[+] (IN)SECUREMagazine

03 | 2021
ISSUE 68

Cybersecurity adaptability

Physical cyber threats: What do criminals leave when they break in?

Tips for boosting the Sec part of DevSecOps

Homomorphic encryption: Myths and misconceptions

COMMAND *LEADERSHIP* IN THE CLOUD

Get to Know the (ISC)² CCSP Credential

How is your organization responding to evolving security threats in the cloud? Are your people, processes and technologies aligned for success? (ISC)² can help you stay ahead of emerging trends and gain a clear competitive edge.

Our globally recognized Certified Cloud Security Professional (CCSP) arms IT & security pros at the forefront of cloud security. But why does the CCSP stand out so convincingly?

For Starters:

- Instant differentiation as an authority figure on cloud security, proving proficiency to keep up with new technologies, developments and threats.
- Unique recognition for achieving the highest standard of cloud security expertise.
- Enhanced acumen to stay ahead of cloud security best practices, evolving technologies and mitigation strategies.
- Versatility to apply knowledge and skills across a variety of cloud platforms.

Organizations today need expert security to command the cloud. Find out how CCSP certification delivers the security to protect – and the power to transform.

CCSP®
Certified Cloud Security Professional
An (ISC)² Certification

Lead the Way

Table of contents

Featured experts

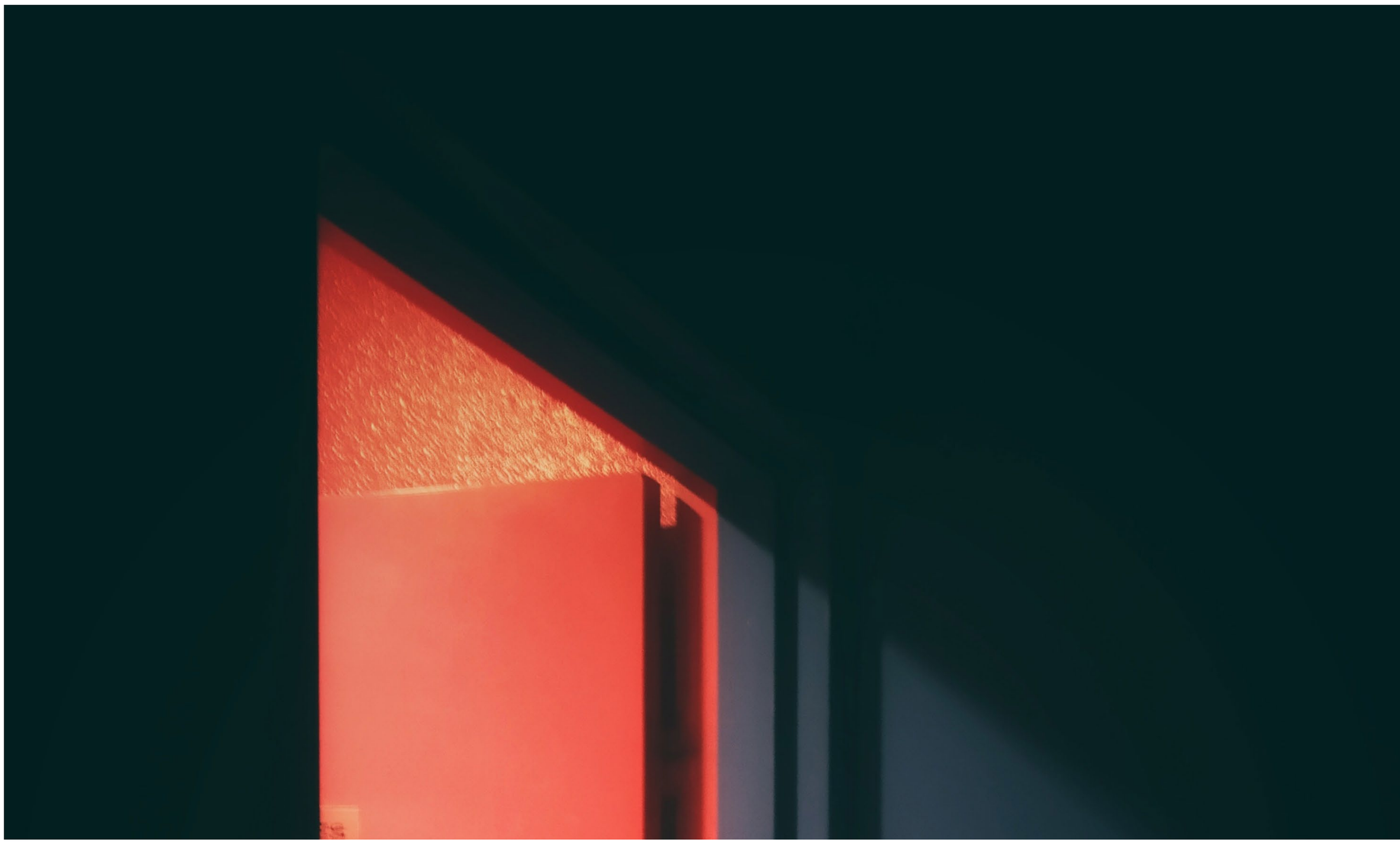
MARC GAFFAN, CEO, Hysolate
BALAJI GANESAN, CEO, Privacera
TONI GRZINIC, Security Researcher
BRIAN HAJOST, President & CEO, SteelCloud
RICHARD HUGHES, Head of Technical Cybersecurity Division, A&O IT Group
ALEX LIVSHIZ, Research Team Lead, SCA, Checkmarx
GREG MARTIN, VP & GM of Security, Sumo Logic
NATHANIEL MERON, CPO & CMO, C2A Security
GANESH PAI, CEO, Uptycs
NIGEL SEDDON, VP of EMEA West, Ivanti
NIGEL THORPE, Technical Director, SecureAge Technology
ELLISON ANNE WILLIAMS, CEO, Enveil

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 Marketing
bkucan@helpnetsecurity.com



Physical cyber threats: What do criminals leave when they break in?

AUTHOR_Richard Hughes, Head of Technical Cybersecurity Division, A&O IT Group

Many organizations have maintained heavy investment in cyber security over the last year, even in an unpredictable time when other spending has faltered. Gartner estimates that IT security and risk management spending still grew 2.6 percent even as IT spending as a whole fell by 8 percent.

However, while businesses have continued to fortify their networks against remote invaders, most have overlooked the potential for cyber threats from physical intruders. With very few exceptions such as government facilities, organizations tend to be extremely vulnerable to cyber attacks that involve a threat actor gaining direct access to the infrastructure.

While such attacks are extremely rare in comparison to the endless virtual attacks launched every day, physical security gaps can allow threat actors to circumvent otherwise strong defenses to inflict serious damage. Unlike an ordinary burglary, the threat is not what is stolen by the intruder, but

what they leave behind – anything from keyloggers to backdoor malware. It's especially important that organizations that are in high-risk sectors such as finance be prepared for such attacks.

> *We have often found that even in industries that have good cause to take their physical security seriously, the focus tends to be on specific valuable assets rather than the building as a whole.*

Fortunately, however, with the right precautions it is possible to minimize the risk of a physical intruder, and spot incursions based on digital and physical evidence left behind.

How do intruders breach the building?

The first part of any physical cyber attack is gaining access to the building, and our red teaming exercises have found this is often shockingly easy to do. While you might forgive a business for being caught out by an elaborate Ocean's Eleven style heist, all too often it is easy enough to simply walk in.

> *One of the most effective techniques is to leave a small drop box device attached to the network. These are inconspicuous and can be easily hidden under desks or on other devices such (e.g., the office printer).*

We have often found that even in industries that have good cause to take their physical security seriously, the focus tends to be on specific valuable assets rather than the building as a whole. Banks, for example, will obviously have their defenses focused on secure vaults and strongrooms to protect cash and other valuable items, but the office portion of the building will be lightly secured.

One of the most straightforward tactics is to simply tailgate an employee through the doors. People tend to instinctively hold doors open for others coming in behind them and are unlikely to question it. Or perhaps, if the building has a back entrance where smokers congregate, the imposter can simply join them for a quick smoke and then drift inside with the crowd.

Invaders rely on the fact that most people want to avoid directly challenging others, even if they don't recognize them. This is particularly true in a shared office environment or at a location that receives a lot of visits from guests and contractors. With many buildings standing largely empty due to social distancing, it can be even easier to go about unnoticed at larger locations.

Even if there are dedicated security checks, these can be quite easily bypassed in most cases. In one red teaming exercise we conducted at a bank, for example, our operative wore a mock-up of the firm's door passes. The pass contained an RFID chip so it triggered a reaction from the scanner, and the guard was happy enough to wave them through with the excuse that the card must be faulty.

What damage can a physical attacker do?

As mentioned, the risk here is less about what attackers steal, and more about what they leave behind. One of the most effective techniques is to leave a small drop box device attached to the network. These are inconspicuous and can be easily hidden under desks or on other devices such (e.g., the office printer). Such devices can be used for a number of purposes, such as monitoring and exfiltrating data or serving to facilitate command and control (C2). Drop box devices can be set up relatively quickly, making them ideal for covert intruders on a time limit.

Given enough time, attackers can pull off any number of malicious activities. Installing C2 or key logging malware via a USB are obvious choices, but they could even go so far as to take out hard drives and image them. Furthermore, if the server room is accessible, they can wreak havoc even more directly. In some of our red teaming exercises, operatives have been able to remain in the office alone for hours after close of business, which would give an attacker ample time to execute more complex activity.

> *Devices that have been left behind can also potentially be located through virtual means, although this is not certain.*

Because security defenses tend to be geared around detecting external threats targeting the network from afar, they are often easily circumvented by direct access. Further, tracing such an attack back to a physical incursion is no easy task, reducing the chances that investigators will find and close the source of the breach.

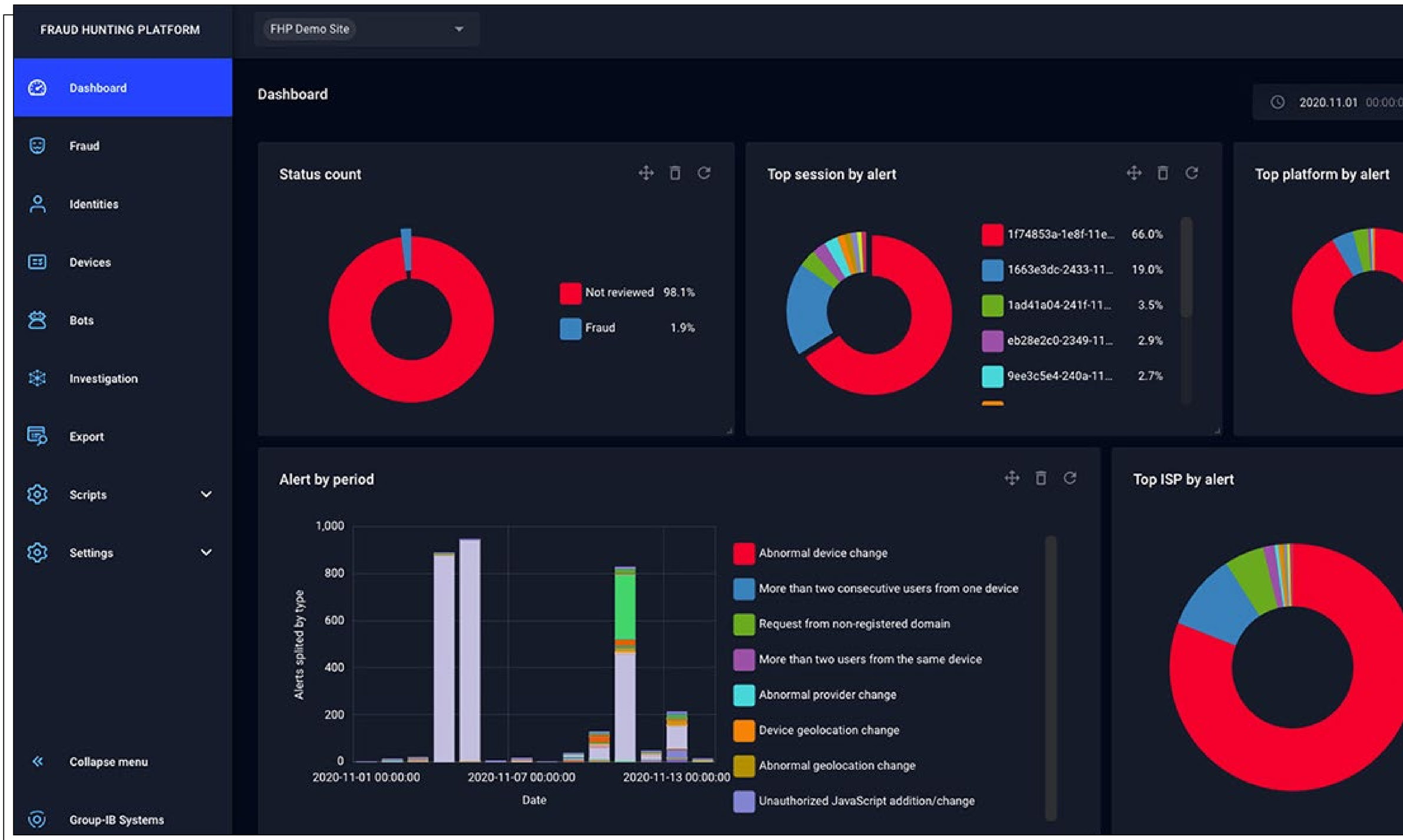
Preventing a physical cyber attack

As with any cyber threat, prevention is better than cure. Just like with phishing and other social engineering attacks, employee awareness is particularly important. Organizations should consider holding training sessions to highlight the risks and the importance of following building security procedures – including overcoming a natural aversion to confrontation and questioning unknown visitors. If the building has security or other front desk staff, they must always ensure people are met by a representative of the company rather than being left to move freely. This is particularly important in a post-COVID world where an office might be sparsely populated and running an irregular staff rota. Similarly, the mask mandate means that it is now perfectly expected for people to move about with their faces obscured.

In addition, the building needs to be equipped with security measures, including alarms and CCTV. Alarms will assist when an intruder stays behind afterhours, and CCTV can be used to trace an attacker's movements to find out where they went and what they did. Any hardware they were near to should then be checked for signs of tampering or unknown devices. Without CCTV to fall back on, finding drop boxes and other devices can be like looking for a needle in a haystack – particularly in large offices with hundreds of workstations. Server rooms should be secured in the same fashion as any other asset.

Devices that have been left behind can also potentially be located through virtual means, although this is not certain. It may be possible to find their MAC address, but these can be easily spoofed to match a genuine and expected device. Scanning and pen testing likewise may succeed but will not be able to find a device if all its ports are closed off. One of the more reliable options is to use MDR and real-time traffic monitoring as the device will typically be connecting back to another location and this will allow it to be located in the same way as a normal remotely executed breach.

While physical cyber attacks are rare, they can be devastating for those organizations that criminals view as worth the additional effort. A lack of consideration for physical cyber security means that any attacker who dares such a move will likely have a straight path to the company's most valuable assets. By treating cyber and physical security as two sides of the same coin, would-be intruders will find their plans foiled just as a virtual attacker will be detected and blocked by the best security solutions.



Today's Internet is a hectic place. A lot of different web technologies and services are "glued together" and help users shop online, watch the newest movies, or stream the newest hits while jogging.

But these (paid) services are also constantly threatened by attackers – and no company, no matter how big, is completely immune. Take the recent Twitter compromise as an example: the attackers hijacked a number of influential Twitter accounts, including those belonging to Joe Biden, Jeff Bezos, Apple and others, and used them to try to pull off a Bitcoin scam. The attackers took advantage of the whole remote working situation, targeted the Twitter support team through a phone spear phishing attack, and successfully phished VPN credentials that enabled them to access the company's internal tools.

How can companies protect their services from similar attacks, as well as identity takeovers due to

Review: Group-IB Fraud Hunting Platform

AUTHOR_Toni Grzinic, Security Researcher

successful exploitation of stolen information such as credit card numbers, user account credentials and authentication tokens?

In this review, we will take a close look at the Fraud Hunting Platform (FHP) developed by Group-IB, which helps web and mobile service owners monitor users' usage and investigate potential misuses. Aside from detecting anomalous use of a service, Group-IB's FHP allows service owners to detect when users are infected by malware that can perform Man-in-the-Browser attacks or alter pages, facts of remote access to a user device, and automated bots looking to access the service and siphon data (e.g., product prices in e-commerce applications).

Test methodology

We used a pre-configured test instance of the Fraud Hunting Platform that monitored two demo sites that require users to create an account and log in to browse products, order them and send the payment.

We tried standard and non-standard attack tactics and techniques that anti-fraud tools should be able to detect. Those include:

- The use of proxies to change the IP/location. VPN hopping.
- The use of remote access tools (Teamviewer, RDP, VPN) by some trojans
- Access through TOR exit nodes
- The use of emulator and virtual machines
- The spoofing of User Agents
- The use of Selenium and scripted bots that try to brute-force the login form
- The manipulation of web pages (JavaScript injections)
- Mobile access tests

After going through each of these test cases or a series of them, we assessed the effectiveness of the Fraud Hunting Platform based on the following criteria:

- Did it detect the relevant event?
- What threat level has it assigned to the event? Are threat levels related to the potential risk represented by the test case?
- Are FHP detections helpful to threat/fraud analysts? Can the FHP improve the process of detecting fraud and potential misuses?
- Usability and ease of use of the FHP web interface

The Group-IB Fraud Hunting Platform

The Group-IB Fraud Hunting Platform is a digital identity protection and fraud prevention system designed to protect end users from various types of online fraud.

Fraudulent or bot activity detection is based on fingerprinting user sessions and identities (by using device and network-related information) and user behavior patterns (mouse movements and clicks, keystroke dynamics), which means that there is no need to write specific rules that detect abnormal/fraudulent behavior.

The FHP enables service owners to perform a global profiling of fraudulent activities across their resources or cross channel analytics (if the needed permissions are provided). That means that they can follow attackers as they are exploiting various services, which can be useful for investigating bigger incidents.

The FHP can detect bots and other attack patterns: malicious injections, attempts to leverage remote access tools, compromised devices, SIM card changes, and so on. It can detect threats to financial and e-commerce sites, cryptocurrency exchanges, social networks and other online services.

The FHP can deliver value to customers by blocking malicious users that request authentication tokens while trying to brute-force accounts with the targeted service. If the services owner delivers authentication tokens via SMS, such attacks can result in increased costs.

Other use cases include detection of users that exploit stolen payment card data or perform fraudulent activities related to user reputation (e.g., boosting reputation as a fake seller on e-commerce sites).

The platform also enables service owners to manage their users better, prevent the locking of wrong accounts, and manage transactional limits better.

According to Group-IB statistics, up to 85 percent of sessions that are subject to extra analysis, can be automatically accepted thanks to additional data and FHP verdicts. The FHP is also useful for detecting compromised systems that are accessing the service's resources - a capability requested by the EU Payment Services Directive 2 (PSD2).

How does the Group-IB Fraud Hunting Platform work?

The main components of the FHP are the client module, the Processing Hub, the Preventive Proxy and the analytical web interface.

The service owner first needs to embed a lightweight data collection script on the client side:

- A simple JavaScript code snippet is embedded into websites to collect data related to user's device and browser settings and user's behavior within the application
- In cases where the service is a standalone mobile application, the FHP provides a mobile SDK that performs the collection of user action and context data

Both the mobile SDK and the code snippet have a minimal effect on the mobile phone or computer resources usage (network traffic, CPU/RAM usage) and application functionality.

The collected data is sent and analyzed by the FHP Processing Hub, which extracts relevant information (session and identities, user actions) and detects abnormal behavior that enables the fingerprinting of bots. Bots are blocked by the Preventive Proxy.

The processed data can be viewed via a handy web interface that provides a clear overview of the monitored sites. The interface allows the service owner to:

- View fraud alerts categorized by risk
- Pivot through all events by identities, devices and sessions
- See detected and blocked bots
- Investigate incidents from a higher level with a graph analysis
- Search events by various fields, and more

The FHP's modular design enables various configurations related to blocking bots, but it also enables integration with other transactional fraud detection systems that companies use for monitoring financial transactions. At the moment, integration with systems by SAS, Bottomline (Intellinx), RSA Transaction Monitoring, and GBG are available.

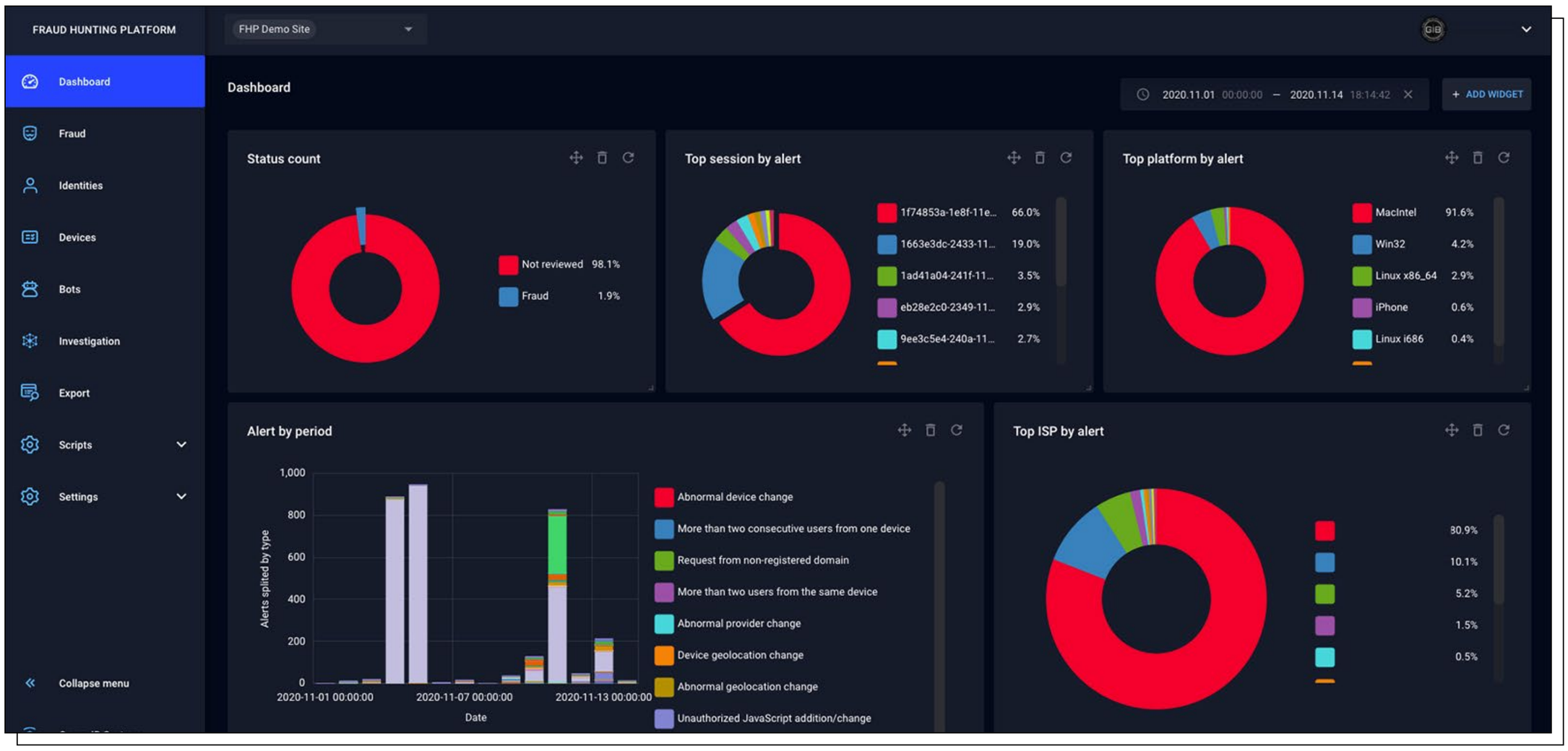


FIGURE 1. FRAUD HUNTING PLATFORM – DASHBOARD SHOWING RECORDED EVENTS

The FHP tracks visitors of the monitored sites by their device and session. Based on that information, it creates the user's "identity". It captures data available to the web browser context (platform specification, browser plugins, mouse and keyboard movements, tab active/inactive), but also network-related data (User-Agents, IPs, etc.). This data is analyzed and used to generate alerts that identify bots and malicious events. Every alert is marked with a score from 0 to 100 (the higher score represents a higher risk). Event detection is not based on signatures – it's achieved through machine learning algorithms that are trained on previously collected data and appropriate intelligence feeds.

