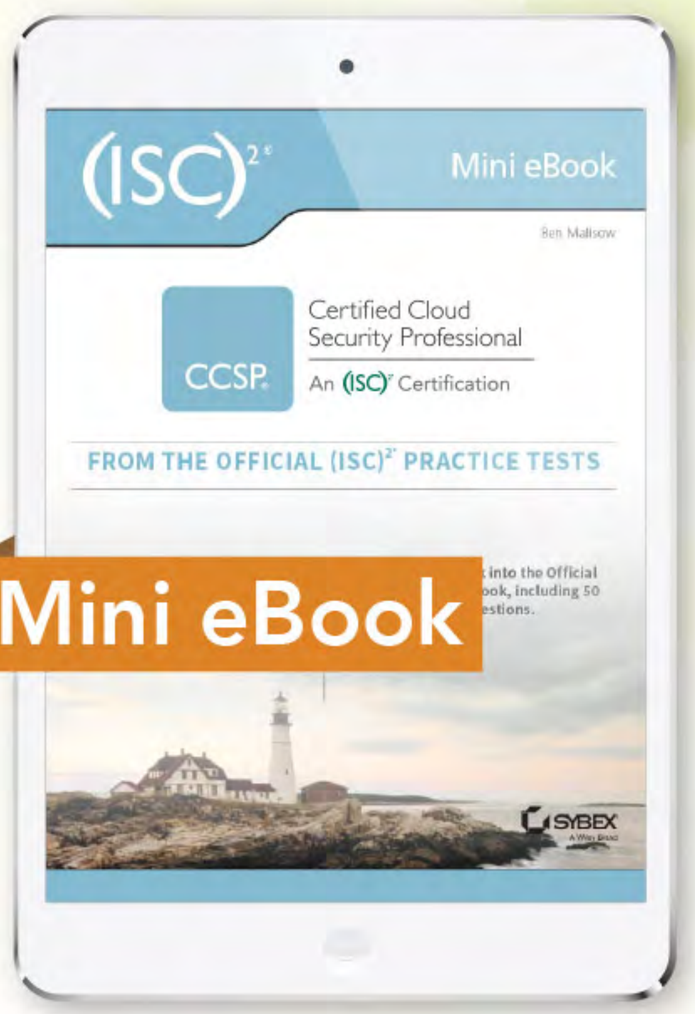
Use these complimentary resources to test knowledge now:



Mini eBook

50 FREE
CISSP practice items

Download CISSP eBook



Mini eBook

50 FREE
CCSP practice items

Download CCSP eBook

(ISC)² | www.isc2.org

Events

RSA Conference 2020

February 24-28, 2020
Moscone Center, San Francisco, CA, USA
http://helpnet.pro/rsaconf2020

Expert-led track sessions. Thought-provoking keynotes. Cutting-edge innovation. Valuable networking opportunities. RSA Conference is where the world talks security, and you can be a part of this important conversation.

Join industry leaders and peers at RSAC 2020 in San Francisco, February 24 – 28. Learn about the latest trends that are most relevant to your needs while helping to shape the future of the industry.

Cybertech Tel Aviv 2020

January 28-30, 2020
Tel Aviv Expo, Tel Aviv, Israel
https://www.cybertechisrael.com

Cybertech is the cyber industry's foremost B2B networking platform conducting industry-related events all around the globe.

Its conferences and exhibitions serve as the go-to place to make business happen and learn all about the latest technological innovations, challenges, and solutions to combating threats within the global cyber arena.

Cybertech events feature top executives, government officials, leading decision-makers from a wide range of sectors including critical infrastructure, insurance, retail, health and government, defense, R&D, manufacturing, automotive, and more!

Multinational corporations, startups, private and corporate investors, venture capital firms, experts, and clients—come and meet all the key players from the cyber industry and be immersed in everything there is to offer.

When is the right time to red team?

AUTHOR_ Ed Williams, EMEA Director of SpiderLabs, Trustwave

“It takes a thief to catch a thief”. Despite being hundreds of years old, this idiom holds true for that most modern of thieves, the cyber criminal. With adversaries consistently evolving their tools and techniques to overcome defensive solutions, foiling their attacks requires ethical hackers who are able to think in the same way and spot the same potential attack pathways.

Red teaming is the epitome of this approach to security, involving a team of highly experienced security professionals taking on the mantle of the cyber attacker and doing everything in their power to breach the organization’s systems.

A successful red teaming exercise can be incredibly effective in exposing potential weaknesses that normal penetration and vulnerability testing activity will miss.