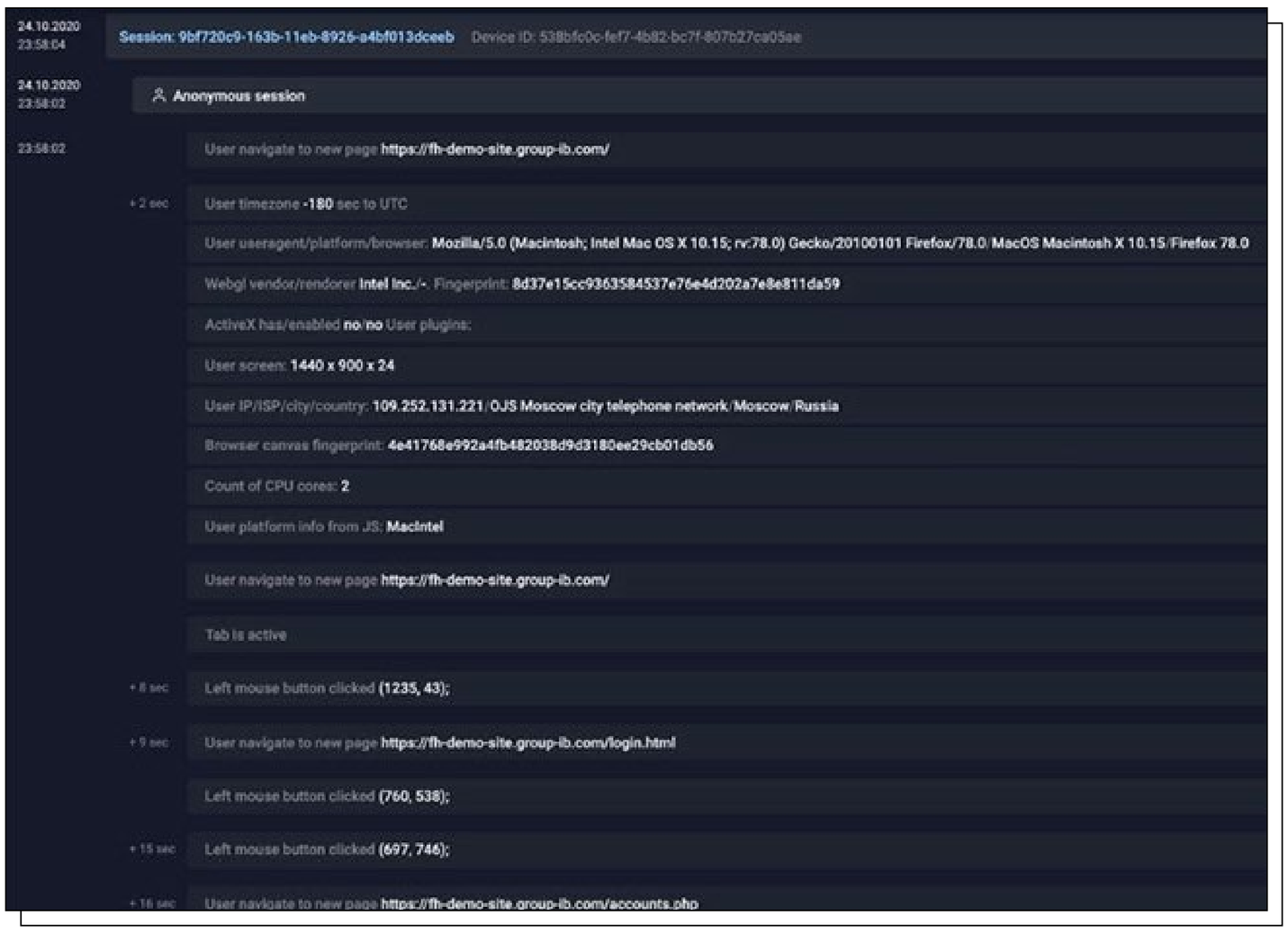


FIGURE 2. FRAUD HUNTING PLATFORM – MOUSE PATTERN

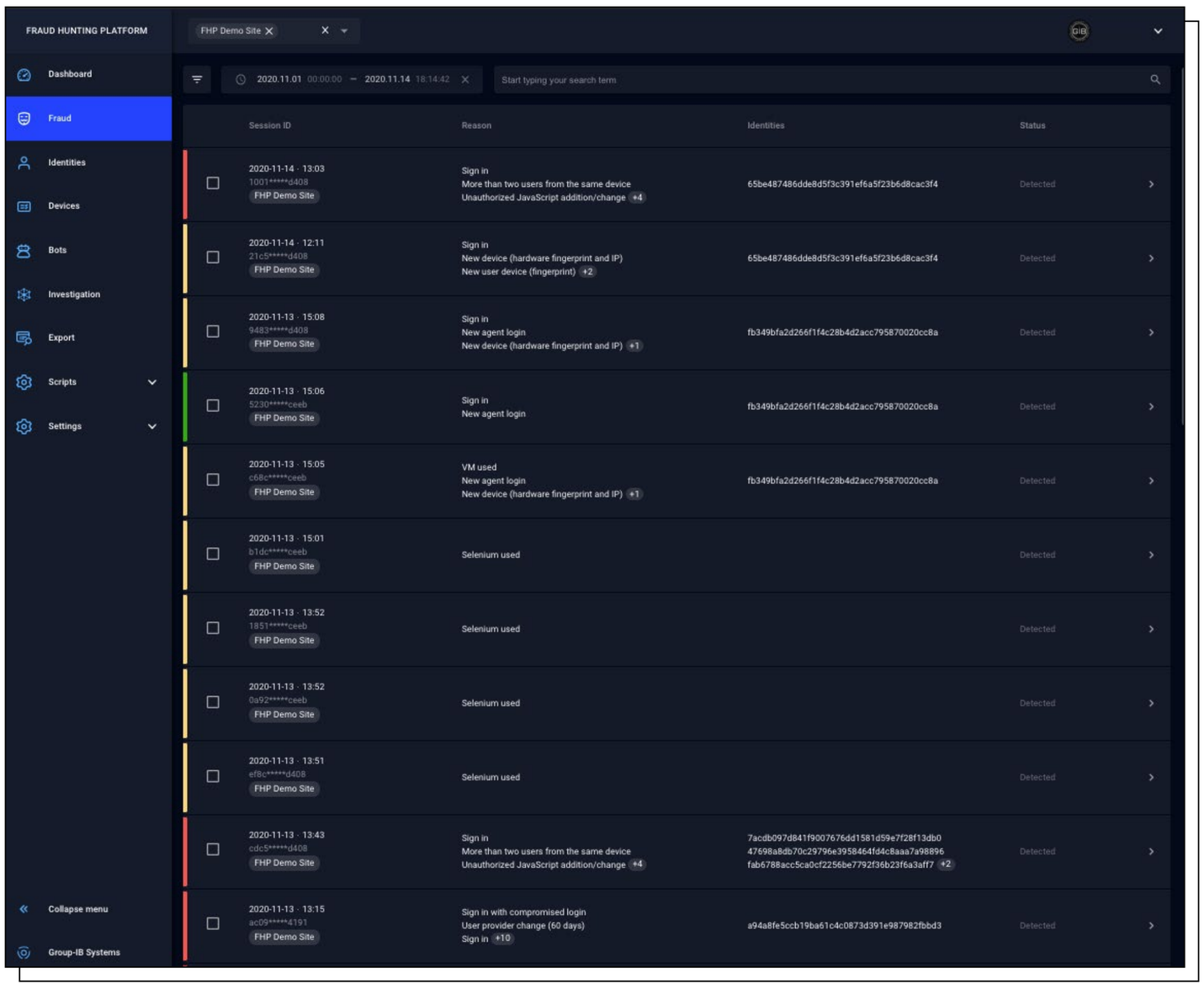


FIGURE 3. DETECTED SESSIONS AND EVENT SUMMARY IN THE FRAUD HUNTING PLATFORM

The FHP does not need users to be logged in the monitored site to "identify" them. Users' identity is based on the user's device fingerprint, i.e., the context within which they are accessing the site. The device fingerprint is derived from various data points: User Agent, operating system, time zone, fonts in use, browser plugins, language, MIME types supported, Canvas fingerprint, emulator usage, cookie parameters, media devices, DirectX and WebGL parameters.

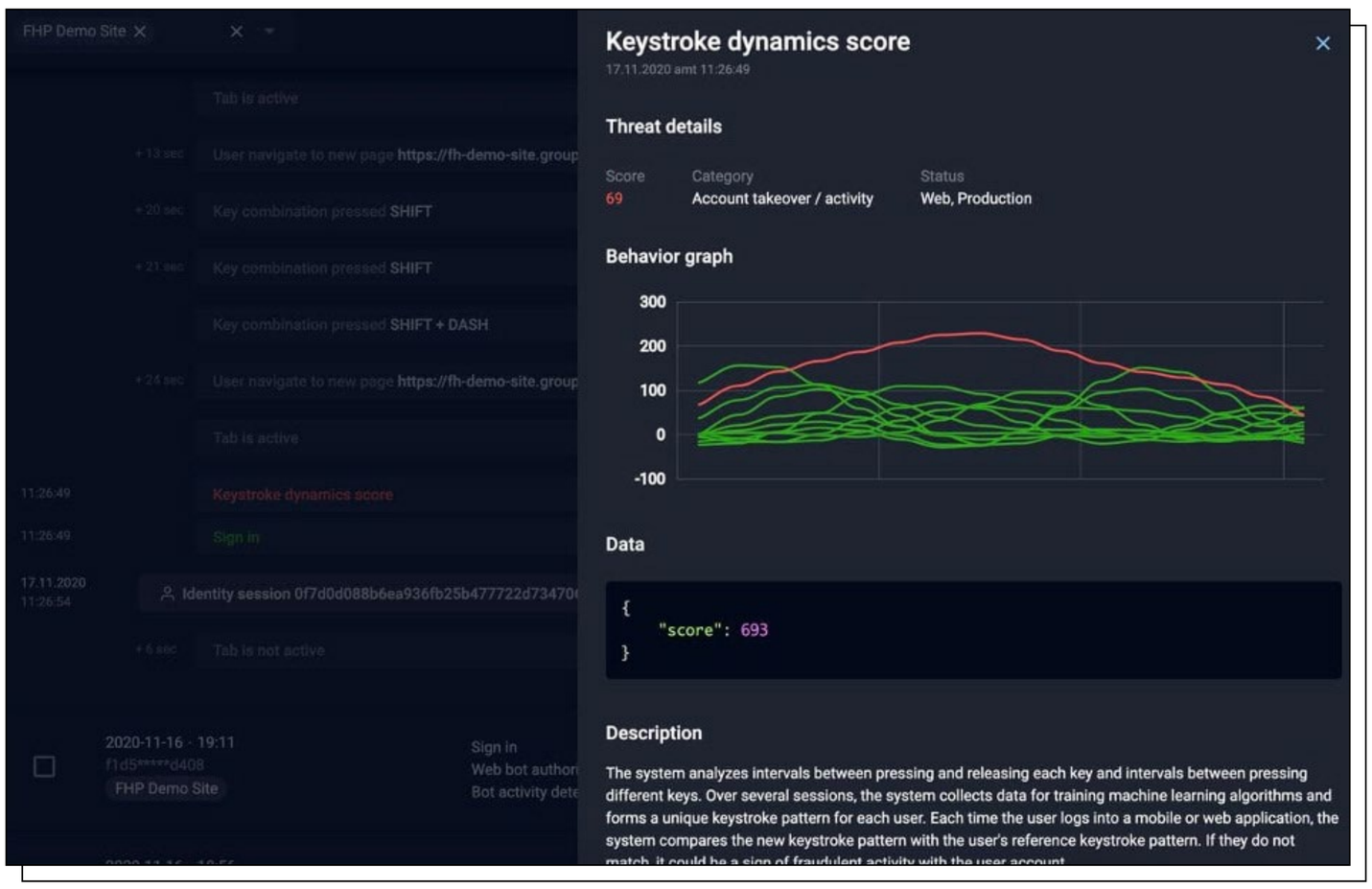
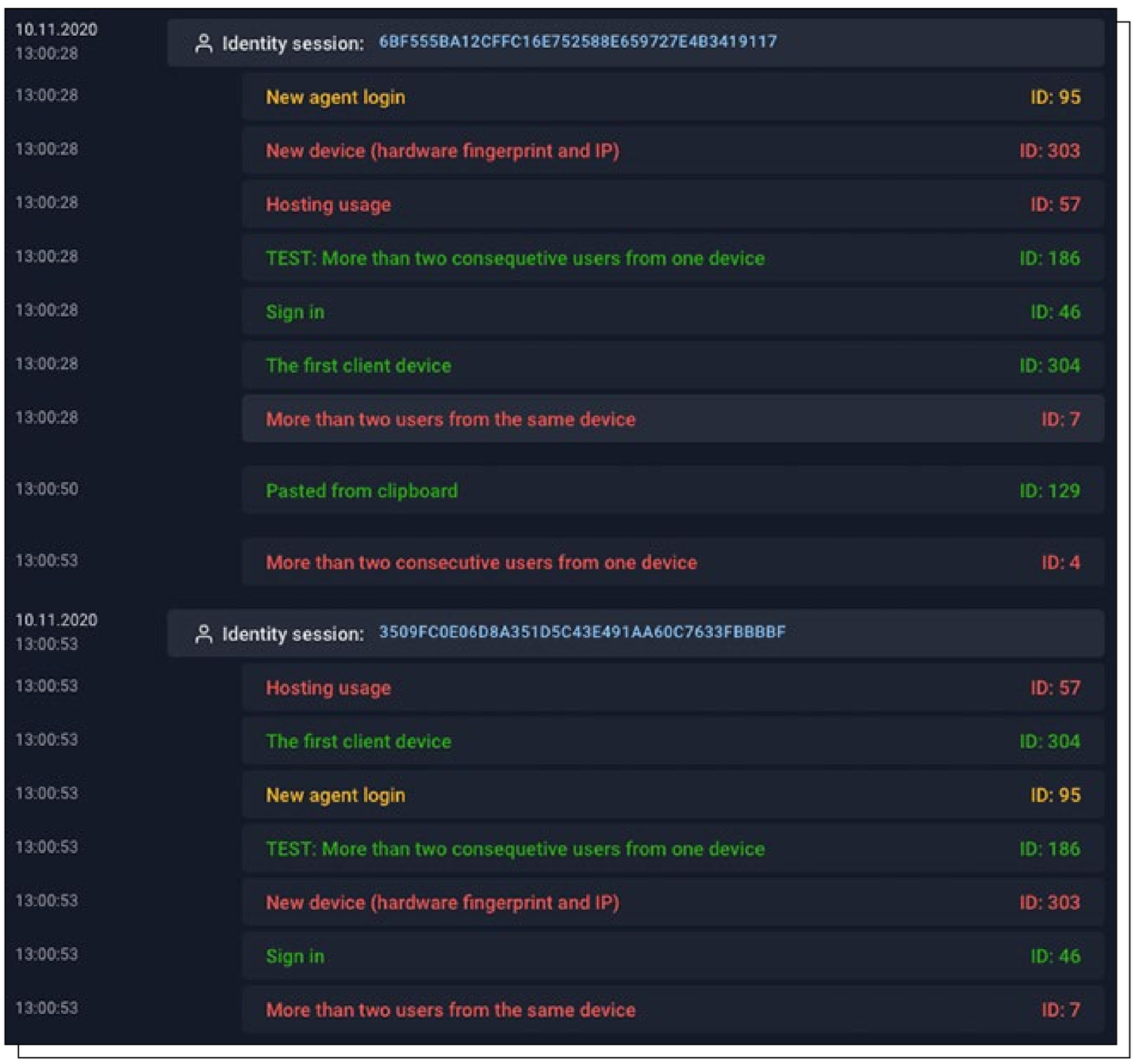


FIGURE 4. GRAPH SHOWING KEYSTROKE DYNAMICS

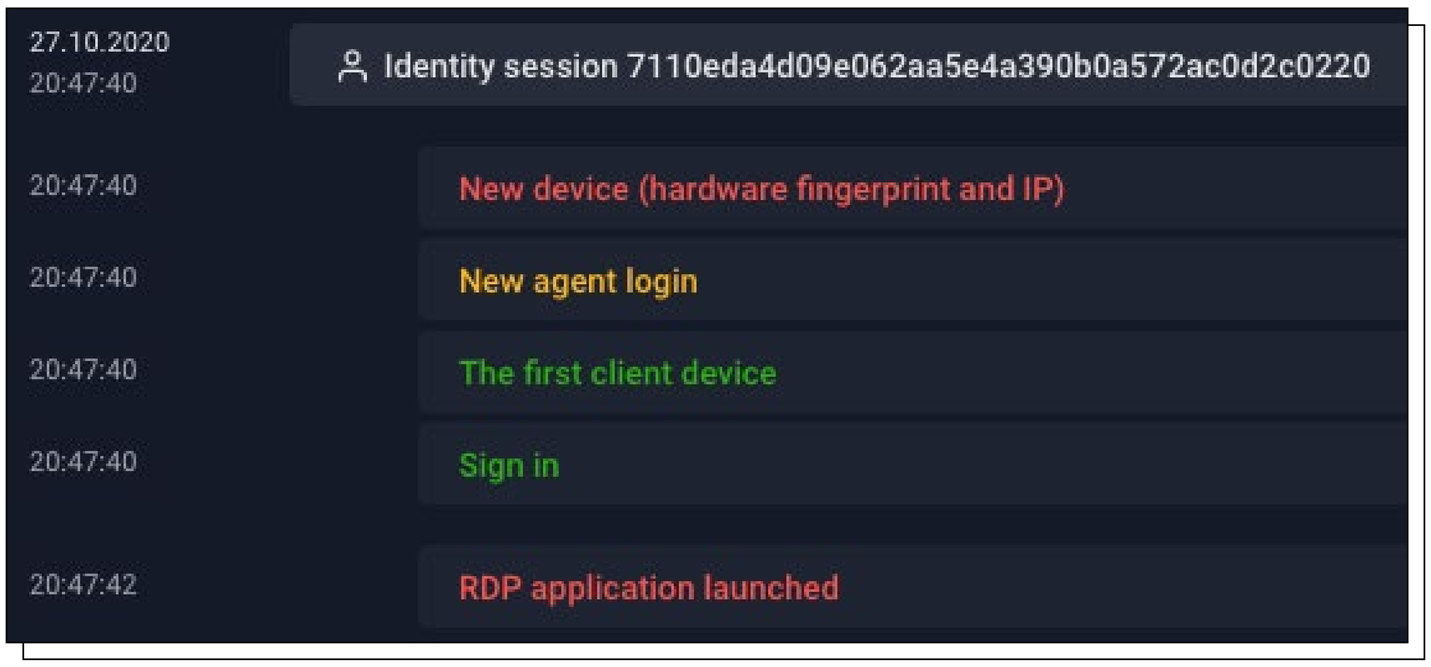
As noted before, the user's behavior is a signal that also helps determine the user's identity. Behavior analysis is based on the user's speed and navigation, mouse movement patterns, typing cadence, and interaction with form fields.

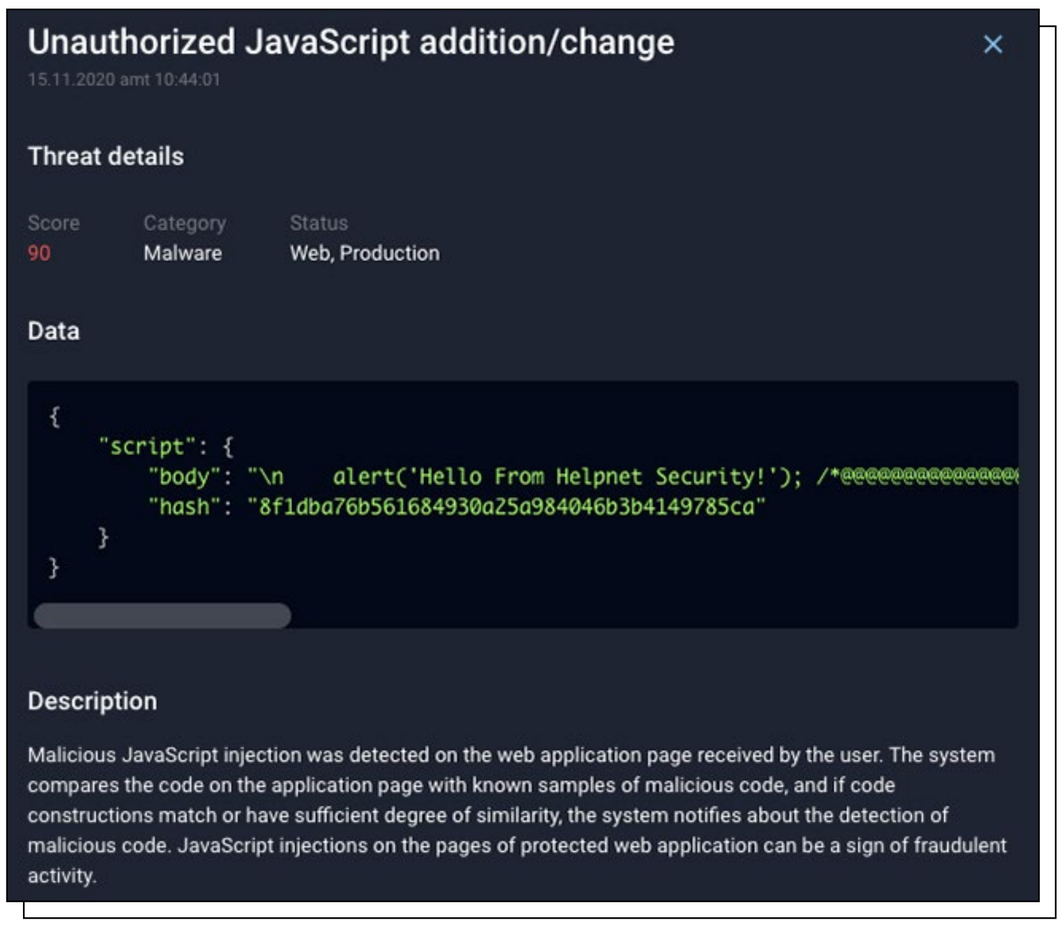
FIGURE 5. THE SESSION DETAILS SHOW THE TRIGGERED ALERTS. IN THIS EXAMPLE, A SUSPICIOUS VISITOR LOGGED IN WITH MULTIPLE ACCOUNTS AFTER CHANGING HIS DEVICE AND IP ADDRESS. THE FHP ALSO DETECTED THAT THE LOGIN WAS PERFORMED BY A PASSWORD COPIED FROM CLIPBOARD.



The FHP detects abnormal user events such as IP and location changes, use of VPN/TOR, proxy use, and User-Agent and OS changes while accessing the monitored site. The FHP also detects automatization technologies such as PhantomJS and Selenium, which mimic user behavior and web page interaction.

FIGURE 6. DETECTION OF AN RDP (REMOTE DESKTOP) SESSION





The FHP can detect malicious injects and remote sessions. Attackers or malware can inject malicious JavaScript code into a website to change its structure or to enable Man-in-the-Browser attacks, with the ultimate purpose of stealing user information. In the FHP Script section, the service owner can configure which script will be treated as dangerous and which as a false positive (e.g., if they use third-party services that change their site's structure).

FIGURE 7. DETECTION OF A JAVASCRIPT INJECT

Some attacks involve the use of remote access tools like RDP, VNC, TeamViewer, etc. The FHP can detect them.

FIGURE 8. DETECTED SCRIPT INJECTIONS CAN BE AUDITED AND CLASSIFIED AS BENIGN TO PREVENT FALSE POSITIVE DETECTIONS

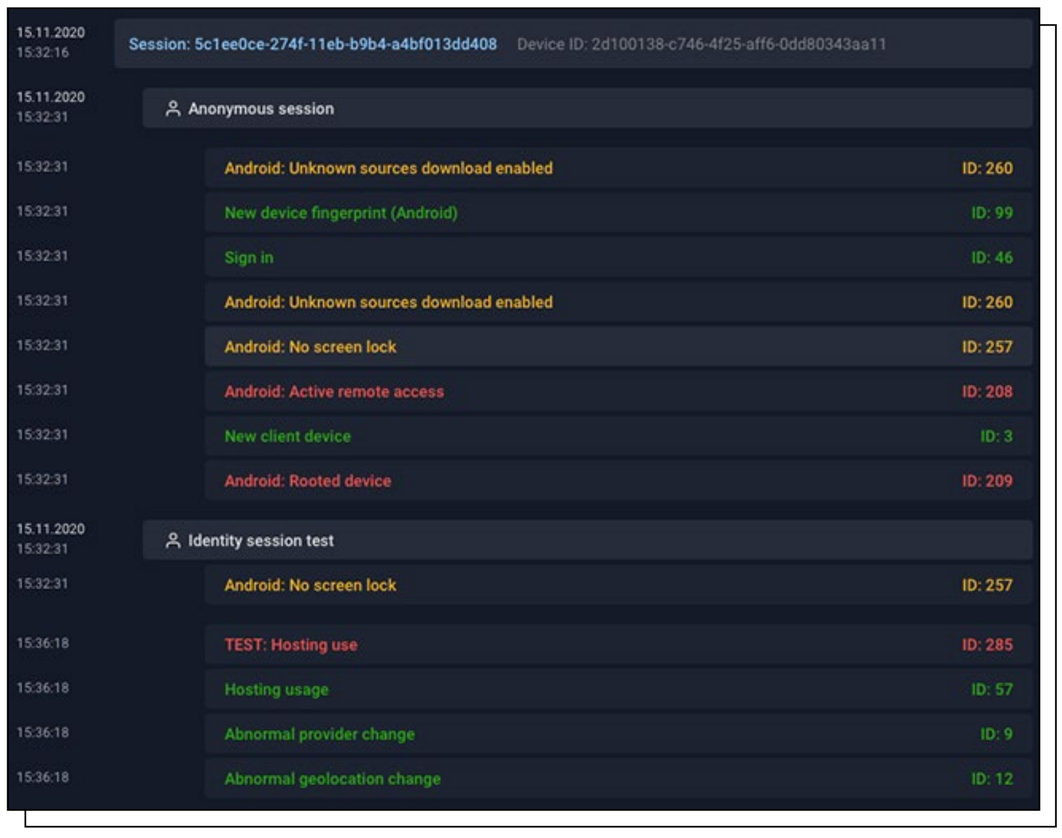


FIGURE 9. WHEN USING THE MOBILE SDK, THE FHP CAN DETECT ROOTED DEVICES AND INSECURE PERMISSIONS AND SETTINGS

Mobile SDK can also detect the use of remote access tools, trojans using Accessibility Service (which is currently employed by such trojans as EventBot, Ghimob, Gustoff), and overlays.

The Preventive Proxy

The FHP uses a component named Preventive Proxy to react to detected bot activity. The Preventive Proxy is a policy-based module that is used to detect traffic type and to define actions related to specific bot detection. It either works on all incoming traffic or on individual requests. After analyzing the device data and user behavior, the FHP can detect whether a specific request to the application API is generated by a bot or is the result of legitimate user activity.

Based on the FHP's verdict, the Preventive Proxy can in real time:

- Pass legitimate request
- Mark suspicious request
- Block malicious bot request

FIGURE 10. THE BOTS SECTION CONTAINS THE DETECTIONS RELATED TO THE PREVENTIVE PROXY

Some of the scenarios where the Preventive Proxy comes useful as a blocking technology are:

- Unethical scraping and use of automation tools (e.g., Selenium) to mimic users
- Brute-force login attacks
- Credential stuffing
- Application-level DDoS
- Cookie theft
- Unauthorized API use

The Preventive Proxy can be tightly integrated with the load balancer serving the website. Two implementation scenarios are possible:

- In the first, the Preventive Proxy is used as an advisor that messages the load balancer on the bot events that should be blocked (Advisor mode). The events are transmitted in the HTTP Header and the balancer should be configured to act according to those events.

- The second scenario is a classic inline installation where the Preventive Proxy acts as a real proxy and blocks detected malicious traffic. For testing purposes, the Preventive Proxy can be set in monitoring mode (to propagate events and not block traffic).

Investigation

The analytical part is where the Fraud Hunting Platform really shines. The Investigation section in the web interface provides useful visualization capabilities based on graph analysis. The graph view allows the investigator to dig deeper into the details of potential incidents and connect the dots between multiple threat actors that are attacking the monitored web site.

The Investigation section allows service owners to search and analyze connections between IP addresses, devices and user identities. They can build a graph based on the data that can be found in the Fraud section, such as IP address, subnet, Identity, Device identifier, or Global ID (we will discuss this identifier in the next section).

FIGURE 11. INVESTIGATION - A GRAPH VIEW SHOWS INTERCONNECTED DEVICES AND MULTIPLE IDENTITIES ACCESSING THE MONITORED SITE FROM DIFFERENT LOCATIONS

The Investigation section provides a good summary for detecting attack patterns that are less obvious and involve a lot of data and interdependencies. The Investigation view can be beneficial while investigating specific cases and for faster resolution of various techniques that attackers use. For example, in cases where attackers use stolen information to perform payment fraud, access private data or perform money laundering, they try to hide their traces by rotating their originating IP address or they spoof their access details. Investigation with the available graph can help fraud analysts to spot those patterns and reduce the time to detect the incident and perform remediation actions.

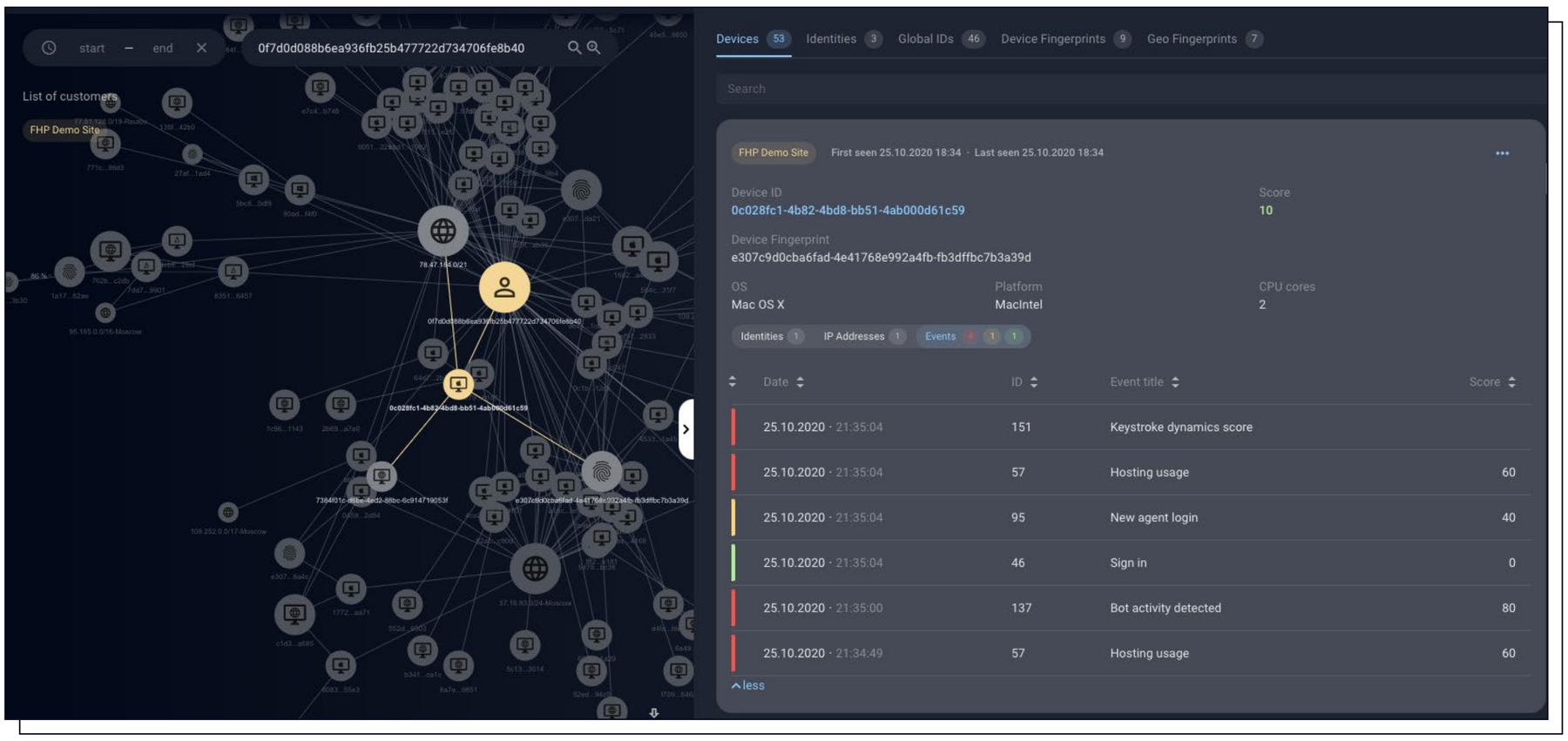


FIGURE 12. THE INVESTIGATION SECTION REVEALS A SUMMARY OF EVENTS TRIGGERED BY THE USER

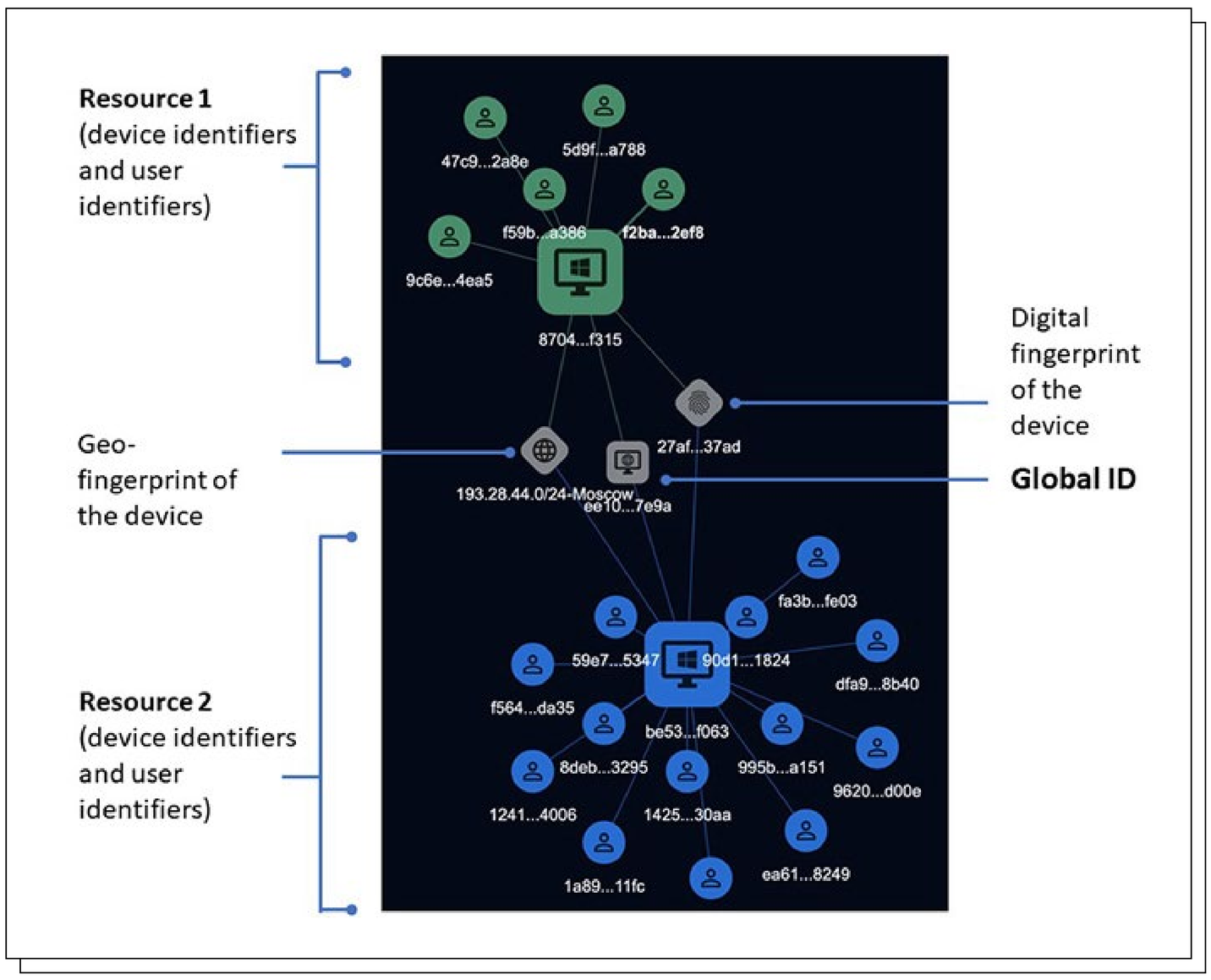
Global ID

Global ID technology provides globally distributed user identification, so if the service owner monitors different sites, they can correlate identified users that access all their monitored resources.

Web browsers (Chrome, Mozilla Firefox) have recently stopped storing third-party cookies by default. Global ID technology works even if this browser policy is enabled and allows users to be recognized regardless of restrictions. Global ID is usually used in the investigation of incidents, and it helps to establish links between devices and events used across all service resources.

Global ID does not require the collection of users' personal information and does not disclose anything about the user except their identification number and can be recorded on a different permission level (global, country, region and organization level).

FIGURE 13. GLOBAL ID CONNECTS THE USE OF DIFFERENT RESOURCES BY THE SAME THREAT ACTOR



This enables Global IDs to be exchanged between FHP users that use the same level, so that they will be alerted when an attacker with a previously known Global ID starts probing their services.

Global ID identifiers exchanged across different protected resources can help investigations that analyze fraudulent activities on a larger scale (e.g., in cases when multiple financial institutions or branches are involved in money laundering or payment fraud).

Final thoughts and verdict

The Group-IB Fraud Hunting Platform is an innovative product that performs bot and fraud detection well. FHP integration on the client-side is very simple. Back-end integration may be more or less difficult, depending on the selected implementation type (cloud or on-premises). The on-premises installation and a tight integration with other systems can require more time and planning. During the tests, no slowdowns were noted on the demo websites that we used.

The FHP provides more information than just plain event logging, because it collects user signals that are relevant for detecting frauds activities. The innovative features extracted from the raw data trigger alerts that can help remove blind spots that you were not aware of.

It can also compete with SIEMs in some use cases, but it's more specialized and gives better insight to fraudulent activities than just doing log correlation would. In other words, the FHP will help you detect fraud and malicious activity faster than your SIEM.

FHP's bot detection capabilities and the blocking performed by the Preventive Proxy can provide a better mechanism for blocking bots than popular CAPTCHAs. The Preventive Proxy does not need any supervision for blocking successive bot requests when they are detected, while CAPTCHAs - when broken - enable attackers to access all the resources through session reuse.

We have tried scraping the demo website without success. The Preventive Proxy marked all responses to our scraper requests as "403 Forbidden". The FHP also makes use of the Group-IB Threat Intelligence database so some targeted attacks to services can be spotted early in the kill chain.

We liked using the platform. No prior training is needed because it's very intuitive, elegant and slick (it also comes in dark mode by default). A gentle learning curve means that you can onboard threat and fraud analysts to use the FHP in minutes, instructing them on just the essential concepts. The FHP will not overwhelm them with a lot of details but give them the ability to pivot their search based on their investigation interest. Events that need additional action are visible and emphasized with colors depending on the risk factor.

The part we liked best is the investigation capabilities. The Investigation is based on graph (network) analysis and can save analysts a lot of time while they are analyzing access patterns. It provides a good summary of events and other relevant details to the investigation (e.g., geolocation, identities, device information, etc.). The Global ID is a great add-on that helps bridge various access patterns between services and can help spot specific attacker groups patterns that are potentially targeting one's service.

Based on the conducted tests and the investigation capabilities, we can recommend the Group-IB Fraud Hunting Platform to those who are searching for more insight about users of their web service(s) or mobile application(s), or to those who want to improve the fraud detection process in their company.

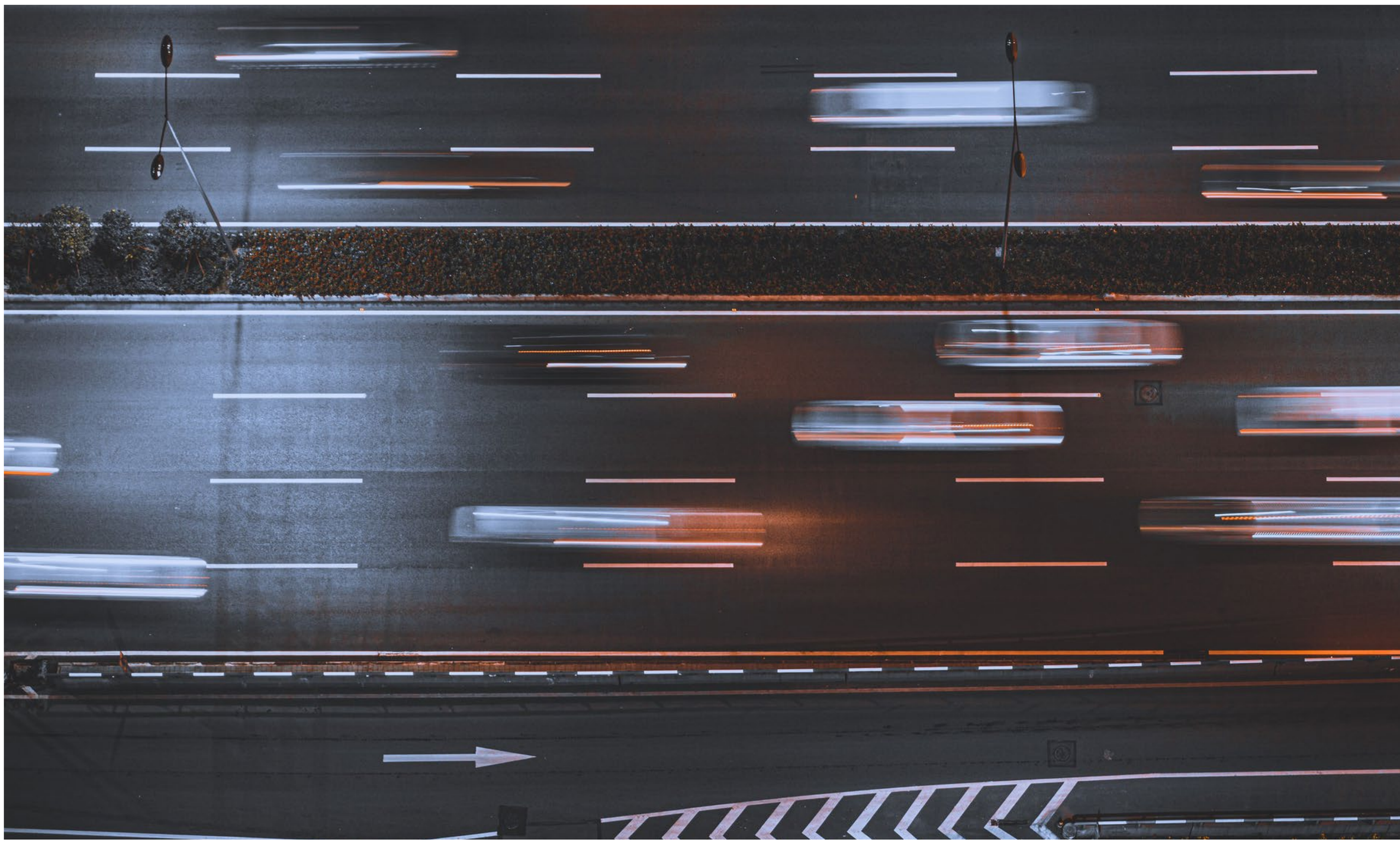
Malware Intelligence

Real-time alerts with
“always on” monitoring
and collection

Detect your adversaries
in minutes

LEARN MORE

INTEL471



The transportation sector needs a standards-driven, industry-wide approach to cybersecurity

AUTHOR_ Nathaniel Meron, CPO & CMO, C2A Security

Despite the uncertainties of the last year, the transformation of the transportation sector forged ahead, dominated by the prevailing trend of CASE (Connected, Autonomous, Shared, Electrified) technologies.

Despite small setbacks caused by COVID-19 that impacted the automotive industry at large, analysts predict electric vehicle (EV) demand will continue on its upward trajectory in 2021, driven by new models, improved batteries, more readily available charging infrastructure, new markets, and price parity with traditional gas-powered vehicles.

As more countries adopt aggressive climate goals and announce plans to phase out gas-powered vehicles, demand for EVs will only continue to rise, jumping from 10% of vehicle sales to 58% by 2040. In the US, the Biden administration's proposed climate change policies are expected to be a significant driver in the short term as well.

Wireless 5G technology will underpin the future success of CASE vehicles by providing more opportunities for seamless integration and rapid connectivity speeds.

Further, autonomous driving draws closer to becoming an everyday reality as popular ride-share companies like Lyft invest heavily in this technology and new autonomous only ventures like Zoox, acquired by Amazon, aim to enter the market. Wireless 5G technology will underpin the future success of CASE vehicles by providing more opportunities for seamless integration and rapid connectivity speeds. A key element that should remain at the forefront of these trends is a standardized approach to automotive cyber security that's prioritized as a safety issue.

Implications for the EV market

Less air pollution, reduced carbon emissions, and a future of improved energy security are exciting benefits of EVs, but they are not without risks. When you consider that the charging infrastructure, commercial EV fleets, and power grids/utilities are all part of the EV ecosystem, cybersecurity must become as critical for mainstream EV adoption as battery performance and other commonly touted aspects.

We have already witnessed attacks on electronic charging stations via the Near-Field Communication (NFC) card, which handles billing for EV charging. The ID cards have inherent vulnerabilities due to third-party providers not securing customer data. Research has shown malicious individuals can copy these cards and use them to charge other vehicles.

Another concern is related to traditional lithium-ion batteries, which are used in EVs and have the potential to explode. While this issue is being addressed by battery suppliers with investment in R&D, this safety effort must also consider the risk of cyber attacks. If it's known that a battery in an EV can explode, this may increase the likelihood that a bad actor may target this type of car with the intent to cause harm. As EV battery technology advances, it's imperative that comprehensive cybersecurity measures evolve and improve in parallel so automakers and technology providers can prevent this type of hacking from occurring.

Risks to autonomous vehicles

As the AV industry advances, so will the incentives for hackers. There is an increased potential for financial crimes committed via ransomware attacks. Further, these attacks could cause vehicles to behave abnormally, potentially endangering human lives.

Robo taxis will most likely be the first AVs to hit the roads, and they are coming sooner than most consumers think. Unlike the current mobility landscape, in which there is a lack of clarity around who is responsible for what in the supply chain, the relationship between consumer and taxi provider is very well defined for robo taxis. The risk to the industry is much higher here, because if this emerging industry is deemed unsafe from the onset due to cybersecurity risks or early issues, it could be doomed to fail before it even has a chance to flourish.

Within the next three years, it's projected that 5G-connected cars will grow from 15% in 2020 to 75% in 2023, reaching 94% in 2028.

Implications of rolling out 5G

Although 5G networks are still a work in progress for mobile operators, we're well on our way to

deployment across the automotive industry. Within the next three years, it's projected that 5G-connected cars will grow from 15% in 2020 to 75% in 2023, reaching 94% in 2028.

While the expansion of 5G will be a boon for both in-vehicle systems and the manufacturing process, it also opens the doors for new cybersecurity risks that will require every link in the supply chain to protect itself.

> *We must adopt a standards-driven, centralized and industry-wide approach to cybersecurity for all vehicles and their supply chains in order to ensure that the automotive sector can adapt to shifting demands and benefit from promising new technologies.*

By 2028, vehicle-to-everything (V2X) communication, which is based on 5G, will be prominently used in all vehicles. This technology enables the exchange of messages both within and between vehicles, as well as infrastructure, pedestrians, cyclists and other elements, in order to improve road safety.

Considering that communications will start to go through cell towers, as opposed to traditional original equipment manufacturer (OEM) servers, it's important that security measures are integrated from the beginning. Since 5G technology also allows vehicles to connect with even more applications through the vehicle, each one will all need its own centralized cybersecurity measures.

What can we do?

To address these risks adequately, it's important that we understand a hacker's goals and motives, as well as how they plan to attack their targets - in our case, vehicles.

As technology advances to include more applications between the vehicle and the "outside," the avenues for attack (surfaces) multiply. Today, a large-scale attack will probably rely on exploiting the communication channel between the OEM and the vehicle itself (e.g., over-the-air). However, the aforementioned technologies are providing new communication channels that can be exploited. What was once a playground has become a Disneyland for attackers with several software-driven systems that can be hacked.

With more opportunities for attack, the chances of finding a successful one increases, bringing down the cost to hackers. The result? Higher ROI for bad actors and an industry that must be ready for new cyber malicious entrants to the automotive ecosystem.

We must adopt a standards-driven, centralized and industry-wide approach to cybersecurity for all vehicles and their supply chains in order to ensure that the automotive sector can adapt to shifting demands and benefit from promising new technologies.

With the much-needed changes in the regulatory environment for automotive cybersecurity finally here in the new ISO 21434 standard and UNECE WP.29, the clock is ticking for the entire automotive ecosystem to act. In 2021, OEMs will need to identify practical ways to rapidly translate current and future policies into practical cybersecurity measures for the connected cars of today and the all-electric, level 5 autonomous vehicles of tomorrow.