Thinking like a cyber criminal

While it is often conflated with penetration testing and does involve similar processes, red teaming is actually a very different activity. Whereas a standard pen test will focus on a tightly defined scope and focus on the technical aspects of the business and aim to find as many potential vulnerabilities as possible, red teaming will see the team take advantage of people and processes as well as technology. It's a no-holds-barred engagement, with the team stopping at nothing to execute a successful attack, just like an actual threat actor.

Only once a business has completed several cycles of vulnerability and penetration testing should it start to elevate its activity with red teaming.

As well as testing the technical side of security, red teaming will test a firm's personnel as well. The internal "blue team" will be tasked with trying to spot the red team intruders and doing their best to stop and remove them from their networks.

Red teaming has become increasingly popular in recent years as firms become more aware of the threats they are facing. However, because it is often thought of as an extension of pen testing, we often find that businesses are keen to jump straight into red teaming before they are ready for it.

Realizing the value of red teaming

A successful red teaming exercise can be incredibly effective in exposing potential weaknesses that normal penetration and vulnerability testing activity will miss. However, these results can only be realized if the organization has a mature security program.

Before letting a team of ethical hackers loose on its system, a firm must already be carrying out automated activity such as asset investigation and vulnerability analysis. The organization should also be combining automated technology with human intelligence by implementing robust, regular penetration testing.

Only once a business has completed several cycles of vulnerability and penetration testing should it start to elevate its activity with red teaming. This will help it to establish a stronger security strategy that looks at the big picture of people, processes and technology. This is absolutely essential for any firm hoping to hold off advanced threat actors, who will target multiple areas of the business in order to compromise the network.

However, attempting to bring in red teaming before getting a good handle on the basics will produce very little value. The ethical hacking team will likely be able to compromise the environment so swiftly and easily that there will be little to learn. To be truly effective, the insights produced by the red team need to be given context by previous penetration testing and vulnerability assessment activity.

The true value of red teaming is what the company does with the insights that are uncovered.

Improving security maturity

Every red teaming exercise I have been involved with has delivered actionable insights, and there is always an element of the blue team reading the report and going "ah, we should have stopped that!".

Carrying out a red teaming exercise is only half the battle. As with more traditional pen testing and vulnerability assessments, the true value of

red teaming is what the company does with the insights that are uncovered.

Organizations need to ensure that any red teaming exercises are properly married into existing risk assessment processes so that potential threats can be closed or mitigated in line with the company's risk appetite.

As with most other aspects of security, red teaming is never a matter of "one and done" - it needs to be a regular, continual process in order to be effective. How regularly this happens is again down to the company's particular risk appetite, but introducing annual red teaming is a good place to start. It can also be useful to carry out ad hoc testing when there are significant changes to the environment, such as M&A activity, the introduction of new software, or the discovery of a new malware or attack technique that may threaten the business.

A red team needs to be equipped with a depth and breadth of experience and skills that will enable them to match what genuine black hats can muster.