Tips for boosting the Sec part of DevSecOps

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

The most significant barrier to achieving DevSecOps is the continued perception that “Sec” is not already a part of “Dev” and “Ops”, says James Arlen, CISO at cloud data platform provider Aiven. Also, the fact this needs to be explicitly called out is actually a barrier in itself.

“In my experience, this is due to the ‘I’m from Security and I’m here to save you’ mentality that continues to pervade the security industry, and the only way to overcome this is with a big bucket of humility,” he noted.

“Security has not actually spent the last 20 years doing a good job of ‘security things’ and we do not have a strong position to say that we have all of the answers. I know that it sounds relatively simplistic, but it really is a case of taking the path of the beginner’s mind and working with developers, operators, and DevOps staff to learn their perspective and then apply domain-specific security knowledge.”

Security needs humility

Arlen has spent most of its career in the information security industry and filled a variety of roles – from firewall operator to CISO – in small startups, large publicly traded companies, and even in the government sector.

He’s also one of the lead authors of the Cloud Security Alliance Guidance for Critical Areas of Focus in Cloud Computing and the associated Certificate of Cloud Security Knowledge.

On the DevOps side, he has experience as a system administrator and has spent years leading the SRE and Production Engineering teams for the hyperscale environment at cloud platform-as-a-service company Heroku (a subsidiary of Salesforce).

When he says that the best way to make security a cooperative function within other business processes is to stop treating security as a special snowflake set of requirements "that can only be brought down to the peasants from the palace," I can't help but laugh, but he insists that he has seen many organizations experience negative outcomes due to the pompous attitude of their security staff.

"Be humble, work with other stakeholders, and remember that security is a priority, but not always THE priority," he advised.

Organizations need to stop treating security as some kind of special thing. We used to talk about how security was a non-functional requirement. Turns out that this was a wrong assumption, because security is very much a function of modern software.

Getting developers on board with DevSecOps

Here's another of Arlen's tips for pushing developers to prioritize security: stop talking about security!

"If there's a thing that, as a security person, you'd call a 'vulnerability,' keep that word to yourself and instead speak the language of the developers: it's a defect," he pointed out.

"Developers are already incentivized to manage defects in code. Allow those existing prioritization and incentivization tools to do their job and you'll gain the security-positive outcomes that you're looking for."

All in all, he says that the primary method for improving the security outcomes of development is both easy and complex.

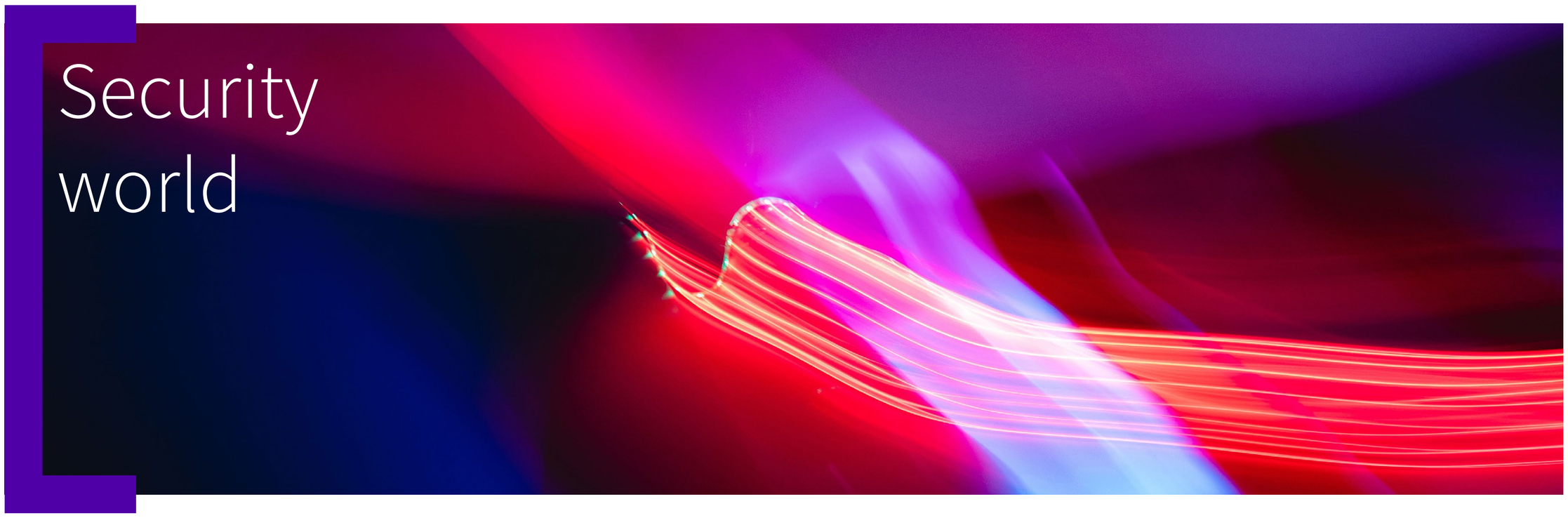
"Organizations need to stop treating security as some kind of special thing. We used to talk about how security was a non-functional requirement. Turns out that this was a wrong assumption, because security is very much a function of modern software. This means it needs to be included as you would any other requirement and let the normal methods of development defect management take over and do what they already do," he noted.

"There will be some uplift requirements to ensure your development staff understands how to write tests that validate security posture (i.e., a set of tests that exercise your user input validation module), but this is generally not a significant problem as long as you've built in the time to do this kind of work by including the security requirements in that set of epics and stories that fit within the team's sprint budget."

Finally, he points out that the most essential thing for achieving DevSecOps is "positive programmatic control," where everything is automated and everything runs because it must.

"Humans should interact with a DevSecOps environment only through adjusting the programming of the control and orchestration systems, rather than by 'fixing' any particular system. Supporting this will require both ephemeral and immutable (or serverless) systems and the tacit acknowledgement that any computer which has had an interactive session (command line) with a human is 'dirty' and must be replaced as quickly as possible."

Security world



Cybersecurity risks connected to AI in autonomous vehicles

By removing the most common cause of traffic accidents – the human driver – autonomous vehicles are expected to reduce traffic accidents and fatalities. However, they may pose a completely different type of risk to drivers, passengers and pedestrians.

Autonomous vehicles use artificial intelligence systems, which employ machine learning techniques to collect, analyze and transfer data, in order to make decisions that in conventional cars are taken by humans. These systems, like all IT systems, are vulnerable to attacks that could compromise the proper functioning of the vehicle.

The AI systems of an autonomous vehicle are working non-stop to recognize traffic signs and road markings, to detect vehicles, estimate their speed, to plan the path ahead. Apart from unintentional threats, such as sudden malfunctions, these systems are vulnerable to intentional attacks that have the specific aim to interfere with the AI system and to disrupt safety-critical functions.

Adding paint on the road to misguide the navigation, or stickers on a stop sign to prevent its recognition are examples of such attacks. These alterations can lead to the AI system wrongly classifying objects, and subsequently to the autonomous vehicle behaving in a way that could be dangerous.

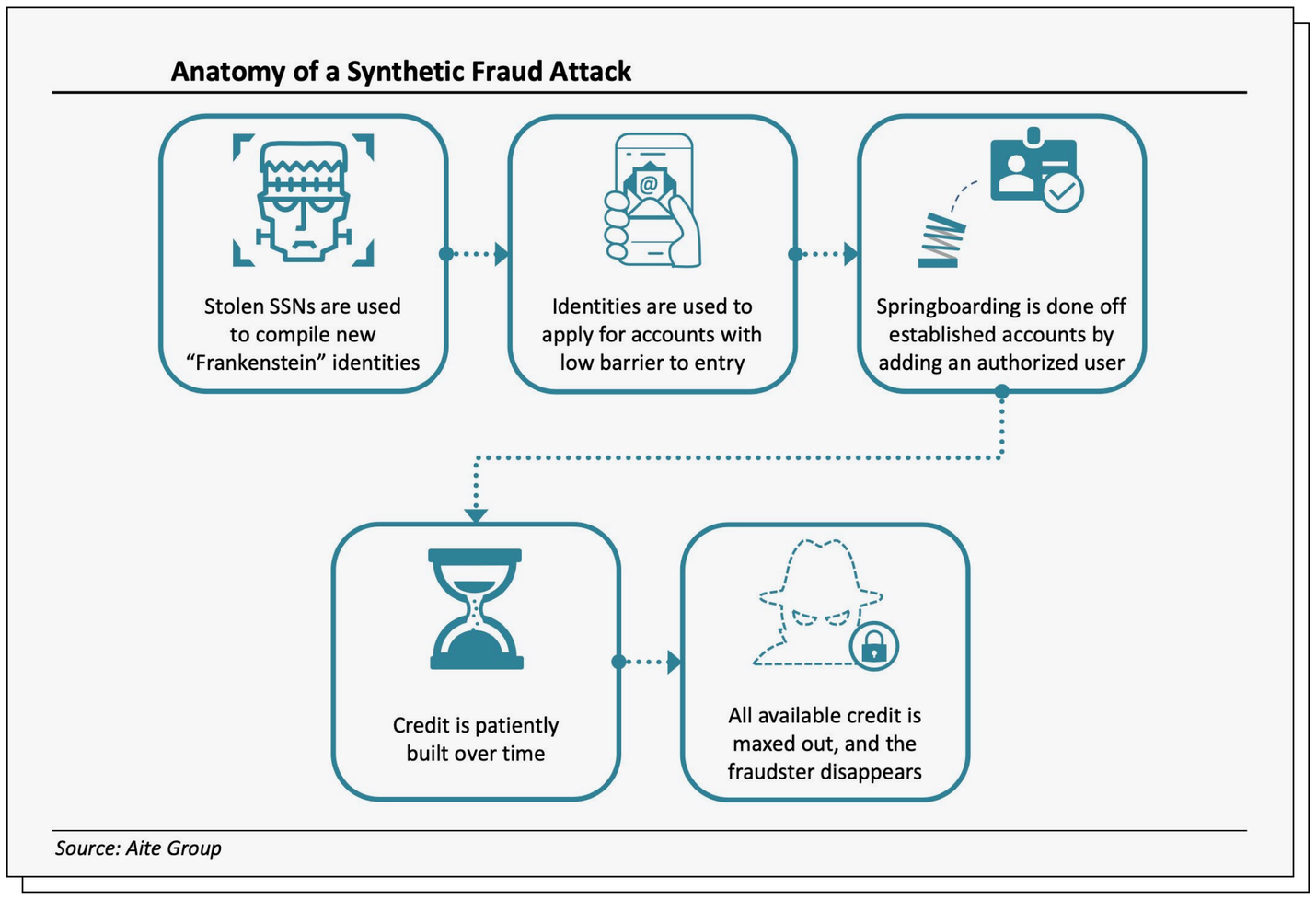
Most security pros think a WAF is high maintenance

An organization's web application firewall (WAF) is a critical line of defense in protecting proprietary and customer data, but the concern is that some organizations are spending an outsized allotment of resources on modifying these mission-critical elements, a Neustar report revealed.

The survey showed that nearly 85% of organizations feel they are spending at least a moderate amount of time on modifications, with almost 40% noting they spend a lot of time.

Moreover, a majority of organizations have siloed their data center services away from cloud services — nearly four in five surveyed — which could have the unintended consequence of increasing labor-intensive protection processes.

The cost of synthetic fraud to reach new highs



A TransUnion research has found that instances of synthetic fraud and outstanding balances for suspected synthetic accounts at U.S. financial institutions have declined significantly after the WHO declared COVID-19 a global pandemic. However, new analysis by Aite Group has found that the cost of synthetic fraud will rebound post-pandemic, reaching new highs.

Synthetic identity fraud involves fraudsters creating fictitious identities by piecing together real identity attributes and fake information with the intent to open fraudulent accounts.

"The dip in synthetic fraud during the pandemic was a continuation of our 2019 findings that showed synthetic fraud was slowing amid the emergence of solutions that connect personal and digital identities," said Shai Cohen, SVP of Global Fraud Solutions at TransUnion.

"We believe this slowdown was compounded by fraudsters who went elsewhere and could be lying in wait to take advantage of pandemic loan forbearance programs that may not have come due yet. Once synthetic fraud reemerges, which we think it will, companies must be ready."

Empowering a remote workforce is a top priority for CEOs

A top challenge for many CEOs over the next few years is managing a remote workforce, a new IBM Institute for Business Value (IBV) study reveals.

CEOs of outperforming organizations – those who were in the top 20 percent for revenue growth of those surveyed – are prioritizing talent, technology and partnerships to position their companies for success post-COVID-19 pandemic.

mHealth apps consistently expose PII and PHI through APIs

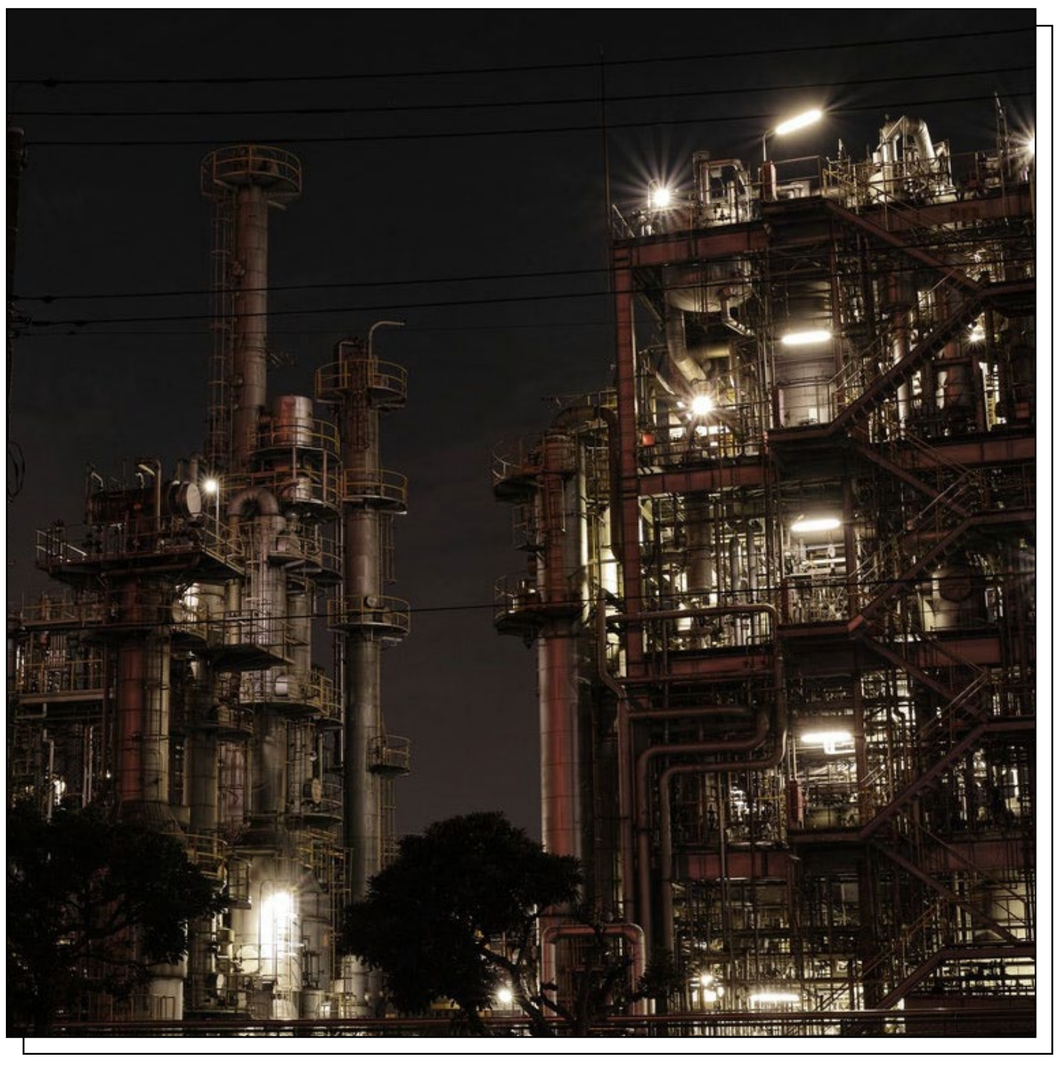
All of the 30 popular mHealth apps that were tested are vulnerable to API attacks that can allow unauthorized access to full patient records including protected health information (PHI) and personally identifiable information (PII), Approov revealed. The study underscores the API shielding actions now urgently required to protect mHealth apps from API abuse.

Cybersecurity spending for critical infrastructure to reach $105.99 billion in 2021

Cybersecurity spending in critical infrastructure has been little impacted by the COVID-19 pandemic, save for some reshuffling on where that spend is most needed. The effect has been mostly in increased demand for secure remote connectivity.

Most of the cybersecurity spending announced by governments has not changed significantly however, with most maintaining similar funding planned in previous years, with an average Year-on-Year growth rate between 5% and 10%.

According to a report by ABI Research, cybersecurity spending for critical infrastructure (CI) will increase by $9 billion over the next year to reach $105.99 billion in 2021.



5G security market to reach 5.226 billion by 2026

The 5G security market size is projected to grow from $580 million in 2020 to $5.226 billion by 2026, at a compound annual growth rate (CAGR) of 44.3% during the forecast period, according to MarketsandMarkets.

The major drivers for the 5G security market include rising security concerns in the 5G networks, increasing ransomware attacks on IoT devices, rising attacks on critical infrastructure, and increasing IoT connections paved way for mMTC with enhanced security requirement.

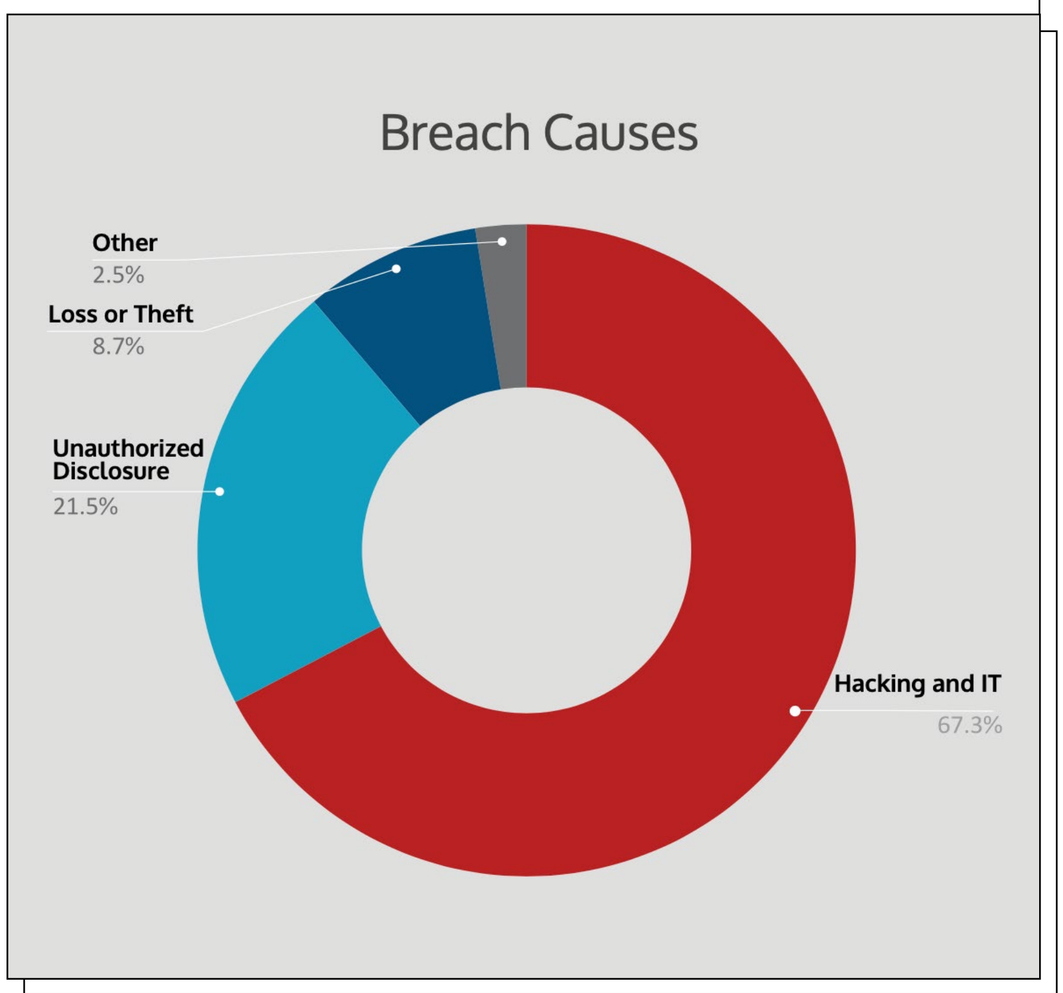
Credential spill incidents nearly doubled since 2016

The number of annual credential spill incidents nearly doubled from 2016 to 2020, according to F5 research. There was a 46% downturn in the number of spilled credentials during the same period.

The average spill size also declined, falling from 63 million records in 2016 to 17 million last year. Meanwhile, the 2020 median spill size (2 million records) represented a 234% increase over 2019 and was the highest since 2016 (2,75 million).

Healthcare breaches increased over 50% in 2020

In 2020, there were 599 healthcare breaches that collectively affected over 26 million individuals. Bitglass' report takes an in-depth look at the breaches that healthcare organizations faced, comparing them to previous years and revealing key trends and cybersecurity challenges facing the industry.



Breaches recorded in the DHHS database are classified into the following categories:

- Hacking and IT incidents: Breaches related to malicious hackers and improper IT security—a cybersecurity events stemming from external parties
- Unauthorized disclosure: Unauthorized sharing of PHI by internal parties or systems
- Loss or theft: Breaches that involve the loss or theft of endpoint devices
- Other: Miscellaneous breaches and leaks

Rampant password reuse puts companies and customers at risk

25.9 million business account credentials and over 543 million breach assets tied to employees in the Fortune 1000 are readily available on the criminal underground, SpyCloud revealed.

"Year after year, studies show that the use of weak and stolen credentials is the most common hacking tactic for cybercriminals, yet 76 percent of employees at the world's largest companies are still reusing passwords across personal and professional accounts," said Chip Witt, VP of product management for SpyCloud.

"People don't seem to realize just how often their credentials end up in criminal hands or how stolen passwords can be used to access other accounts they think are safe."

Regardless of security guidelines that warn against such behavior, many employees, even at the executive level, are using corporate credentials as personal logins for other accounts. When those third-party sites are subject to data breaches, reused employee logins provide criminals with easy access to corporate systems and networks.

Dark web analysis shows high demand for hackers

Positive Technologies' experts have analyzed the ten most active forums on the dark web, which offer services for hacking websites, buying and selling databases, and accessing web resources.

The research found that in the vast majority of cases on these forums, most individuals are looking for a hacker, and in 7 out of 10 ads, their main goal is to gain access to a web resource.

The research discovered that in 90% of cases, users of dark web forums will search for hackers who can provide them with access to a particular resource or who can download a user database.

Only seven percent of forum messages analyzed included individuals offering to hack websites. The remaining three percent of the messages analyzed were aimed at promoting hacking tools, programs and finding like-minded people to share hacking experience.

Consumers not protecting data online despite having privacy concerns

Startpage announced results of its survey exploring the attitudes of Americans towards protecting their own privacy online. The results found a gap between the high levels of online privacy awareness and concern respondents report, and the low levels of action they take to combat increasingly egregious assaults on their privacy.

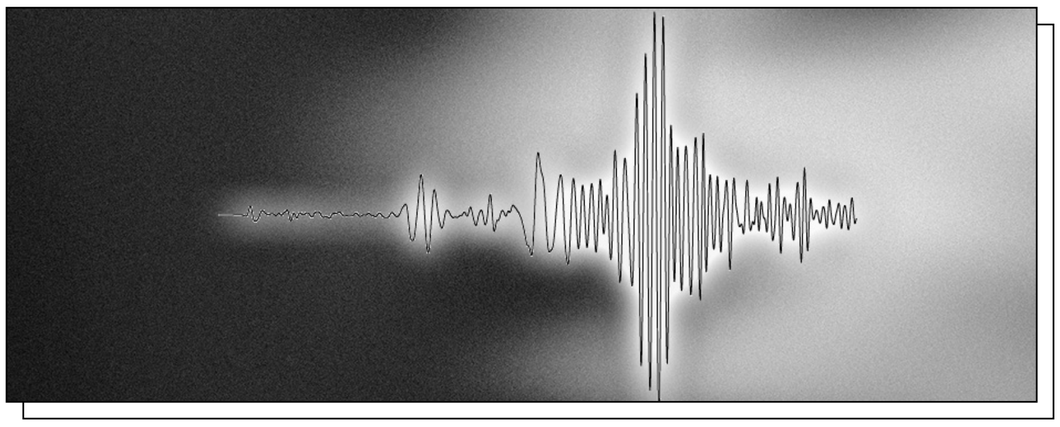
Beyond getting a pulse on Americans' online privacy concerns, the survey explored what action individuals have taken, and plan to take, to protect their personal data online. Startpage found a gap between the 72% of respondents that are very or extremely concerned about their online privacy and concrete action taken to combat these concerns.

17% of people admitted to taking no action to protect their personal data online in the past 12 months and among those that did, 60% updated a password online. Not many people are actively taking precautions beyond changing passwords.

The cybersecurity issues of seismic monitoring devices

Seismic monitoring devices linked to the internet are vulnerable to cyberattacks that could disrupt data collection and processing, say researchers who have probed the devices for weak points.

Common security issues such as non-encrypted data, insecure protocols, and poor user authentication mechanisms are among the biggest

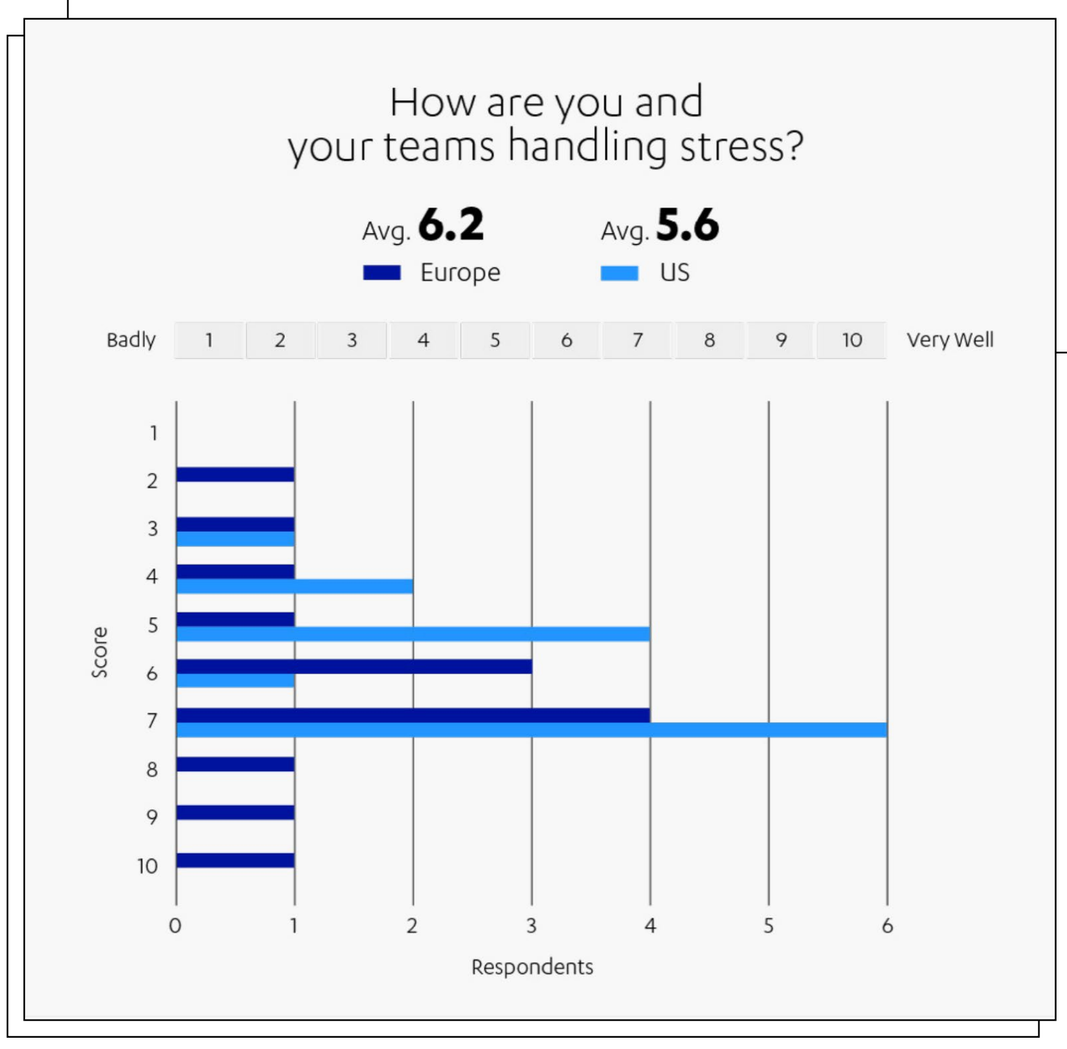


culprits that leave seismological networks open to security breaches, Michael Samios of the National Observatory of Athens and colleagues wrote in a new study.

Emotional intelligence playing an increasingly important role for CISOs

The increasing importance of emotional intelligence and other skills required to work with different stakeholders are placing new demands on CISOs. However, it's also creating opportunities for CISOs to become leaders of their organizations, according to a report from F-Secure.

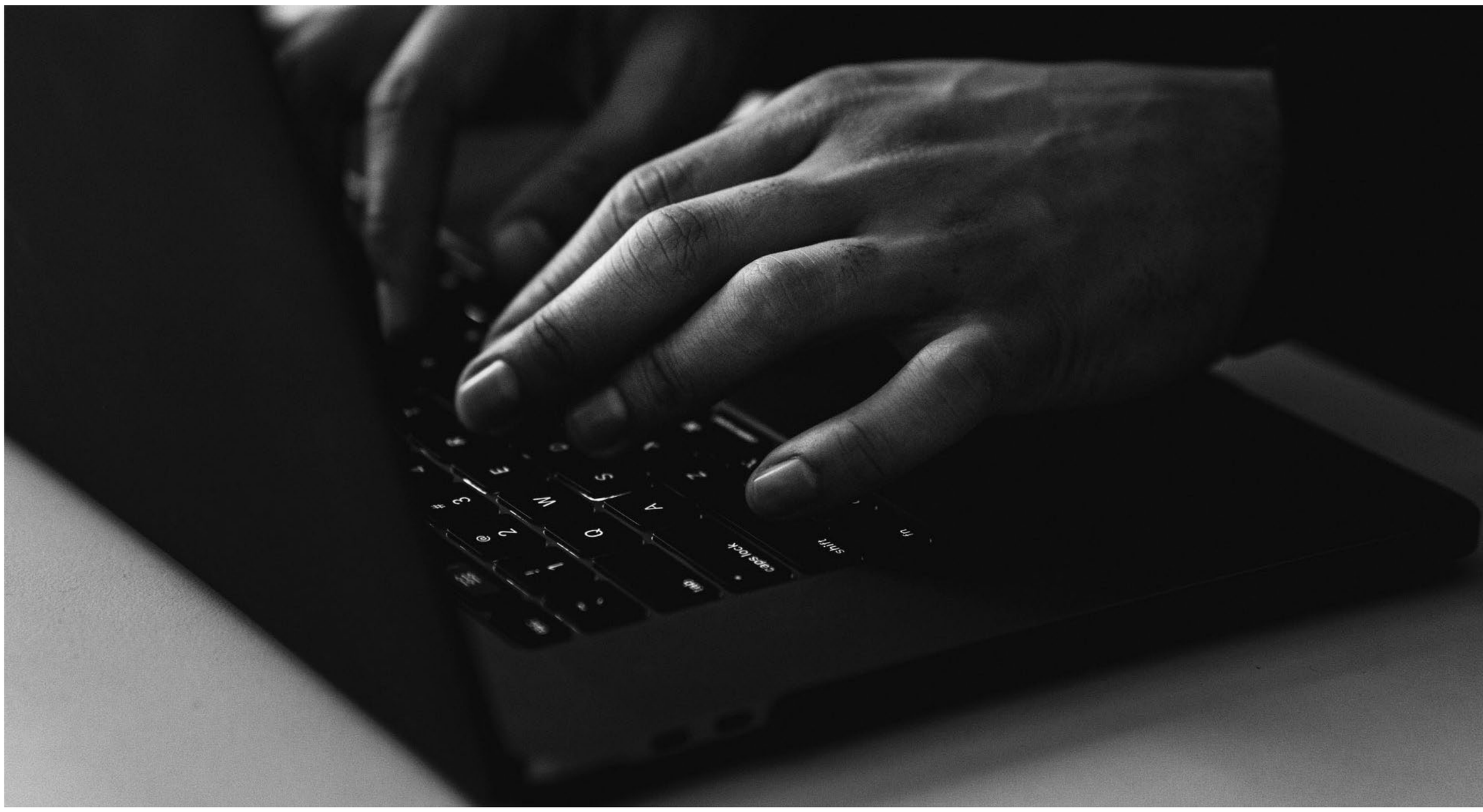
Traditionally, CISOs' roles were treated as technical roles first, with secondary importance placed on non-technical skills. However, a series of in-depth interviews conducted for the report with CISOs in the US, UK, and other European countries, suggests that this idea is quickly becoming obsolete.



Most zoombombing incidents are inside jobs

Most zoombombing incidents are "inside jobs," according to a study featuring researchers at Binghamton University, State University of New York.

Researchers found that the vast majority of zoombombing are not caused by attackers stumbling upon meeting invitations or brute-forcing their ID numbers, but rather by insiders who have legitimate access to these meetings, particularly students in high school and college classes. Authorized users share links, passwords and other information on sites such as Twitter and 4chan, along with a call to stir up trouble.



Automated vulnerability reports generated by scanning tools are returning hundreds, if not thousands of vulnerabilities.

When it comes to vulnerability triage, ditch CVSS and prioritize exploitability

AUTHOR_ Alex Livshiz, Research Team Lead, SCA, Checkmarx

When it comes to software security, one of the biggest challenges facing developers today is information overload. Thanks in part to the widespread proliferation and use of open-source code (a study by Red Hat showed that 36% of software in use at surveyed organizations was open source), as well as the increasing complexity of the average application, a given project can now be expected to have a massive amount of dependencies. In turn, each of these dependencies represents a potential opportunity for a vulnerability to arise if not properly secured.

Owing to this state of affairs, developers face a new challenge. Automated vulnerability reports generated by scanning tools are returning

hundreds, if not thousands of vulnerabilities, and with a great deal of organizations reporting a lack of skilled cybersecurity professionals, teams are already stretched too thin to fix each one. The prospect of quickly remediating every single vulnerability identified by a scan is unfeasible.

> *Exploitability is a much more important benchmark when it comes to triaging efforts.*

In an effort to resolve this, developers and security professionals have traditionally relied on vulnerability scoring systems to help them prioritize the most critical flaws and streamline remediation efforts. And while this is a good way to get software out the door faster with fewer vulnerabilities, this methodology is too simplistic. Exploitability is a much more important benchmark when it comes to triaging efforts.

Why legacy scoring systems are no longer sufficient

The large number of vulnerabilities returned by automated scans is not a new problem. In fact, it is commonly cited by developers as an obstacle to security. To attempt to filter through these large data sets, developers conduct vulnerability triage where they categorize the flaws that have been detected in order of risk they pose to an application's security or functionality. Then, developers can fix vulnerabilities that seem to be most pressing in order to get software out the door faster.

Currently, many developers rely on the Common Vulnerability Scoring System (CVSS). The system represents a basic standard for assessing the severity of a vulnerability. Scores range from 0-10, with 10 being the higher end of the scale (indicating the highest severity). Developers will often assign CVSS scores to the vulnerabilities they detect and order them from highest to lowest, focusing their efforts on those with the highest scores.

Unfortunately, this method is suboptimal, ultimately resulting in oversights and less "safe" code.

Don't be a foo() when it comes to vulnerability remediation

A large part of getting the most out of security scanning tools comes down to a developer's approach to triaging the vulnerabilities scans detect. Rather than focusing on severity as determined by CVSS scoring, developers should prioritize vulnerabilities by focusing on the potential path they offer for exploitability.

So, what exactly does it mean for a vulnerability to be exploitable? There are two core factors:

- The vulnerable method in the library must be called directly or indirectly from a user's code
- An attacker needs a carefully crafted input to reach the method to trigger the vulnerability

As an example to illustrate this point, imagine a scenario where a vulnerability is triggered by a foo() method in a library being used, but when examined, it is determined that the code itself actually does not call foo() at all. This is an example of how a vulnerability might seem severe on its surface, but when considered in context, offers no real path for exploitation. With this knowledge, a developer can pass on fixing this vulnerability for others that are actually exploitable.

By leveraging automated scanning tools that can analyze the project's source code, and the source code of all used packages, when examining the call graphics and data flows, exploitability and risk can be truly evaluated.

Taking a holistic approach to evaluating the probability of exploitation

The modern developer is equipped with entire libraries of code for a single API method out of dozens. Furthermore, the libraries they employ have other 3rd party libraries themselves that only partially use the available APIs. This means that if a vulnerability is detected in an application's dependencies, the probability of it actually being exploited can be below five percent.

This has a number of important implications for developers attempting to secure software while maintaining efficiency:

- Current approaches to prioritization are focused on the wrong areas, and valuable time is being spent fixing vulnerabilities that may not even be exploitable
- Vulnerabilities that cannot be exploited are, in essence, false positives. If a given code flow cannot be reached by an attacker, it can safely be ignored for other, more pressing issues
- Despite scans returning what appear to be insurmountable lists of vulnerabilities in software, the true number of vulnerabilities that need to be remediated after a scan is significantly lower than is commonly understood today

By leveraging automated scanning tools that can analyze the project's source code, and the source code of all used packages, when examining the call graphics and data flows, exploitability and risk can be truly evaluated.

Security at speed via exploitable path

Developers are facing a number of challenges in the form of a demand for both quicker software delivery and better security in finished code. As a result, we've seen the growth and adoption of open-source code and automated vulnerability scanning technologies.

But while these tools serve a valuable purpose, vulnerability triage is equally essential in software development where agility can either be lost or gained.

To date, the more common triage strategy has been to leverage CVSS scoring, but the exploitable path philosophy offers a different alternative that can help achieve greater efficiency. By focusing efforts on those vulnerabilities that represent a real threat to a piece of software's security, developers can vastly cut down the number of bugs they need to address.

This approach leads not only to faster delivery but should also result in greater confidence on the part of developers who are sure that those vulnerabilities which had actual paths for exploitation have been fixed.

One of the challenges with the current pace of innovation is deciphering what is real and what is vaporware. Most of us are understandably skeptical when we hear of technical advances that sound too good to be true – our skepticism is rooted in our experience filtering endless marketing claims.

As a mathematician, I understand and even celebrate a certain degree of skepticism and believe that the best way to address questions is to present the evidence in a direct manner so individuals can make their own judgements on the topic at hand. I like tackling misconceptions relating to innovative technical advancements in my own line of work, and here I'll talk about homomorphic encryption.

Homomorphic encryption: Myths and misconceptions

AUTHOR_ Ellison Anne Williams, CEO, Enveil

If you're thinking that homomorphic encryption sounds incredible and that we should use it to encrypt everything, you're not alone.

What is homomorphic encryption?

The field of homomorphic encryption has been the focus of academic research for more than four decades, but it has garnered increased attention of late as a pillar of a broader category known as Privacy Enhancing Technologies (PETs).

Grouped together for their ability to enhance and preserve the privacy of data during its processing lifecycle, these business-enabling technologies address an important need for organizations facing global regulatory challenges as well as a consumer base that values privacy more than ever before.

> *While regulations are an effective means for minimizing data exposure risk and safeguarding consumer privacy, they can also make it challenging for banks to discover and expose criminal activity.*

Within the PETs category, homomorphic encryption stands out for its ability to allow encrypted operations (think search or analytics) to be performed on data. From a technical standpoint, it enables operations to be performed on ciphertext as if it were plaintext. This allows data to be used without exposure, delivering an unmatched level of security and privacy enablement.

If you're thinking that homomorphic encryption sounds incredible and that we should use it to encrypt everything, you're not alone. In fact, homomorphic encryption is often hailed as the "holy grail" of crypto for its paradigm-shifting potential to revolutionize how and where organizations can securely and privately leverage data resources and assets.

The advances that have brought homomorphic encryption from land of theoretical research to commercially practical are absolutely worthy of celebration and are transformative to a wide range of business use cases across a variety of verticals. The excitement that continues to build around the space is justified as there are a plethora of ways that it can – and is – being used now for commercial applications in areas including anti-money laundering, financial fraud, and data monetization.

Of course, no technology is a magic bullet that can be used for anything and everything. Homomorphic encryption is no different and there are tradeoffs that come with its use. Moreover, due to its "holy grail" status, there is naturally a lingering degree of skepticism about whether it is ready for broad commercial use. Here are four misconceptions about homomorphic encryption that should be considered by anyone interested in potential use cases.

Myth #1: Homomorphic encryption is not ready for commercial use

When homomorphic encryption was first theorized, it was simply not practical. Performing even the most basic operation (something as simple as 1+1) in ciphertext would take days and an amount of compute power that made it unreasonable for any broad applicability. But that is no longer the case. Advances in the underlying technology, as well as efficiencies relating to its use, mean that homomorphic encryption can now operate at the speed of business for a number of use cases.

Encrypted searches can be performed over millions of data records and returned within seconds rather than days or even weeks (yes, it started out that slow). Commercial and government entities are using homomorphic encryption operationally at scale today. Not working toward using it, but actually using it in production environments to solve real problems.

One of the areas where early adopters have emerged is the financial services industry, for anti-money laundering applications.

While regulations are an effective means for minimizing data exposure risk and safeguarding consumer privacy, they can also make it challenging for banks to discover and expose criminal activity. Regulatory directives frequently prevent global banks from effectively sharing data across privacy jurisdictions, even when that data is contained within branches of their own institutions. For example, if a bank in the UK wants to check information relating to a possible new customer during onboarding, there is no efficient or automated privacy-preserving way for them to ask other branches across the globe if they know anything about the customer being considered. Homomorphic encryption is uniquely able to solve this compliance challenge because it keeps data encrypted during processing, thereby never revealing sensitive data or PII in the other operating jurisdiction.

By creating an encrypted search to run over data in another jurisdiction, the onboarding bank can get the information it needs in real time while respecting the privacy of the potential customer. Homomorphic encryption eliminates compliance risk by ensuring this new sensitive personal information is never exposed to others — or that any unrelated regulated data is introduced into its own jurisdiction.

Myth #2: Everything needs to be encrypted

Homomorphic encryption uniquely enables encrypted processing, allowing thusly-encrypted searches/analytics to be performed over both encrypted and unencrypted data. While HE-encrypted operations can be run over encrypted data, in many use cases, that level of protection is unnecessary. Take, for example, an investor performing research to inform his or her decision-making regarding a possible merger or acquisition. The investor likely turns to standard industry tools, including data aggregators, that can provide the most current information available. Is the underlying data within these third-party environments sensitive? Not at all — the investor just needs to tap into this existing information to understand more about the company and its market positioning. However, is the content of the search and reason behind the query sensitive? Absolutely. Exposing the investor's interest in a specific company could expose intent, potentially signaling it to other interested parties and jeopardizing the investor's bargaining power. In multi-million dollar transactions, the exposure of any such information is extremely significant.

One of the most exciting use cases for homomorphic encryption today is in the area of secure data sharing and collaboration.

Homomorphic encryption solves the problem by enabling investors to specifically protect the part that matters - the content of the query and its corresponding results delivered by the third-party data aggregator - thereby ensuring that their interests and intents are never exposed. In most scenarios, the homomorphic encryption capability can be delivered within the data aggregator's existing environment without the data needing to be moved or changed in any way.

Myth #3: In order to collaborate using homomorphic encryption, all data needs to be pooled

One of the most exciting use cases for homomorphic encryption today is in the area of secure data sharing and collaboration. By allowing third parties to securely and privately work together, it opens the door to never-before-possible opportunities for public-private collaboration, as well as across

private industry. Just consider the gains that could be realized if organizations were able to come together to collectively combat the horrors of human trafficking and drug smuggling on a global scale.

One of the key elements that has prevented such efforts from moving forward in the past is the need to pool sensitive data assets in order to make them accessible to a collective group. This is impractical for a number of reasons, at the core of which is an understandable unwillingness of organizations to increase their own risk and liability by giving up ownership of their assets. Doing so puts the organization in jeopardy of violating privacy regulations, not to mention the broader reputational risk associated with compromising customer trust by exposing their data to third parties - even if it is done with the best of intentions.

While some implementations of homomorphic encryption suggest data must be pooled and encrypted in a centralized location, it is rarely practical or desirable. When homomorphic encryption is used to specifically protect the interaction with the data (in this case, the query or analytic being performed), it can be done in a decentralized manner that allows all contributors to maintain control and ownership of their data assets.

Myth #4: A homomorphic encryption library is a homomorphic encryption solution

While it can sometimes be confusing to people unfamiliar with the space, there is a significant difference between a homomorphic encryption library and an HE-powered solution. Think of it this way: a homomorphic encryption solution is the house; homomorphic encryption libraries are the raw lumber. Homomorphic encryption libraries provide the basic cryptographic components for enabling the capabilities, but it takes a lot of work including software engineering, innovative algorithms, and enterprise integration features to get to a usable, commercial grade product. Companies who build and maintain these libraries do so from their research teams and often offer consulting services to help organizations think about how to design plans to put these basic elements to use.

The impact that ongoing advances in homomorphic encryption – and PETs more generally – will have in the data privacy arena are not being overstated.

Vendors providing homomorphic encryption solutions have already built the house and many times leverage various homomorphic encryption libraries — while some may require remodeling to ensure the product addresses specific needs, the heavy lifting is done. When investigating offerings in the space, it is important organizations know what they are getting: raw building blocks, plans, or a house.

Conclusion

The impact that ongoing advances in homomorphic encryption – and PETs more generally – will have in the data privacy arena are not being overstated. These technologies are positioned to change the way we use and process data, ensuring the organization can perform critical business functions while prioritizing privacy.

Gartner predicts that more than half of organizations will be using privacy-enhancing computation to process data in untrusted environments by 2025. Amid the fast-moving advances taking place to achieve this milestone, it is important we understand what is true and what is not. I am confident that homomorphic encryption will prove compelling enough to stand up to any skepticism encountered along the way.

CIS SecureSuite®

Assess system endpoints from wherever you are.

CIS Center for Internet Security®

www.cisecurity.org

How to motivate employees to take cybersecurity seriously

AUTHOR_Zeljka Zorz, Managing Editor, (IN)SECURE Magazine

How can we push employees/users to take cybersecurity to heart? Dr. Maria Bada, external behavioral scientist at AwareGO, has been working on the answer for years.

After studying media psychology, focusing her Ph.D. on behavior change, and working towards the treatment of excessive internet use in children and adolescents, nearly ten years ago she opted to join Oxford University as a postdoctoral researcher on cyberculture and online behavior.

Her research focused on the human factor of cybersecurity, the assessment of cybersecurity awareness campaigns and their impact in changing online behavior and, gradually, it expanded from the user to the offender.

“The application of traditional theories of psychology in studying cybercrime is something I find fascinating and this research is also

contributing to the emerging discipline of cyberpsychology. Within my current role at the University of Cambridge Cybercrime Centre, my research focuses on the human factor in cybercrime. More specifically, I work on the profiling of cybercriminals, the cybercrime ecosystem and how the Internet supports criminal behavior online," she told (IN)SECURE Magazine.

Users often avoid cybersecurity because they cannot understand it or because understanding it requires a lot of effort.

She believes in the importance of understanding both the offenders' behavior AND users' needs in order to develop effective prevention interventions, and her current collaboration with AwareGO provides her with the opportunity to apply her research in a practical way to develop innovate methods in cybersecurity awareness training and assessment.

All members of the digital community need to develop a cybersecurity mindset and create a cybersecurity culture where knowledge is being shared and communicated to all.

In this interview, she talks about the requisite factors for successful security awareness education.

[Answers have been edited for clarity.]

_ I've often found that people don't grasp cybersecurity topics when they are explained in abstract language. Some shut down immediately, others have trouble imagining the wide variety of instances when the imparted knowledge can be used, and many are afraid to ask "stupid" questions. How can one make sure to address all of these and other stumbling blocks in the way of successful cybersecurity knowledge transfer?

It's true that cybersecurity is often assumed to be purely technical. However, when we look at the threats and how they become reality, that we can see and truly understand that cybersecurity is about people more than it is about technology.

Users often avoid cybersecurity because they cannot understand it or because understanding it requires a lot of effort. Convenience is most of the times preferred over security and this is a serious stumbling block.

During the COVID-19 pandemic we witnessed organizations having to quickly advance or coordinate their cybersecurity efforts as many employees started working from home. That meant that even employees who avoided thinking or learning about cybersecurity had to do some training or follow specific policies around remote working.