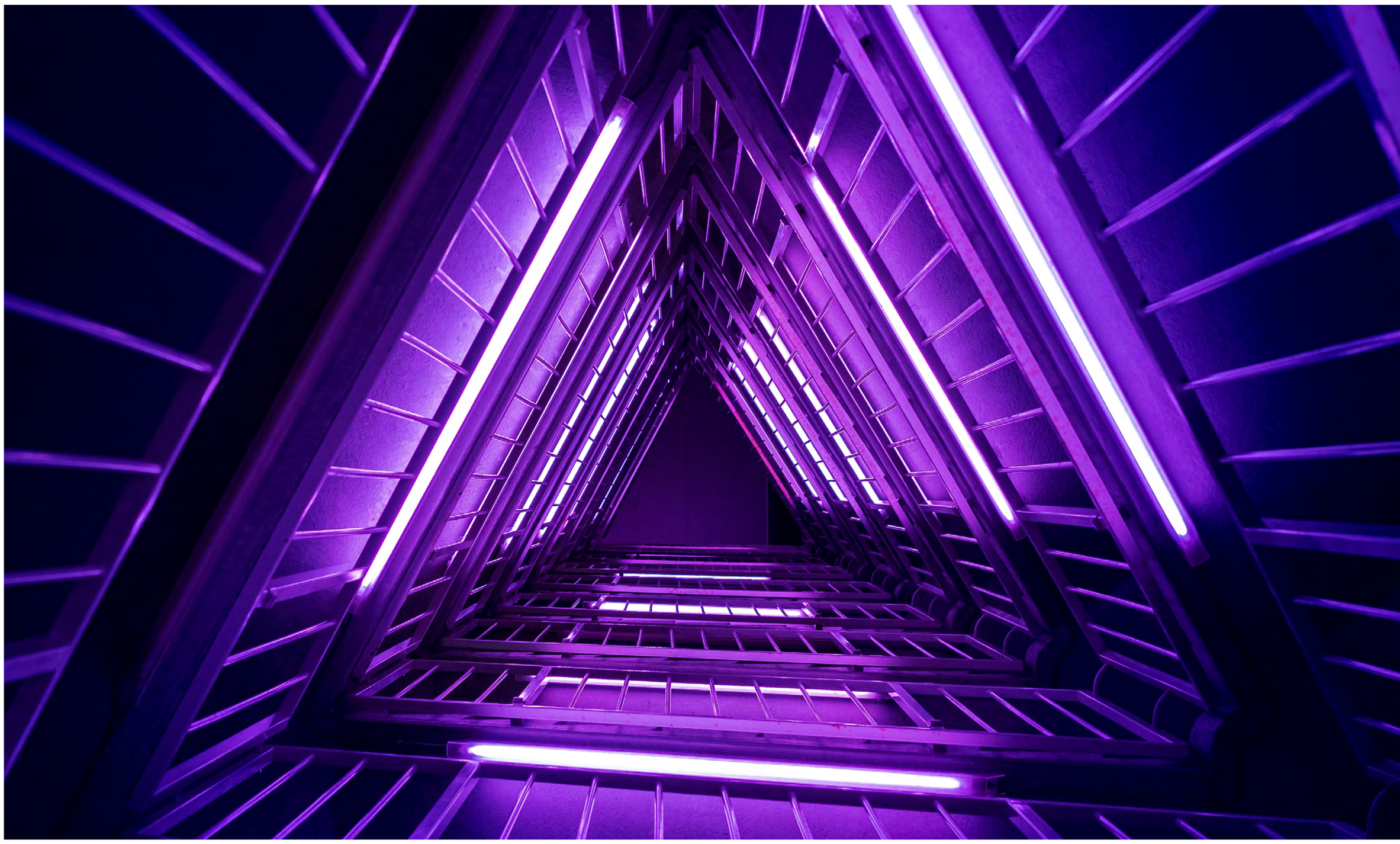
Once the organization settles into a routine, red teaming can help it make serious progress in improving its security maturity. One of the most important steps is understanding that security vulnerabilities are universal across the business. It's common to find that one department will discover and mitigate an issue, but it will be left open in other areas of the organization. Just like a genuine attacker, ethical hackers will quickly identify these gaps and exploit them for maximum impact, which can be a very effective way of forcing the business to start breaking down silos.

Managing red teaming

To accurately emulate a real threat actor, a red team needs to be equipped with a depth and breadth of experience and skills that will enable them to match what genuine black hats can muster. More importantly, an ethnical hacker needs to be able to step into an adversary's head and be as creative and persistent as a real criminal hunting for a huge payday.

Accessing this kind of capability is a challenge at the best of times, and doubly so thanks to the on-going skills gap. With this in mind, all but the largest organizations will need to engage external third parties to carry out red teaming. Because it should be a regular and on-going process, it can also be beneficial to form a long-term partnership with a managed security service provider (MSSP). Using the same partner for red teaming, penetration testing, and other essential activity can also make it easier to assemble various jigsaw pieces of intelligence into a single coherent picture.

However, firms that try and jump straight into red teaming without doing the groundwork first will find themselves with a handful of pieces and no puzzle to put them into.



Remember when, three years ago, several Mirai botnets hit DNS provider Dyn and caused part of the Internet to be unreachable for most users in North America and Europe? For a moment there it really seemed that IoT security would become an indisputable necessity.

Unfortunately, that did not happen, and security professionals and consumers are left trying to minimize the dangers of insecure IoT and industrial IoT devices as best they can.

> IoT is an ecosystem, as secure as its weakest link

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

The problem with IoT devices

IoT devices are often connected directly to the Internet and they are rarely hardened against unwanted access and compromise. They often use obsolete protocols like Telnet. Many legacy IoT devices that are still being utilized either cannot be updated or the vendor no longer supports the device, while new vulnerabilities are discovered

every day. Finally, detecting that their IoT device has been compromised is difficult for most consumers and, occasionally, enterprises.