For something like that to be effective at a large scale there has to be knowledge transfer at all levels of an organization, language needs to be as simple as possible and actions required need to be as clear as possible. Therefore, to ensure that cybersecurity is being considered by the user, the training and instructions need to be targeted, actionable and (easily) doable.

All members of the digital community need to develop a cybersecurity mindset and create a

cybersecurity culture where knowledge is being shared and communicated to all. The most important part is to use that knowledge to improve everyday life. Technology should be part of our lives, fit our comfort zone, and be something we trust and don't feel intimidated by due to lack of knowledge and digital literacy.

_ *What are the dos and don'ts of setting up successful security awareness training and campaigns?*

Before developing a cybersecurity awareness training campaign, we need to identify our target group and the specific needs of this group. Changing behavior requires more than providing information about risks and reactive behaviors – people need to be able to understand and apply the advice we provide and they most important they need to be willing and motivated to follow that advice.

Many campaigns in the past have demanded a lot of effort and skills from the audience, setting unrealistic expectations, while solutions are not aligned to risks. One of the tactics often used in cybersecurity awareness campaigns have been fear invocations, but they generally proved insufficient to change behavior, so avoid those.

The offered advice/knowledge needs to meet the needs of the target group while training and continuous feedback is needed to sustain the information received.

Also, different cultural or personality characteristics need to be considered since these factors can influence the outcome of the campaign. For example, an individualistic culture needs a different approach compared to a more collectivist one.

> *People are aware of cybersecurity because they hear a lot about it. But that doesn't mean that people are behaving how we would like when it comes to matters such as password authentication and social engineering attacks.*

_ *What currently uncommon IT and cybersecurity educational practices / tools you believe have a future?*

In my opinion, we will be seeing a lot of efforts internationally in raising cybersecurity education and awareness across all disciplines. To do that, new technologies will be utilized, such as virtual reality. Virtual reality can spark the imagination, encourage creative learning, and offer memorable training experiences for employees.

_ *Technology is evolving too fast for a great chunk of humanity to be able to catch up and learn the nuances of its use. The gap is particularly wide when it comes to using the internet and keeping up with the ways the dissemination of information, disinformation efforts and propaganda are evolving. Malicious actors and even businesses are essentially hacking and hijacking the human brain and emotions. Is there a light at the end of that particular tunnel and what will it entail?*

There is currently a digital divide at a national and individual level. We see many countries leading in cybersecurity technologies but also legislation

on cybercrime. Other countries are now beginning to develop their capacities, their strategies and efforts. This gap is being exploited by criminals but also governments to promote fake news shaping public opinion or behavior.

In order to reach the light at end of this tunnel, we need to focus our efforts on promoting digital literacy in society at a broad scale. Part of effectively finding and consuming digital content focuses on how well users can discern facts from misinformation and determine trustworthy sources while understanding risks.

People are aware of cybersecurity because they hear a lot about it. But that doesn't mean that people are behaving how we would like when it comes to matters such as password authentication and social engineering attacks.

Psychologists have studied human perceptions and behavior, how we think and behave and what can influence that. For example, risk perception and the impact an action might influence our behavior. But also:

- Internet users tend to select content that is consistent with their attitudes and opinions and tend to evaluate attitudinally consistent information more favorably
- People are inclined to believe information and sources that others find credible
- People are inclined to believe information based on the reputation or name of a website or resource without much critical scrutiny of that site or content.

Based on these clues, we know that many information seekers avoid more effortful processing of online sources and information.

In order to reach the light at end of this tunnel, we need to focus our efforts on promoting digital literacy in society at a broad scale. Part of effectively finding and consuming digital content focuses on how well users can discern facts from misinformation and determine trustworthy sources while understanding risks.

_ *How can IT technology developers aid cybersecurity efforts? What else must be taken into consideration when aiming to create effective IT solutions?*

Effective IT solutions should be usable. For example, designers and developers often approach web accessibility as a checklist to meet specific standards (e.g., ISO/IEC 40500), and the focus is only on the technical aspects of accessibility. As a result, the human interaction aspect is often lost, and accessibility is not achieved.

Combining accessibility standards and usability processes with real people ensures that web design is technically and functionally usable. Such considerations need to be made for people with different disabilities, but also low literacy, etc. Technology is being developed for people and people are different, therefore we cannot expect the same usability levels of different solutions to work for all.

Enable secure remote workspaces without trashing your entire IT infrastructure

AUTHOR_ Marc Gaffan, CEO, Hysolate

Roughly 12 months ago, when the world shifted seemingly overnight to work-from-home, few companies were well-positioned to seamlessly scale their remote work solutions. Legacy remote desktop solutions, like Virtual Desktop Infrastructure (VDI) and Desktop-as-a-Service (DaaS) were pressed into wider service than they had been custom fit to provide. Security policies governing remote working and secure access were either scaled up or slapped together in an ad hoc fashion to keep operations going, but they often interfered with worker productivity.

Along the way, too many companies struggled in a tug of war between IT freedom for employees and robust security for the company. CIOs, CISOs, and others within executive leadership were right to be concerned: prior to COVID-19, 70 percent of security breaches started at the endpoint. Those responsible for security at companies of all sizes are taking it day by day, waiting and watching to see whether their current security profiles are up to the task of protecting invaluable customer data and company intellectual property.

The problems with unanticipated demand for secure remote work

At the start of the pandemic, many large enterprises had VDI or DaaS solutions in place for a subset of their workforce. Many medium-to-large enterprises did, as well. Even so, as companies tried to scale these remote work solutions overnight, they realized they were ill-prepared:

- Most weren’t ready to enable a wider range of remote worker tasks involving a larger set of corporate assets
- Some had to accommodate a new or broader BYOPC approach
- Most needed to expand remote access to the company’s more sensitive systems and data

- Many feared that current restrictive security policies would limit worker productivity
- Most have had a difficult time easing the increased strain on IT personnel working to support such a rapid and all-encompassing transition

Enterprise leaders that view IT freedom and corporate security as opponents in a zero-sum game are looking at this business challenge through the wrong lens.

According to our own survey of CISOs conducted in Q3 2020 in tandem with Team8, the scramble to "enable remote by any means" prompted a range of responses:

- 35 percent of enterprises relaxed their security policies to expand IT freedom for their employees
- 26 percent went the other way and tightened security policies
- The rest - 39 percent - made no changes, perhaps unsure of exactly what they should do to maximize worker productivity without compromising corporate security.

Employee IT freedom vs. corporate security: The wrong question and a false choice

Figuring out where to draw the line between giving employees IT freedom to browse, download, install and store as needed and asserting security policies that adequately protect assets from the wide range of corporate activities comprising the enterprise workday was anything but obvious. There's a good reason for that: the question isn't "Which should the enterprise favor?" Instead, we should ask ourselves "How do we get both greater freedom and enhanced security at the same time? "

Enterprise leaders that view IT freedom and corporate security as opponents in a zero-sum game are looking at this business challenge through the wrong lens. It is an understandable posture, though, since older methods of securing legacy infrastructure were formulated around the idea that the best way to maintain control over corporate assets was to severely limit what end users could do on their computers. Lock down user activity = maintain security. Loosen end-user restrictions = increase vulnerability.

Rethinking remote working in the cloud era

Fortunately, new technology approaches to remote work have proved the freedom-versus-security way of thinking to be archaic. Advances in isolation technologies, in particular, are helping enterprises scale their remote work operations, broaden the latitude workers have to access digital tools and information, and increase defense of the corporate network, data and other intellectual property.

Many IT administrators are already familiar with web isolation, which allows end users to peruse websites freely in an isolated remote environment, like a virtual machine or a sandbox, that won't allow malicious code to infiltrate the endpoint's browser. The concept of isolation is sound, but the range of tasks that comprise most workers' daily activities extends well beyond web browsing, and managing at scale an incomplete solution like web isolation is very difficult.

Remote workflows have required end users to install video conferencing applications to collaborate with team members. Workers routinely depend on numerous different line-of-business applications. Developers download, install and update various types of software.

Employees frequently rely on peripheral devices like thumb drives to upload, transfer and download files. Cloud applications often offer full

desktop clients that provide superior features and convenience. And the list goes on. If even a subset of the above activities applies, web isolation is going to fall short of what's needed to fully protect corporate assets.

OS-based isolation: Providing the best of both IT freedom AND corporate security

Today, there's a different approach to isolation that extends the protections and benefits of web isolation beyond browsing activity to cover most anything a worker has to do in the course of a normal business day. OS-based isolation creates an instantly provisioned virtual machine on a user's device, establishing a second, entirely separate and pristine environment on the endpoint.

With OS-based isolation, whatever happens inside the VM cannot in any way affect the underlying OS (or vice versa). In this way workers can browse less secure websites, but they also have the freedom to download and experiment with necessary web-based applications and tap into all the commonly used tools and solutions that make work easier, without risking infiltration of malware or exfiltration of business-critical data.

With enterprises now having to enable a broader range of activities in a work-from-home scenario, security leaders would be wise to consider tapping OS-based isolation to establish multiple isolated operating systems on a single endpoint.

Further, OS-based isolation can make VDI or DaaS connections even more secure. Unless an enterprise is enabling VDI or DaaS connections exclusively through thin client endpoints, there's a real risk that a remote worker will access the corporate network from an already-compromised non corporate managed or personally owned laptop or workstation. In this scenario, malware can have direct access to the enterprise's most sensitive assets. But utilizing OS-based isolation in conjunction with one of these legacy remote desktop solutions obviates that threat, allowing unrestricted access to the internet, email and non-privileged information via an "unlocked" OS (which may pick up malware in the course of engaging in these activities), while reserving a second, privileged OS for accessing high-value corporate assets, including sensitive data and other systems, through the VDI or DaaS session.

It's worth noting that OS-based isolation can now (and someday likely will) fully take the place of VDI and DaaS. But with so many enterprises having one or the other of these legacy remote desktop solutions firmly entrenched in their IT stack, it's far more likely that enterprises will choose to "layer on" OS-based isolation atop their VDI or DaaS instantiation to expand worker freedom while improving corporate security, at least until the incumbent remote work solution is due for a refresh.

With enterprises now having to enable a broader range of activities in a work-from-home scenario, security leaders would be wise to consider tapping OS-based isolation to establish multiple isolated operating systems on a single endpoint. With HR, developer, financial, customer service and other call center activities now having to be conducted from workers' kitchen tables or living room couches, reserving a pristine environment for handling such sensitive business has become a mission-critical imperative. And seeing how remote work at scale is very likely here to stay long after the pandemic has faded to nothing more than a bad memory, it's time for enterprises to wake up to the reality that IT freedom and corporate security can perfectly co-exist in the new enterprise remote work toolkit.

During the past year, business leaders have seen first-hand the benefits of adopting an “everywhere enterprise” model of working and are now carefully considering its role in the future of work. A study by Mercer revealed 94% of employers agreed that productivity was the same or higher than pre-pandemic levels, even with employees working remotely in 2020.

IT departments whose approach to cybersecurity even remotely resembles the traditional perimeter will be fighting a losing battle.

Protecting productivity within the disappearing perimeter

AUTHOR_ Nigel Seddon, VP of EMEA West, Ivanti

It is therefore unsurprising that Gartner’s research has found that 90% of HR leaders will allow employees to continue to work remotely in the future. Whilst this may be music to the ears of employees enjoying a better work-life balance, for

many IT staff, alarm bells will be ringing.
In a survey of 1,600 global IT professionals, Ivanti found for 63% of those interviewed, IT workloads increased 37% since remote working began.

So why are IT staff workloads increasing, and how can CISOs relieve some of the pressure without compromising productivity?

The disappearing perimeter

IT departments whose approach to cybersecurity even remotely resembles the traditional perimeter will be fighting a losing battle. Prioritizing on-premise assets in the age of the cloud is outdated. Cloud applications and mobile devices have become essential to the everyday tasks that have kept productivity high during the pandemic crisis and are accessible everywhere.

Zero trust is based on the notion that we must assume bad actors are on our network, no matter which security controls or technologies we have in place.

Additionally, devices have become integral to productivity. 72% of employees agree that their device has been important to ensuring their productivity during lockdowns. As a result, corporate resources are no longer restricted within a physical perimeter that IT departments can monitor and secure. Against a backdrop of increasing cyber threats, and with the rise in the number of on-premise, cloud and edge devices accessing business data, the attack scenarios for IT to bear in mind are innumerable.

As more employees use personal devices and networks to access business applications, the line between business and personal data becomes blurred. If a bad actor penetrates a device through a personal channel, what is to stop them from breaching a business application?

Zero trust

The approach to cybersecurity needs to change to align with the approach to work. When employees left the office, cybercriminals followed. So, if they are working from anywhere, they need to be protected everywhere.

As the device and networks that were once defined become less prominent, IT staff need to assume that anyone trying to gain access to the corporate network is a bad actor.

Zero trust is based on the notion that we must assume bad actors are on our network, no matter which security controls or technologies we have in place. When users log into a network, they should have minimal access to resources until they and the device they are using have been authenticated and authorized.

Coupling this approach with on-device biometrics such as facial recognition creates a stronger standard of authentication. Biometric technology removes the burden and the responsibility for employees to consistently supply strong passwords. This also improves the user experience by unlocking single-sign-on (SSO) capabilities, drastically reducing the number of IT help desk tickets.

When an entire workforce is remote, IT battles routine and novel requests simultaneously and continuously which can overstretch capacity.

Around the clock automation

Knowing what devices employees are using to access corporate data is an important first step

to protecting that data. Having full visibility into all IT assets, therefore, remains a priority for IT departments, but as the number of devices employees are using continues to grow, it is becoming an increasingly impossible task for IT to visualize their full IT environment.

Using IT asset management (ITAM) software with built-in automation to discover what assets employees are using to access business data will provide IT staff with real-time analysis of their software and hardware inventory. This ensures continuous visibility in real-time through active and passive scanning, network scanning and third-party connectors.

What began as a rushed reaction during a crisis has evolved to be the preferred model of work for employees and their bosses.

Automation can also be used to bolster compliance and user productivity, by frequently detecting and solving IT issues before users even notice them. AI-driven mobile threat defence tools constantly monitor application and user behaviour on devices, meaning they can respond in real time when suspicious activity is taking place on the device and protect against potential vulnerabilities.

They are also completely unobtrusive and require no action to be activated from the end-user, meaning employees can go about their work productively, while businesses' IT departments are safe in the knowledge that their devices are operating securely.

Self-service problem management

Service management in the "everywhere enterprise" presents IT teams with yet more issues. When an entire workforce is remote, IT battles routine and novel requests simultaneously and continuously which can overstretch capacity. Ivanti found the most common requests to be VPN issues (74%), video conferencing (56%), bandwidth constraints (48%), password resets (47%) and messaging issues (47%).

Organizations need quick solutions that allow IT support to prioritize risk to effectively distinguish routine tickets from genuine causes of concern. Effective IT service management (ITSM) tools that utilize automation are key to this.

The use of intelligent bots to process inquiries and complaints from employees can contribute towards faster diagnosis and resolution of problems. An issue can then be appropriately escalated if it requires extra attention whilst ensuring end users are communicated with promptly and effectively. With more employees working outside of traditional 9-5 working hours, self-servicing will enable them to troubleshoot after IT has clocked off.

What began as a rushed reaction during a crisis has evolved to be the preferred model of work for employees and their bosses. With the role of IT proving to be essential in enabling productivity, it is crucial that they are not overwhelmed and can continue to assist in innovating business continuity and prosperity. Implementing automation and zero trust allows IT departments to optimize their time more efficiently and productively without compromising quality or security.

Closing the data divide: How to create harmony among data scientists and privacy advocates

AUTHOR_Balaji Ganesan, CEO, Privacera

Balancing data privacy within an organization is no easy task, particularly for data scientists who need quick access to data, and security and governance teams whose job it is to protect it. Too many of our customers have told us they are being inundated with tickets for requesting data access, which is a task that sounds simple and easy to accommodate but, in practice, is not.

In typical cloud data architectures, there is no magic button for IT or data architects to gain instant access to the different data sets that are created by users across the enterprise and often distributed across different cloud services. As our customers will attest, this is a real need that forces organizations to search for a solution that won't compromise data privacy and security requirements.

The real problem in the quest for both data usability and privacy is the difficulty of deploying a scalable compliance solution across multiple cloud services. Migration to the cloud is an unstoppable evolution of data storage, analytics, and reporting. Yet, this plethora of cloud data services creates an untenable nightmare for those looking to keep tabs on — and maintain access control over — the data being created, stored, and shared.

According to Gartner, the world-wide public cloud services market is expected to grow 18.4% in 2021 to total $304.9 billion, up from $257.5 billion in 2020. McKinsey & Company mirrors the statistic, saying they expect about 35 percent of all enterprise workloads to be on the public cloud by 2021, and anticipate 40 percent of companies will use two or more infrastructure-as-a-service (IaaS) and software-as-a-service (SaaS) providers.

With the escalating scrutiny of regulatory authorities around the world moving towards increased control of personally identifiable

information (PII) data, enterprises must embark on a journey that not only migrates data to the cloud but also satisfies the privacy and security requirements outlined by data governance teams and chief security officers.

The longevity of a data access control solution's success often lies in its ability to scale due in part to the sheer volume of data migrating to the cloud.

Clearing a path to fast, scalable data privacy

In order to effectively leverage and protect all data assets, careful consideration must be made to ensure data privacy and security policies are implemented in a consistent manner across the enterprise. This is because, regardless of the infrastructure, the same regulations apply to the data itself. For example, social security numbers cannot be divulged, only specific portions of a credit card number can be displayed, and names/addresses of customers cannot be conjoined in a way that would allow unscrupulous hackers to easily steal someone's identity.

Unfortunately, IT and security teams are often left with a piecemeal approach that straddles different methods and user interfaces to implement data security and compliance policies across the myriad of cloud services. Keep in mind, the speed at which an organization deploys a data access control solution is important; however, a fast rollout must never exceed its ability to handle petabytes of data. A rollout that is quick yet stops working once there is too much data is a futile and often expensive effort to correct.

The longevity of a data access control solution's success often lies in its ability to scale due in part to the sheer volume of data migrating to the cloud.

Intuitive and visually appealing user interfaces are equally needed aspects of a complete solution.

When it comes to selecting a data access control solution to manage the privacy of customer account data - payment card and healthcare data, social security numbers, membership points, credit scores, and bank account info — IT and security teams must ask themselves how much risk is acceptable. For instance, a solution that works in pilot projects may not work as effectively in production scale environments.

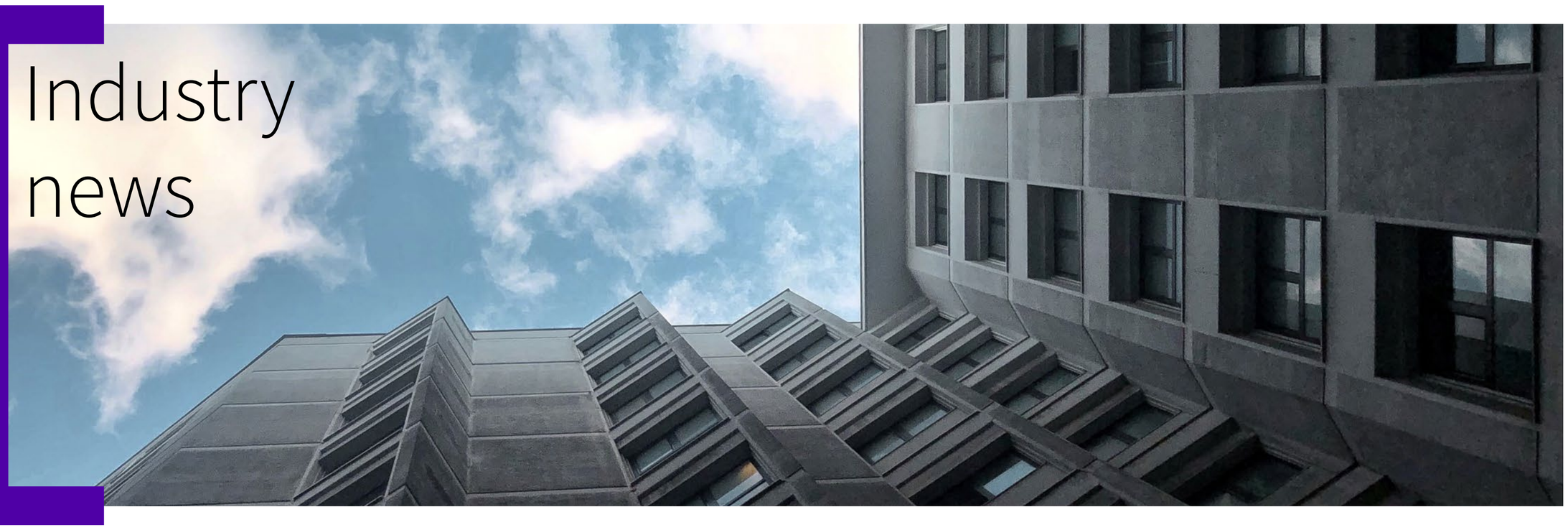
To ensure success at the onset, here are some key questions to ask when selecting a data access control solution include:

- How long does it take to deploy across all cloud services?
- What deployment options are available? Any limitations on future usability?
- Does the performance of the solution change based on data volume?
- Can all data types be secured by the solution?
- Once implemented, are data scientists able to execute queries of data at performance expectations?

The key to closing the data divide lies in adequate planning and verification of a solution's capabilities as data teams need access to information in a timely manner. They also need to run queries without performance limitations from the data privacy and security solution itself.

Failure to manage the needs of data scientists with those in charge of data privacy and security can prohibit the organization from uncovering "the next best decision" or from gaining long-term benefits due to a lack of scalability.

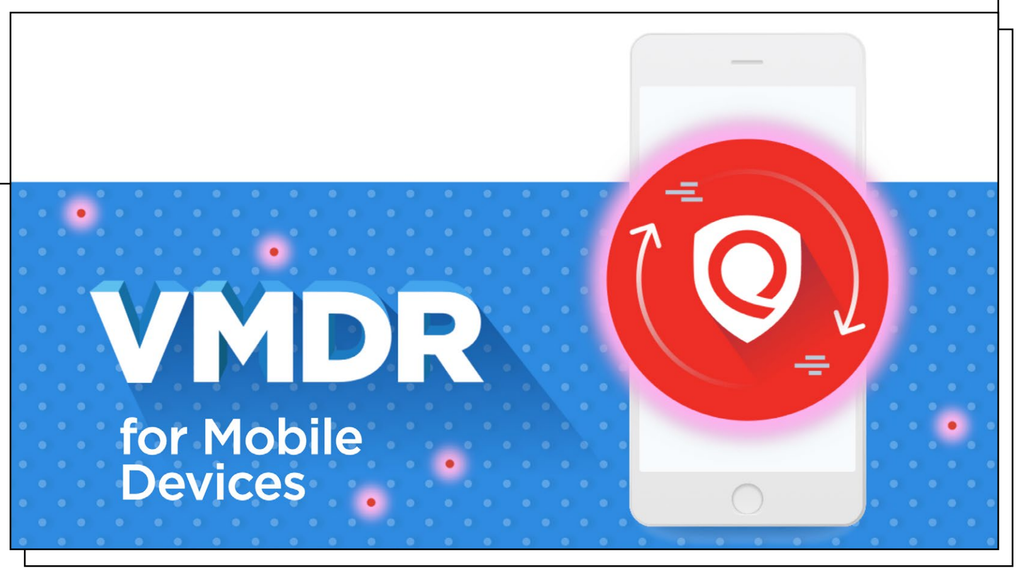
Industry news



Qualys expands VMDR to mobile devices with support for Android and iOS/iPadOS

Qualys announced it is expanding Qualys VMDR (Vulnerability Management, Detection and Response) to mobile devices with support for Android and iOS/iPadOS delivering an end-to-end solution for mobile device security.

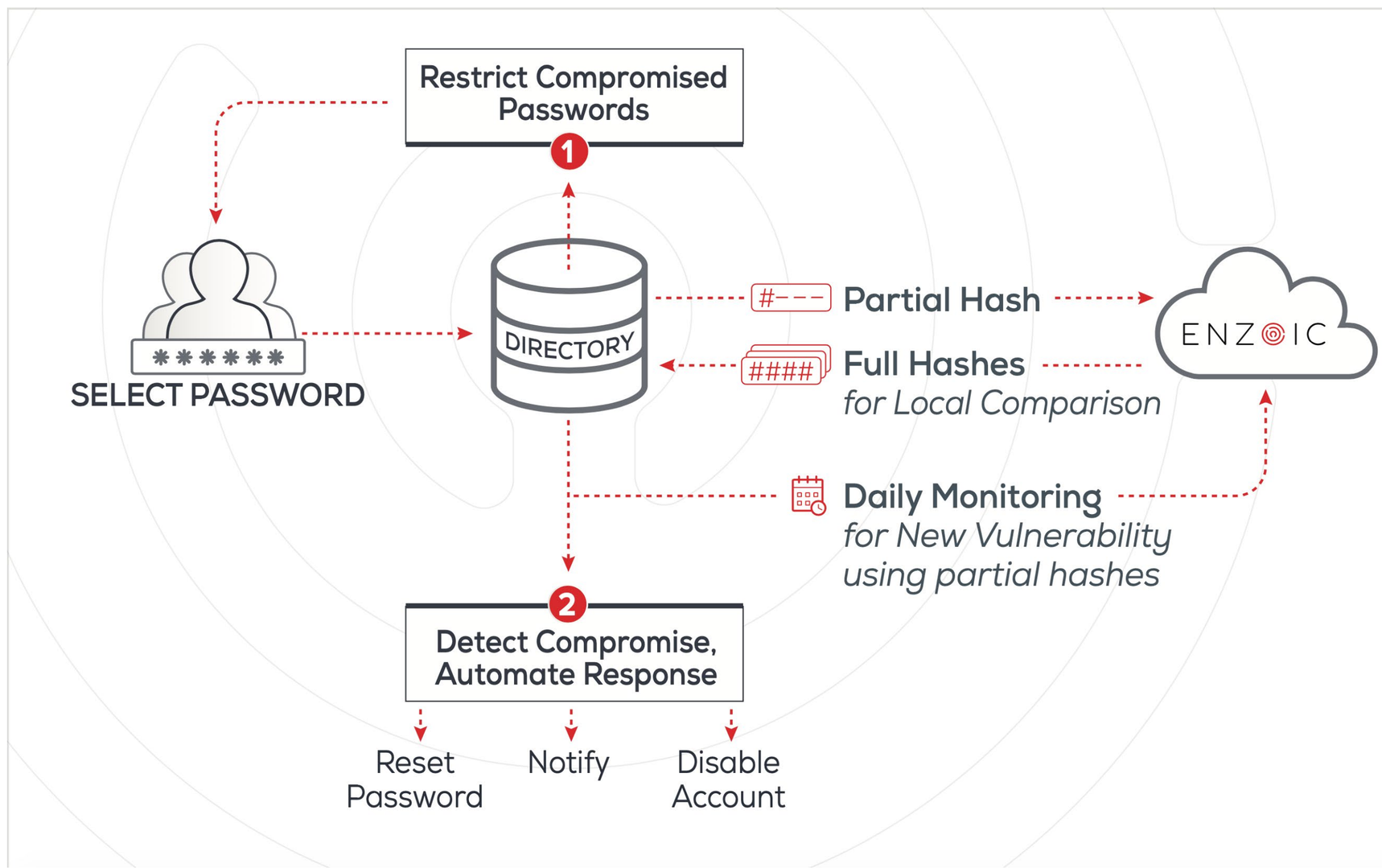
Qualys' all-in-one VMDR provides in-depth mobile device visibility, data security insights, proactive posture monitoring, and automated response for all iOS and Android devices and installed apps – just like VMDR does for on premises, endpoints, clouds, containers, OT and IoT assets.



CircleCI announces privacy enhancements for engineering teams

With a new single, centralized interface for CircleCI private orbs help developers automate repeated processes with reusable packages of YAML configuration. These open-source config packages speed up project setup for users and have integrations for a variety of use-cases, from vulnerability scanning to test coverage of applications.

To further assist teams with their delivery to production, CircleCI now provides developers with the ability to create private orbs, allowing teams to share configuration exclusively within their organization. All available private orbs will be easily accessible for developers across the same organization via CircleCI's command-line interface (CLI).



Enzoic for Active Directory updates help organizations prevent use of compromised credentials

The latest release of Enzoic for Active Directory raises the bar for compromised credentials protection in corporate environments. With Enzoic's new initial scan option, the organization's passwords can be comprehensively checked for compromise immediately after installation.

Users with compromised passwords can then be optionally prompted for a reset at the next login. Within just a few minutes, organizations can now identify and remediate any weak or compromised passwords in their systems.

After this initial check, user passwords are then monitored continuously for future exposure in data breaches or phishing attacks.

SentinelOne acquires Scalyr to deliver XDR platform for realtime threat mitigation across enterprise and cloud

SentinelOne announced the acquisition of Scalyr. With this acquisition, SentinelOne will be able to ingest, correlate, search, and action data from any source, delivering the industry's most advanced integrated XDR platform for real-time threat mitigation across the enterprise and cloud.

Through this acquisition, SentinelOne sets the bar for the XDR market and solves one of the biggest challenges in delivering a fully integrated XDR platform: ingesting and actioning all operational data in real-time from a security-first perspective.

WatchGuard Cloud: Delivering simplified security management for MSPs

With a new single, centralized interface for delivering and managing network security, advanced threat detection, MFA (Multi-Factor Authentication), and more, MSPs will benefit from simplified client management while enabling rapid, efficient and profitable growth.

The latest version incorporates WatchGuard's ThreatSync features, advanced Firebox policy management capabilities and authentication policies that enable zero trust.

MSPs can create policy templates for easy, repeatable security deployments across many subscriber accounts. The platform makes it simple to manage and report on Firebox security environments and AuthPoint MFA deployments from a single pane of glass, while its intuitive interface helps MSPs minimize arduous administrative tasks and maximize productivity and profitability.

Kaspersky And Waterfall Security Solutions announce partnership to secure industrial networks

Kaspersky and Waterfall Security Solutions have partnered to enable additional levels of security for safe, state of the art analysis of industrial control system network traffic for anomalous and suspicious activities. The joint solution provides non-intrusive industrial network traffic inspection and deep packet inspection, while providing industrial networks with hardware-enforced unidirectional protection for safe and reliable operations.

RSA NetWitness Detect AI provides advanced analytics for actionable threat detection

RSA NetWitness Detect AI applies cloud-scale processing for behavior analytics and uses unsupervised machine-learning to detect and respond to threats without manual oversight.

The all-new SaaS solution provides high-fidelity, actionable insights on data captured by the RSA NetWitness Platform that empowers security teams to find, prioritize, and resolve threats faster and more efficiently.

ShiftLeft Illuminate reduces risk to organizations' software code base

ShiftLeft Illuminate leverages ShiftLeft technology to identify insider attacks, offer remediation advice and reduce overall risk to organizations' software code base. While cyberattacks on the CI/CD pipeline have been theoretical for some time, high-profile breaches over the past year have underscored a clear and urgent need for attention to this area.

ShiftLeft Illuminate will help organizations eliminate insider threats within this vulnerable phase of the development pipeline.

CrowdStrike acquires Humio to expend its XDR capabilities

CrowdStrike announced it has agreed to acquire Humio. Under the terms of the agreement, CrowdStrike will pay approximately $400 million to acquire Humio, subject to adjustments.

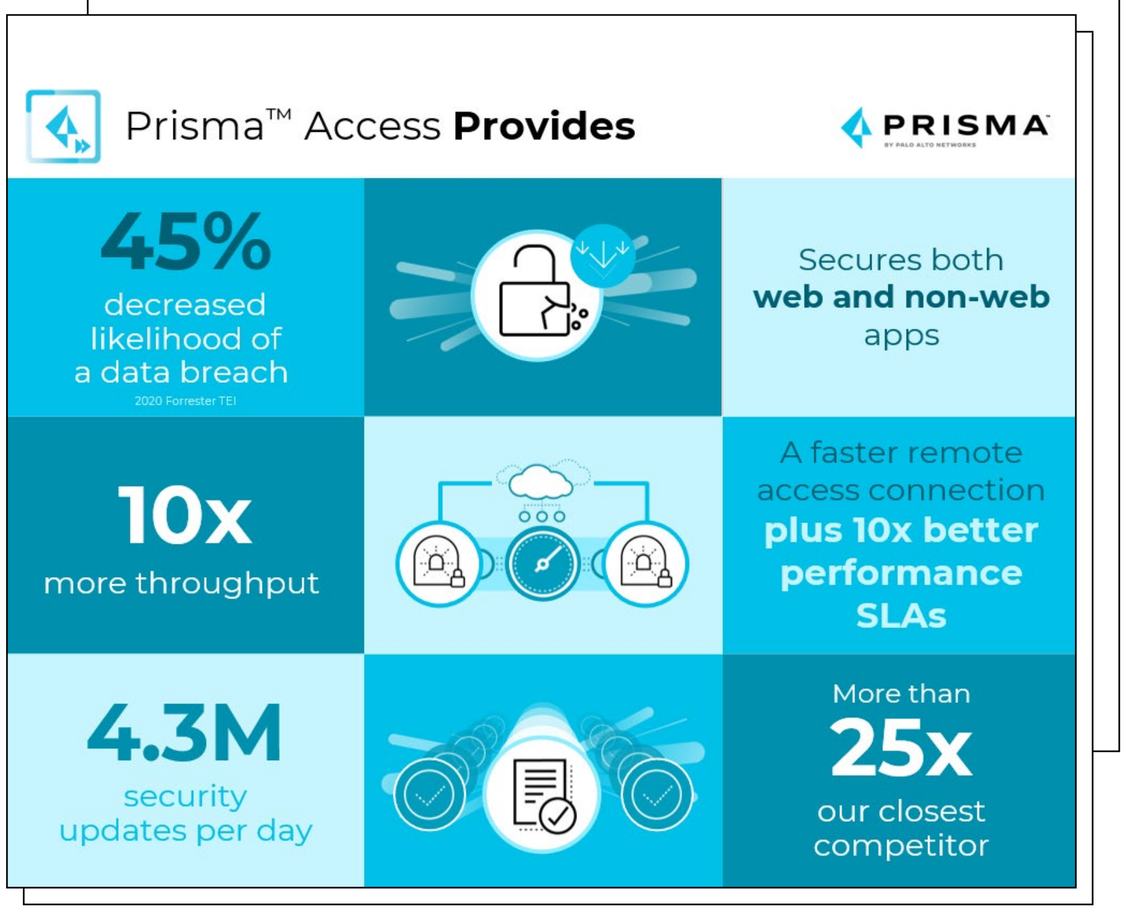
The acquisition is expected to close during CrowdStrike's fiscal first quarter, subject to customary closing conditions.

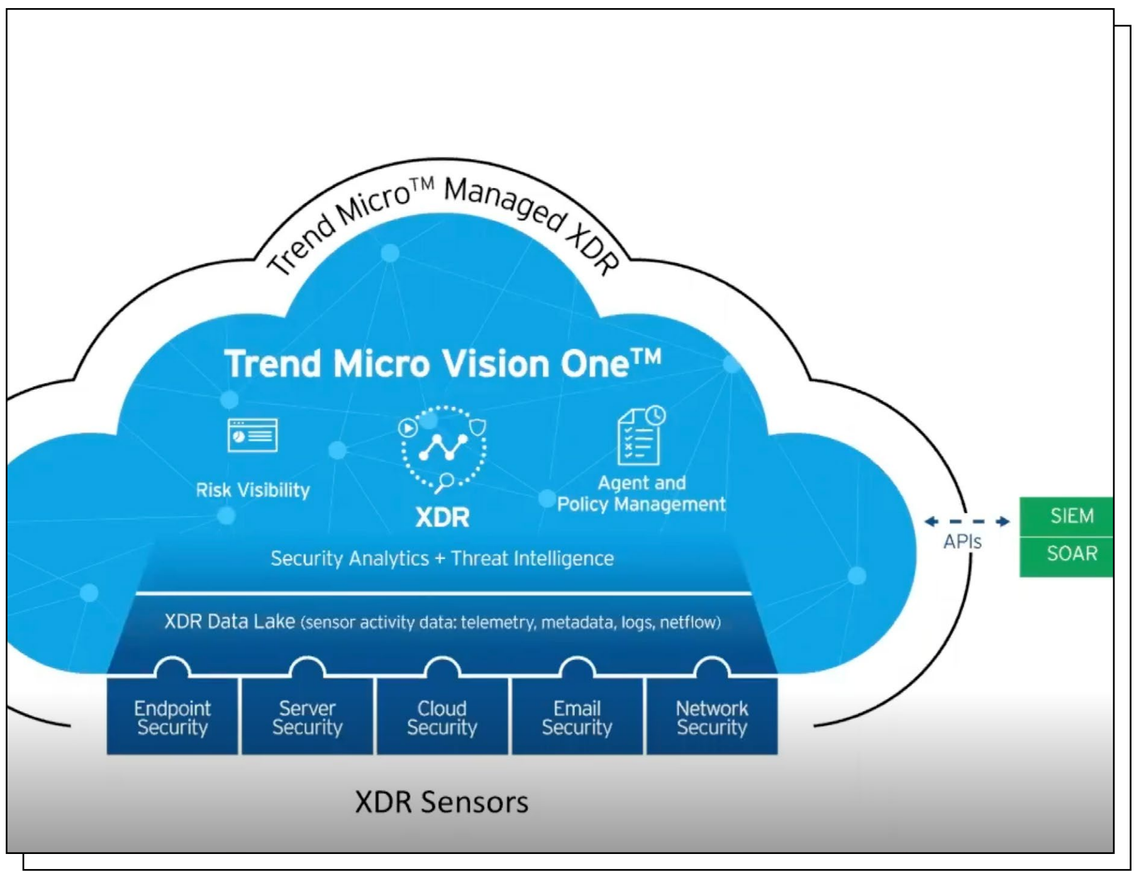
With this acquisition, CrowdStrike will further expand its eXtended Detection and Response (XDR) capabilities by ingesting and correlating data from any log, application or feed to deliver actionable insights and real-time protection.

Palo Alto Networks Prisma Access 2.0 securely enables work-from-anywhere

As work continues to change and needs to be done securely everywhere, with no compromise on speed, security or performance, Prisma Access 2.0 introduces critical enhancements, including self-healing infrastructure for optimal experience, ML-powered security to help prevent attacks in real time, cloud SWG capabilities for a secure web gateway regardless of user location, and a reimagined cloud management experience.

The Prisma Access 2.0 release provides 10 times more throughput than other solutions for a faster remote access connection and 4.3 million security updates per day — about 25 times more than the closest competitor — to help organizations rest assured their users and data are secure.



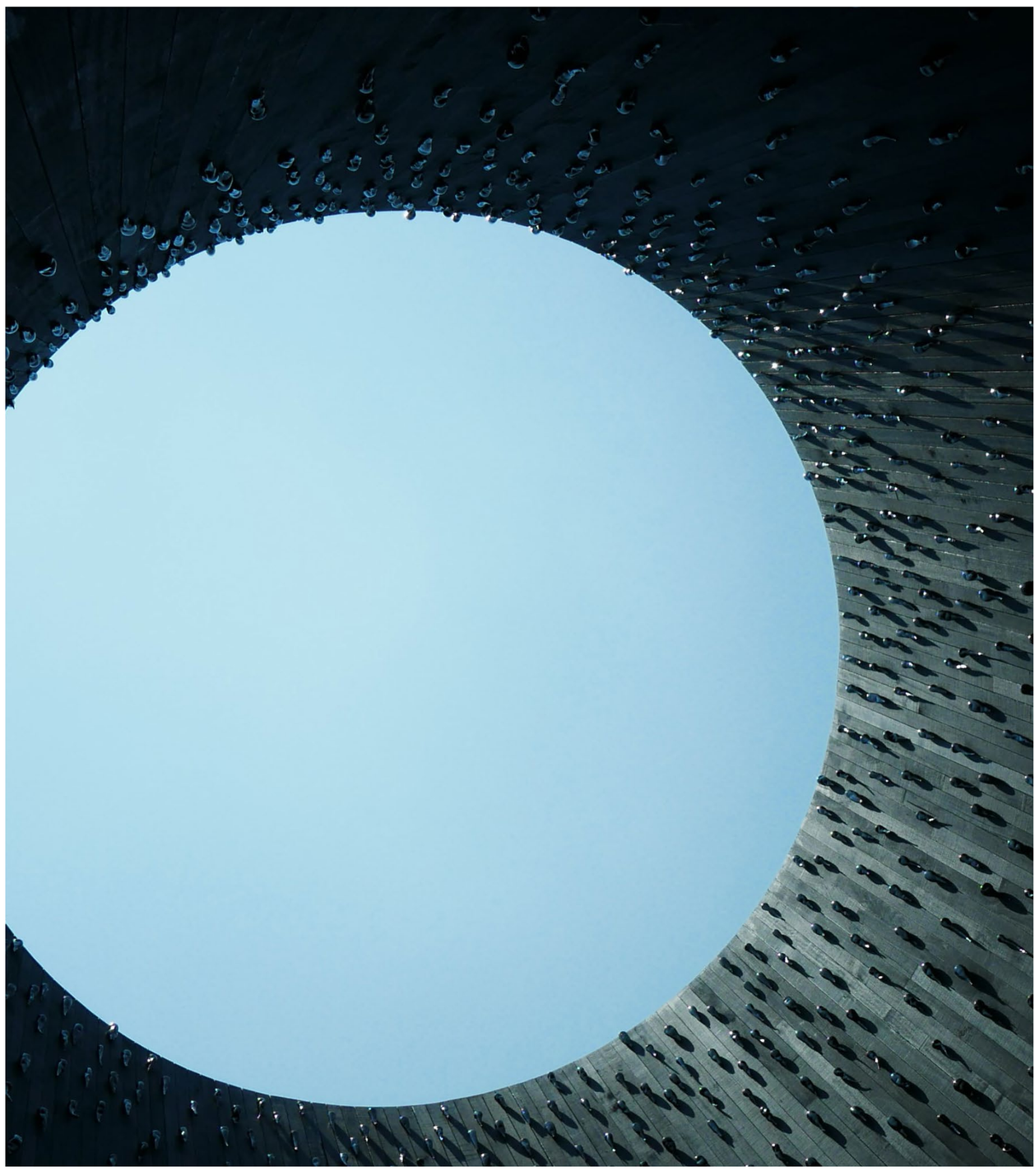


Trend Micro Vision One: Extended XDR to help security teams see more and respond faster

Trend Micro combats security alert overload and resource constraints with an extensible platform that provides visibility and response from a single console.

The new platform, Trend Micro Vision One, has extended detection and response (XDR) at its core and raises the bar with new capabilities to help security teams to see more and respond faster.

Organizations are struggling with siloed tools, disjointed alerts and stealthy, sophisticated threats, whether they have a Security Operations Center (SOCs) or are relying on stretched IT security teams for SOC functions.



Database encryption: Protecting the crown jewels

AUTHOR_ Nigel Thorpe, Technical Director, SecureAge Technology

Databases are the lifeblood store of information for every organization. Without them, the organization's efficiency, productivity and scope to prosper would be curtailed severely.

Protecting the company crown jewels is something that most organizations take seriously, using network security, robust authentication and access controls within their toolsets.

The main problem is that you are just one IT security manager faced with thousands of potential attacks. Sooner or later, someone will try to gain access to your databases and steal the data contained in them. IT security measures plug gaps we know about, but cybercriminals are very clever, very lucky or very manipulative – often all three. They mount many attacks in the sure knowledge that at least one will succeed. Just look at organizations like FireEye and Malwarebytes. If they can be breached, how can a less cyber security-savvy organization cope?

If you're facing a disgruntled employee inside the finance department, they can access sensitive data because it's part of their job.

Potential data theft scenarios

Let's assume that your organization has been hacked. First and foremost: what was the cybercriminal looking for? Any data they can use as a ransom or which they can sell - or both? This could be data currently inside a database, but many users will also have reports, documents and presentations containing information they extracted from the database. These are nice, easy targets.

Let's say you happen to be a government organization running a virus track-and-trace system and you might store everything in a spreadsheet.

Let's also assume that there is a cybercriminal who has compromised your defenses and is snooping around the network looking for anything of value. Or maybe this is a member of staff, already inside the network, feeling malicious or just nosey.

If you're facing a disgruntled employee inside the finance department, they can access sensitive data because it's part of their job. For them, information theft is simple – they just log in to the database and extract all the staff records and corporate finances onto a USB stick and away they go. The same could be true if an external hacker managed to compromise a user account through phishing or social engineering.

The case of the administrator or the hacker are likely to be similar to each other. They can both exfiltrate documents, reports and spreadsheets which users have created. But they can also copy the entire database - including files that contain many of the corporate crown jewels.

Finally, the administrator as the authorized user holds the keys for the backups, so can steal a whole backup that contains not only database files but also all the ad-hoc documents created by users.

Types of database encryption

There are a variety of technologies for database encryption.

Transparent Data Encryption (TDE), usually provided as an option from the database vendor, is commonly used. This encrypts data so that, in the event that the database files themselves are stolen, the information remains secure. With no impact on the way the database works and with no need to change the application, this is an attractive option.

Another option is Column Level Encryption (CLE) which encrypts specific data fields. CLE offers stronger protection from within the running application but requires manual setup in the database and application software changes. Again, the cybercriminal or administrator thief is foiled by this kind of security.

Data masking is a further technology that is aimed at hiding sensitive information from database authorized users. For example, rather than showing the entire credit card number to the call center operator, data masking could hide all but the last four digits. This technology conceals data from application users when they have no need to see it. However, the information stored in the database is not secured.

There are, however, problems with these approaches. Our first challenge is that TDE and CLE are specific to the database technology vendor. In a perfect world this would be fine. But in real life, organizations grow over time, through acquisition and because of changes in technology direction. This leads to an infrastructure consisting of multiple vendors' technologies.

To encrypt all your databases, you now have to purchase, deploy, manage and maintain multiple different database security products. Not a great situation.

In addition to that, there are reports, spreadsheets, documents, logs and temporary files scattered all over the organization, unprotected from disillusioned employees and determined hackers.

> *The problem with only encrypting the most sensitive data is that it's difficult to pinpoint exactly and reliably what "sensitive data" really is.*

Since we're assuming that the cybercriminal has already gained access to the network, endpoints and servers, this is an alarming situation.

Focus on the data

At the end of the day, we're trying to protect information. If you can organize your infrastructure in such a way that, when data gets stolen, it's in a form that is complete garbage to the thief, then the information remains protected even though it's in the wrong hands.

> *A single security solution is not able to fill all security gaps, and even if they were able, I would suggest avoiding that approach.*

Enter data encryption. More specifically: file-level encryption. Data encryption traditionally gets a bad rap as it's seen as something complex, expensive and scary, so we tend to toy with it rather than embrace it. For example, full disk encryption is easy – we leave it up to the OS vendor and just forget about it. The catch is that full disk encryption doesn't actually stop anyone stealing data from a live system. And TDE for databases is fit-and-forget too – but all it does is to create another security silo outside of which data becomes unprotected.

File-level encryption seems to be treated as something dangerous; something a bit edgy that needs to be applied with care only to the most sensitive information. Which is odd, since modern file-level encryption can – and in my opinion – should be applied universally.

The problem with only encrypting the most sensitive data is that it's difficult to pinpoint exactly and reliably what "sensitive data" really is. And, most importantly, where it is. I've already pointed out that people will run reports, write documents and manipulate potentially sensitive information in spreadsheets. And people do what's easy – not necessarily what the IT department expects them to do. It might be company policy to store all documents on the user's "P:" drive, but maybe it's easier to store them locally – especially if the individual is just playing around with some numbers.