Pentesters who specialize in IoT have told me that they've, so far, never tested a device that they were unable to penetrate and take over.

It's no wonder, then, that botnet masters now prefer to target IoT platforms instead of Windows machines.

"Pentesters who specialize in IoT have told me that they've, so far, never tested a device that they were unable to penetrate and take over," noted Bob Carver, Principal Cybersecurity Threat Intelligence and Analytics, Verizon.

However, some are harder to hack than others. For consumers, the general advice is to stick to known brands that have a reputation of supplying their products with operational and security updates, and to implement these updates as soon as they are provided.

Enterprises, though, should do much more than that: test before deployment, continuously pentest and remediate discovered vulnerabilities, verify patches, configure and harden devices against attacks, and more.

With the massive proliferation of IoT devices, we'll have to start treating all IoT as part of an ecosystem, with security and reliability issues to be addressed for it all and not just for each individual device.

"If involved with industrial IoT, organizations should consider joining a consortium of vendors where credentialing of systems is required to take place. Or they might consider partnering with a vendor that has been developing a secure IoT ecosystem, credentialing all parts of the IoT ecosystem for reliability and security," Carver added.

The enterprise and IoT security

Privacy and how to protect that privacy will be an issue that affects both individuals and organizations/businesses. The former will want their personal and other data safe when traversing networks, the latter will want to keep their proprietary corporate data secure every step of the way.

"With the massive proliferation of IoT devices, we'll have to start treating all IoT as part of an ecosystem, with security and reliability issues to be addressed for it all and not just for each individual device," Carver opined.

"IoT devices are not only connected together, but may be connected to the cloud, databases, edge networks and other devices. Not only do they need to be secured individually, but every network connection, cloud, data and edge network must be secure and reliable."

Security updates must be provided over the air or the network – there should be no shipping of devices to manufacturers for updates. Verifying the authenticity and security of these updates is also a must. "Systems should be designed securely preventing cybercriminals from breaching and updating systems with malicious code," he noted. The data that travels through the IoT ecosystem must also be secured. No clear text – it should be encrypted or sent via virtual tunnels so that MitM attackers can't view it and get their hands on it.

Organizations must also start thinking about security, privacy and reliability in real-time and find ways to implement and perform real-time protections/corrections.

> *Another thing that we'll need in the long term is IoT cyber security legislation and regulation.*

All this and more is especially important for organizations providing and securing critical infrastructure.

"Those involved in protecting critical infrastructure who had the foresight to start cyber resiliency program years ago may do well fending off future attacks. Those that only recently started such a program may not fare so well," he added.

Legislation and regulation

Another thing that we'll need in the long term is IoT cyber security legislation and regulation.

"There needs to be a law to determine who is going to be responsible for the security of IoT and who will be required to take appropriate action when things go wrong. At present no one is taking responsibility. There needs to be a delineation of responsibility between the owner of the IoT device, its manufacturer, the ISP and the government," Carver opined.

In October 2018, California Governor Jerry Brown signed into law a bill that requires manufacturers of internet-connected devices sold in the state to "equip the device with a reasonable security feature or features." The UK and Japan have also made commitments to address IoT cybersecurity and develop guidelines and regulations for manufacturers and industry stakeholders.
It is encouraging, he says, that the U.S. Congress has been making attempts to place IoT cybersecurity bills into law.

"Some security professionals have attempted to put in place a cybersecurity 'Underwriters Laboratory' seal of approval for devices, but there hasn't been any political will to implement this. It's also difficult to put it into a written policy of what is considered 'good enough' for that seal of approval," he noted.

"One good suggestion regarding commercial IoT devices would be for buyers to require, in their purchase contract, security updates from the manufacturer for a specified length of time (e.g., 5 years). If vulnerabilities are discovered after that time period has passed, the device should either put out of service (end-of-life) or the vendor can be paid for providing additional vulnerability patches."

> *Some security professionals have attempted to put in place a cybersecurity 'Underwriters Laboratory' seal of approval for devices, but there hasn't been any political will to implement this. It's also difficult to put it into a written policy of what is considered 'good enough' for that seal of approval.*

WATERFALL®
Stronger Than Firewalls

The OT Security Company

Is your OT network 100% protected?
OT attacks result in production losses

Physical losses demand physical protection -
Waterfall provides safe OT visibility with disciplined control:

- Vendor Support
- Remote Access
- Scheduled Updates
- Continuous Control

SCAN ME

Explore these topics and more in the latest Waterfall download - Safe OT Visibility With Disciplined Control