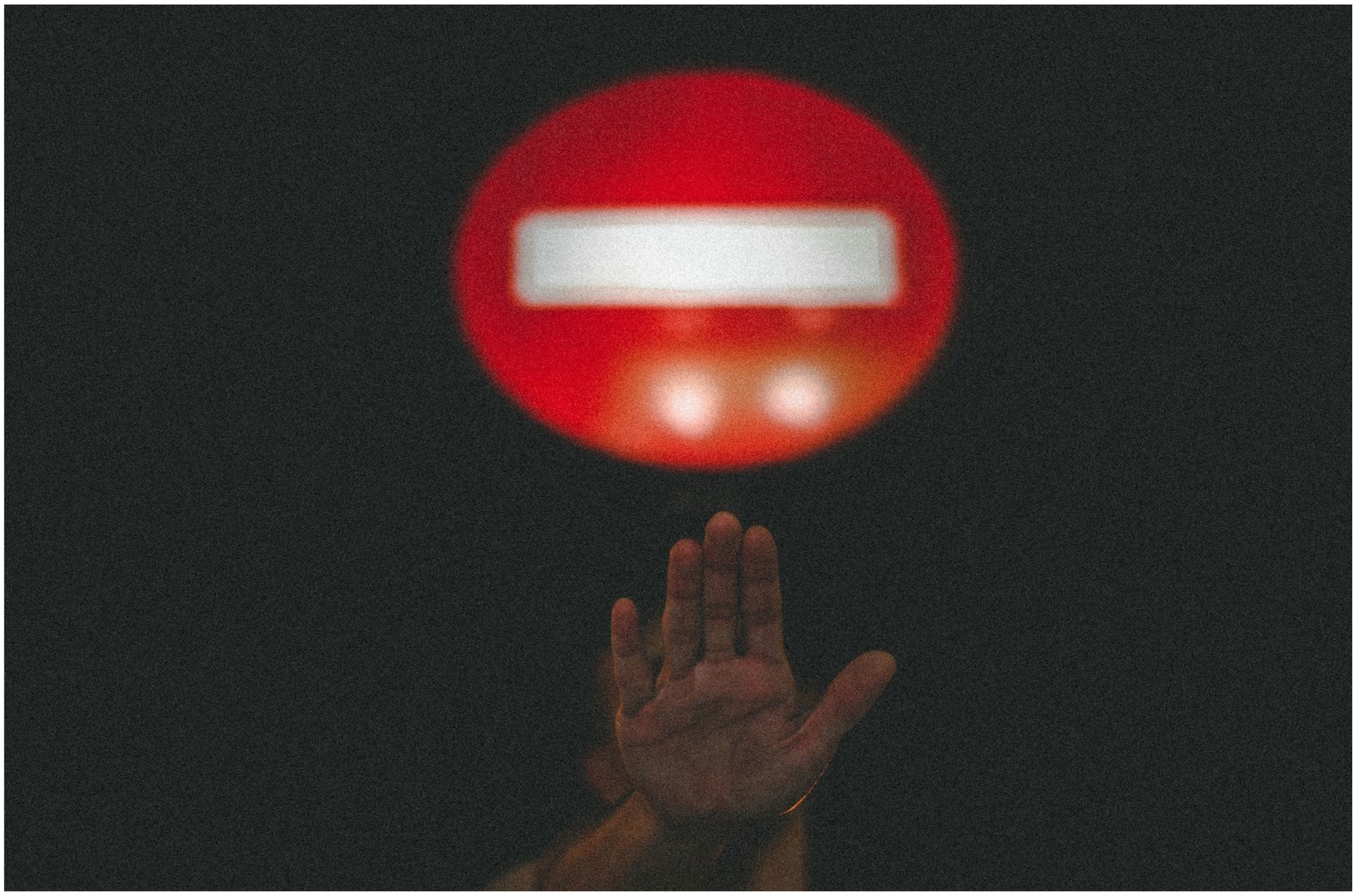
The great thing with file-level encryption is that it works for databases, too. Databases, under the covers, are just a bunch of files, so if we just encrypt all the underlying files then the entire database is naturally secure against both our hacker and the rogue admin stealing them. So now we have a single piece of security technology that works not only across all vendors' databases, but also across all unstructured, report, temporary and log files.

This approach offers comprehensive protection without changing any software. And any misconfigured storage that's open to the internet now contains only encrypted data. We don't actually want anyone to get in and steal them, but regardless, they're useless to an outsider. Even the rogue administrator or finance executive can only steal encrypted data.

Mix-and-match is good

A single security solution is not able to fill all security gaps, and even if they were able, I would suggest avoiding that approach. Why make life easy for a cybercriminal? Using a carefully selected suite of tools is a superior method of securing networks and data, placing lots of roadblocks in front of hackers.

It doesn't matter if information is stored in a database, a Word document, a presentation or a spreadsheet. By accepting that data breaches will happen it becomes apparent that building security into the data is the only approach that ensures persistent information protection.



Can we put a stop to cyber harassment?

AUTHOR_Zeljka Zorz, Managing Editor, (IN)SECURE Magazine

Cyber harassment via social networks, media, and other online channels is an everyday reality for too many people, and the problem is getting worse.

It might seem inevitable, as people are spending more and more time online, but Matthieu Boutard, Managing Director at Bodyguard, a French technology start-up that protects users against cyber-bullying, hate speech and toxic content online, believes that to understand what is fueling the rise of cyber harassment, we should look at the current social and economic context.

> *There is a very thin line between harassment and cyber harassment.*

"The Covid-19 pandemic's social restrictions, repeated lockdowns, travel and movement limitations have led to isolation, job loss, increased

stress, and anxiety in people. These have, in turn, led to high levels of frustration, as well as a stronger tendency to react in the wrong way (e.g., be more aggressive or hurtful towards others)," he told (IN) SECURE Magazine.

"The second point worth considering is the evolution of internet culture. Users did not act like this when the internet first came around but, gradually, toxic content started to appear: first a hurtful comment here and there, then more and more hateful comments as people saw that posting toxic comments is not 'punished' by platforms. From there, things kind of spiraled out of control."

In this interview, Boutard talks about the issue of cyber harassment and the challenges of blocking/preventing it.

[Answers have been edited for clarity.]

_ ***Cyber harassment does not happen only through social networks. What other online/electronic mediums are abused by harassers?***

There is a very thin line between harassment and cyber harassment. Back in the day, you could physically "walk away" from your harassers. Now, however, harassers can reach you via a multitude of online channels, and they are getting very creative in finding new ways to reach you.

In some cases, harassers who were not able to reach their victims through usual channels found ways to get through to their victims' networks – for example, sending personal information on geo-localized platforms based on the victim's location.

+

People need the ability to determine what bothers them personally and what their community is sensitive to.

We've seen cyber harassment nowadays affecting even sites such as Vinted (an online marketplace for secondhand clothing) and LinkedIn. Basically, where there is the possibility for a communication exchange, harassers will use it to harass their targets, even on platforms which are not primarily designed for socializing.

_ ***What are the various challenges when it comes to detecting cyber harassment on a large scale on social media?***

In order to have the desired effect (i.e., protect people), cyber harassment detection on social media needs to be preventive and to take place in real-time. It needs to work even for live streaming, for any large volume of content being posted at the same time or continuously.

This is difficult for social media as it was traditionally built around human moderation. The danger is that when you take too long to remove a comment, the damage has already been done, as it has already reached the person or the people it intended to harm.

Another challenge is the fact that people have different sensitivities and moderation needs: what will hurt me could leave you completely unaffected, and vice versa. Because of this, a one-size-fits-all approach does not work. People need the ability to determine what bothers them personally and what their community is sensitive to.

_ ***Some people's livelihood is very dependent on using social networks and media, so they can't stop using them even if the cyber abuse they are experiencing takes a toll. Your apps come between the target and their harasser and prevent the harassing messages from being delivered. What's the feedback from your customers?***

You are completely right – we've seen so many cases where people need to use the Internet as part of their daily work, but just know that they need to brace themselves for the wave of toxic comments coming their way. And this is the main reason why Bodyguard exists – to allow people to focus on their work, without having to dread each time they open their notifications.

Creating a technology capable of detecting context and nuances, as well as relationships between people, has been an interesting challenge.

Many of our users feel a great sense of relief as they can now focus on doing what they set out to do in the first place: create content and have meaningful exchanges with their community. We've noticed that some users create more content after starting to use Bodyguard.

As for the harassers, some just give up as there is no reaction from their victims (who don't see the toxic comments). Others stop because they realize that their comments are monitored and worry that legal action could be taken against them.

_ ***If you've succeeded in creating a solution for blocking harassing messages, it seems logical that social networks, media, streaming and gaming platforms should have succeeded, too. In your opinion or to your knowledge, why haven't they created or implemented similar tools themselves?***

Lots of social networks and Big Tech use tools that focus on the technological aspect (i.e., machine learning) rather than the social aspect. They keep trying to enhance their ML models, but the improvement is slow and still not quite there yet in terms of being able to offer a fine-tuned moderation. They do a good job moderating things like racism, homophobia, and detecting widely used toxic keywords, but when it comes to toxic content that is more nuanced, they often fail.

Creating a technology capable of detecting context and nuances, as well as relationships between people, has been an interesting challenge. We also needed to ensure that we are able to include the latest toxic content trends as soon as they appear. If you wait before adding new toxic terms to your moderation solution, you will experience a critical delay where you have failed at protecting people against those terms.

Compared to machine learning, where the algorithm needs lots of data and time to "learn" what to do, we have a team of Natural Language Processing (NLP) specialists who monitor social media and all the latest toxic content trends to make sure we detect everything as soon as it appears.

_ ***Which platforms and which languages you aim to support in the next 1-3 years?***

We released our business moderation solution recently and have seen a high interest in it, with lots of platforms being aware that they need moderation, and willing to invest in it to solve this problem. Businesses can used out technology with any platform, network, community, or app via an API.

In terms of our solution for individuals, that's available for now on Twitter, YouTube Instagram, and Twitch. We would love to extend the solution to other platforms such as TikTok in the future but are limited by these platforms' APIs, which don't allow us to access the data in order to protect their users.

At the moment our technology can protect people in English, French and Italian. We're working on adding Spanish and Portuguese in the short term, and then we'd love to focus on expanding into the Asian market.

_ What's your opinion on the effectiveness of current laws against cyber harassment (in France and the U.S.)?

In France there are actually no laws specifically targeting cyber harassment. We're dealing with pre-internet laws which are missing out on a lot of the current context. When you go to court as a victim, it's a very long and difficult process to win. For example, the first time a cyber harasser was sentenced to prison was 2 months ago. There was a possibility for a new law in France, the "Avia Law," which didn't go very far due to political tensions surrounding freedom of expression.

In Europe, there are new discussions around the Digital Services Act (DSA), which aims to focus on ensuring a safe and accountable online environment. I personally think this is a move in the right direction, but we'll have to wait and see how it evolves.

As far as the U.S. is concerned, I would say that the majority of Americans can see that cyberbullying, cyber harassment, and cyberstalking are real problems that are difficult to solve. This is evidenced by the growing number of states either introducing new cyber harassment legislation or altering existing statutes to include online activity for traditional crimes (usually stalking and harassment).

More and more of the states in America are starting to criminalize cyber harassment but finding consistent and fair consequences remains a tricky situation. I think the intent is clear that the legislation introduced has a secondary purpose of wanting to penalize perpetrators of these cyber crimes, but the primary objective is to try and stop cyber harassment. Research-informed and -defined sections of punitive codes based on the varying instances and severities of cyber cases will go a long way in helping these legislations better achieve these goals.

Preparing for the CMMC onslaught

AUTHOR_ Brian Hajost, President & CEO, SteelCloud

For the Defense Industrial Base (DIB), the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) compliance requirement is the hot news topic of 2021. In fact, across the DIB market, CMMC compliance will probably stay a focus through at least 2025.

However, for the long term, many organizations are looking to understand the potential impact that CMMC will have outside the DIB. On January 21, the DoD's CISO subtly announced that her agency is working with the Department of Homeland Security (DHS) to implement CMMC in their contracts. In other words, companies that contract with other agencies are starting to ask, "How do I get compliant efficiently and cost-effectively?" The answer should include looking to NIST 800-170, hardening their systems, and automating STIG compliance.

> *The time, effort, and money spent on creating CMMC mean that other agencies that need to secure their supply chain can achieve a faster and better return on investment using what's already done.*

Why are agencies jumping on CMMC?

The short story is that CMMC offers the first federal compliance requirement that looks to create clear cybersecurity standards.

The real story is a little longer.

Any company that contracts with the DoD, or any federal agency, needs to meet various compliance requirements already. There's ITAR, DFARS, FAR, NIST 800-171, NIST 800-53, NIST Cybersecurity Framework (CSF), and CERT Resilience Management Model. Cross-mapping all of these compliance standards is time-consuming, tedious, costly, and challenging.

CMMC pulls from all of these, creating a single set of requirements that every DIB member can use to prove its cybersecurity posture.

Outside the DIB, cloud computing companies that want to work with agencies need to get FedRAMP approval. Again, this is another time-consuming, tedious, costly, and challenging compliance requirement. Also, FedRAMP pulls a lot of its compliance requirements from the same standards CMMC uses. Further, in August 2020, the Pentagon said that FedRAMP certified organizations will receive reciprocal authorization for CMMC. Although not formalized yet, the need to reduce duplicative compliance activities and their associated costs make sense.

When complying with checklists, organizations often document their reviews, exceptions, and updates. This documentation acts as an audit trail.

The time, effort, and money spent on creating CMMC mean that other agencies that need to secure their supply chain can achieve a faster and better return on investment using what's already done. After all, as the old saying goes: "If it ain't broke, don't fix it." Then again, at this point, no one knows whether CMMC is broken or not.

What does this mean for companies working with other agencies?

Despite jokes about bureaucratic red tape, the reality is that most agencies lack the resources and funding necessary to control their supply chains adequately. This pain point drives CMMC's requirement that primes monitor their subs and that those subs monitor their subs. This flow down may not be new to companies already meeting other privacy or security compliance mandates, like the European Union General Data Protection Regulation (GDPR) or the New York Department of Financial Services (NY DFS) Cybersecurity Rule. For organizations working directly with agencies, this responsibility model may be concerning.

Fundamentally, this model creates two new requirements. Companies need to step up their own cybersecurity maturity, but they also need to get their supply chain to mature its cybersecurity. Supply chain management can impact a company's ability to meet its contractual obligations.

First, the company that falls within these requirements needs to mature its cybersecurity. Conversations within the DIB supply chain already estimate a total industry cost of $6.5 billion to get compliant. Now, any company that works with an agency that contracts with the DoD will need to apply the same compliance requirements. Companies with DHS contracts that apply to the contracts DHS has with the DoD create an entirely new supply chain that needs to accelerate their cybersecurity maturity. As of yet, no one knows how many suppliers this involves. However, now is the time to start figuring that out.

Second, companies need to find solutions that help them monitor their subcontractors. If a subcontractor fails to meet the appropriate CMMC Level compliance, then the company can no longer maintain that relationship. Consider this scenario: Company A makes software that requires Subcontractor 1's services. Subcontractor 1 fails to meet CMMC compliance requirements. Company A needs to replace Subcontractor 1 and find a compliant subcontractor. Until Company A finds that new, compliant subcontractor, it can no longer bid on contracts.

The biggest problem CMMC causes for organizations contracting with government agencies who look to adopt CMMC as a common cybersecurity maturity standard is their supply stream.

Gain visibility and get compliant

One way organizations can get themselves compliant faster is to automate Security Technical Implementation Guide (STIG) compliance. The cross-references and cross-mapping in CMMC lead back to NIST 800-128, ultimately giving organizations a faster way to get compliant.

Getting to STIGs

After mapping out the references between all of the different NIST requirements, the interconnectedness looks like this:

- CMMC makes hundreds of references to NIST 800-171. NIST 800-171 makes 7 references to NIST 800-128.
- CMMC makes hundreds of references to NIST 800-53. NIST 800-53 makes 76 references to NIST 800-128.
- NIST 800-128 makes 5 references to the CMMC Assessment Guide for Level 3 compliance
- NIST 800-128 leads directly to NIST 800-70

What really stands out for organizations that need to get compliant quickly are the references that NIST 800-128 and NIST 800-70 make to STIGs:

- NIST 800-128 makes 9 references to STIGs
- NIST 800-70 makes 4 references to STIGs

Leveraging STIGs for CMMC Compliance

NIST 800-70 “National Checklist Program for IT Products - Guidelines for Checklist Users and Developers” explains that security configurations checklists provide a series of instructions for hardening or benchmarking IT product configurations. NIST specifies STIGs as one of the approved checklists.

Organizations use checklists to enhance their security posture which ultimately leads to enhancing their cybersecurity maturity. Another way they use checklists is to prove governance over their security posture. When complying with checklists, organizations often document their reviews, exceptions, and updates. This documentation acts as an audit trail.

Functionally, DIB members and others that need to meet CMMC compliance requirements can leverage STIGs as a way to accelerate their NIST 800-171 and 800-53 strategies. When setting up their STIGs, many companies find that compliance can break their systems, keeping them from functioning. Also, the STIGs are updated every 90 days. Getting STIG compliant might get the company secure, but it comes with costs such as productivity loss from downtime or operational costs from manually updating.

Automating STIGS: Get CMMC compliant faster and for less

Automation gives companies a way to make STIGs a value add. The checklists are considered best practices for securing data, and their connection to CMMC shows that documenting STIG compliance can streamline the process. Also, when automating STIGs with the right technology, organizations create an audit trail that reduces compliance costs.

CMMC is here to stay, and with it, DIB members need to get ready as fast as possible. Non-DIM members must start watching the signals coming from the DoD and other agencies. As the DoD applies CMMC to its contracts with other agencies, those agencies will likely begin to start implementing CMMC within their own supply chains. At the end of the day, the goal for organizations that want to bid on US federal agency contracts at any level should be looking to get compliant sooner rather than later and in a cost-effective way.

Tools for analytics and automation are providing today's SOC teams with enhanced visibility, improved productivity, and unlimited scalability—and it couldn't come at a better time. In the wake of the Covid-19 pandemic, security has become a top priority for nearly all organizations.

> *SOC analytics and automation, including security monitoring and incident management tools, are now mission-critical apps and services that are required to support revenue generation in today's changing business landscape.*

For SOC teams, the analytics and automation hype is real

AUTHOR_ Greg Martin, VP & GM of Security, Sumo Logic

With employees being required to work remotely, companies' data and critical assets are now exposed to more threats as the attack surface has—and continues to—expand dramatically. And SecOps teams are the first line of defense against

the data breaches and cyber threats that will undoubtedly become more frequent and more sophisticated as time goes on.

Although many enterprises have slashed budgets due to COVID-19, IT and IT security spending has gone relatively unscathed. In many cases, digital properties now represent companies' only channel for revenue generation, so investment in the systems that support these properties can't be cut. SOC analytics and automation, including security monitoring and incident management tools, are now mission-critical apps and services that are required to support revenue generation in today's changing business landscape.

Let's take a look at why analytics and automation are so vital for modern security teams, the possible downsides, and why a cloud-native platform is the future for the SOC.

Three core benefits

Nobody could have foreseen the explosion of machine data that the world is witnessing today. As technology continues to weave itself into businesses and peoples' everyday lives, the volume of data being generated is astronomical. And as more and more data is collected, it becomes invariably more expensive to manage, maintain, and derive insights and value from.

> *SecOps teams are routinely drowning in alerts, many of which are false positives and lack the context of both the business and the risk.*

Tools for analytics and automation are key for making sense of this data as it pertains to security, and provide three major benefits:

Visibility

Automation and analytics can provide security analysts with increased visibility into threats across both on-prem and cloud environments. This enhanced visibility helps SOC teams to better manage security alerts and investigate compliance-based risks.

Productivity

The automation of alert triage and threat analysis can help SOC teams achieve higher quality downstream response efforts and faster response times. This results in a jump in productivity, as security analysts can leverage this freed-up time to tackle other high-priority tasks.

Scalability

Organizational needs change just as fast as the threat landscape. Scalable security solutions for automation and analytics provide the resource elasticity to automatically scale data ingestion up or down as demand varies, along with the performance necessary for rapid big data analysis.

Have SOC teams found their silver bullet?

Although SOC analytics and automation provides significant value to security teams, it's not a silver bullet. Many teams still struggle with alert fatigue, which requires the proper technology and personnel to manage. In fact, a study from Sumo Logic found that 75% of SecOps teams said they needed to hire three or more analysts just to address all the alerts they receive daily. Furthermore, 70% reported the number of security alerts they receive on a daily basis has at least doubled over the past five years.

SecOps teams are routinely drowning in alerts, many of which are false positives and lack the

context of both the business and the risk. So, even when alerts are legitimate, analysts have to put in considerable effort to understand the impact that each security event might have. And this high number of alerts will only continue to grow as companies modernize their security stack. Cloud-native security platforms are essential for giving SOC teams more streamlined security insights, so they don't get lost in a sea of noise.

The magic of cloud-native platforms

According to Gartner, 69% of Board of Directors (BoDs) have accelerated their digital business initiatives as a result of the pandemic. As enterprises of all sizes increasingly accelerate digital transformation and move to the cloud, a new security architecture is required to address the challenges of defending evolving threats.

This modern enterprise security architecture must secure a dynamic, highly distributed, and constantly changing environment that spans remote workers, applications, devices, and cloud-based services and infrastructure. Cloud-native platforms fit the bill by providing SecOps teams with unparalleled security insights and enhanced visibility across hybrid environments, without the overhead of supporting infrastructure.

As the business landscape continues to evolve, and the number of remote workers increases, we can expect to see the adoption rates for cloud SIEM to increase dramatically. The need for a cloud-native security platform that features analytics and automation for improved visibility, productivity, and scalability will become a non-negotiable for ensuring the success of enterprises now, and in the future.

Three ways MITRE ATT&CK can improve your organizational security

AUTHOR_ Ganesh Pai, CEO, Uptycs

There's a good reason everyone's talking about MITRE ATT&CK: it's an objective, third-party standard with which organizations can measure their own detection coverage, as well as the coverage provided by EDR solutions. Still, even while you appreciate ATT&CK, it's not always clear how you can use it to improve your own organizational security. In this article, I'll lay out how you can use ATT&CK for the greatest effect.

It's worth going over some basics: ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge, and MITRE has developed matrices for enterprise, cloud, and industrial control system (ICS) environments. A September 2020 study by UC Berkeley found that 81% of surveyed organizations employ at least one of the ATT&CK matrices—not a bad level of adoption for a framework introduced in 2015!

MITRE ATT&CK has replaced Lockheed Martin's Cyber Kill Chain as the favored framework for understanding attacker behavior. Built using real-world observations, ATT&CK provides greater depth when describing attacker techniques, enabling red teams to reproduce the behavior of various threat groups (with tools such as ATT&CK Arsenal). ATT&CK also encompasses the post-compromise lateral movement left out by the Cyber Kill Chain, making it useful when designing detection capabilities for attackers who have successfully penetrated perimeter defenses and insider threats who are misusing legitimate credentials.

"That's cool," you say. "But how can I apply MITRE ATT&CK in my organization?" The best practices described below will help you answer that question.

1_Hone your threat model with ATT&CK

You can use the framework to understand the modus operandi of the threat groups most likely to target your organization. ATT&CK is built from

community contributions documenting the behavior of specific techniques observed in the field, such as exploits and malware used.

This information can help you to better understand how the threat groups targeting your industry behave and then prioritize your detection efforts accordingly. ATT&CK helps you to map out the detection capabilities you need to prioritize. And prioritization is key - after all, the exploits that are most important aren't necessarily the ones with the highest CVSS score but the ones that you are most likely to encounter in real life. Each organization is going to have a different threat profile depending on the data they must protect, the regulations in their industry, and which threat groups target their line of business.

2_Evaluate vendor capabilities with ATT&CK

Once you understand the techniques that you need detection capabilities for, you can use ATT&CK to evaluate which vendor solutions are most appropriate for your organization. A quick note here: one vendor's capabilities might not provide all the detection coverage you require. It's up to you to decide what there are other compensating controls you can put in place or whether you will need to purchase a complementary solution.

MITRE makes mapping vendor capabilities easier with their annual evaluations. For the past three years, MITRE has invited EDR vendors to participate in tests demonstrating their detection capabilities. Each year, the behaviors of a different threat group are used as a test baseline.

- In 2018, the evaluations simulated the behavior of APT3, attributed to China's Ministry of State Security.
- In 2019, the baseline was APT29, attributed to the offensive cybersecurity arm of the Russian government.
- In 2020, the evaluations looked at the behavior of Carbanak and FIN7, two financially motivated criminal groups that are known for targeting retail and financial services companies

Thanks to the ATT&CK evaluations, security buyers can now measure the efficacy of EDR solutions using an objective, third-party framework. The evaluations put vendors on an even playing field and provide buyers with quantitative evaluation criteria that complements the more qualitative data that you get in analyst reports.

3_Map detections to ATT&CK to make analysts' jobs easier

ATT&CK can also be used to speed up your analyst workflows, providing richer context around detections. For example, you should look for a platform that maps detection signals to the relevant tactic and technique so that analysts can quickly answer important questions such as "How are these behaviors related?" and "What is the potential severity of this attack?"

Time is an analyst's most valuable commodity. By providing them with at-a-glance context, analysts can more quickly determine whether an alert is legitimate, and if so, what needs to be done to stop the attack. Speeding up the detection triage workflow is incredibly important because it means that analysts can tackle more detections in their queue faster and with greater confidence. And that's your best shot at decreasing attacker dwell time.

Conclusion

As MITRE ATT&CK gains more prominence in the cybersecurity industry, it's important to know how to best put it to use in your organization. In this transparent standard, security leaders have a tool that can help them to better understand their threat profile, create a shortlist of appropriate EDR solutions, and supercharge their analyst workflows.

accurics™

RESEARCH REPORT

Cloud Cyber Resilience Report

Evolving Risks, Insecure Defaults, Watering Hole Threats

Download the report today:

http://bit.ly/cloudreport2021