SWIMLANE

ExpertFocus

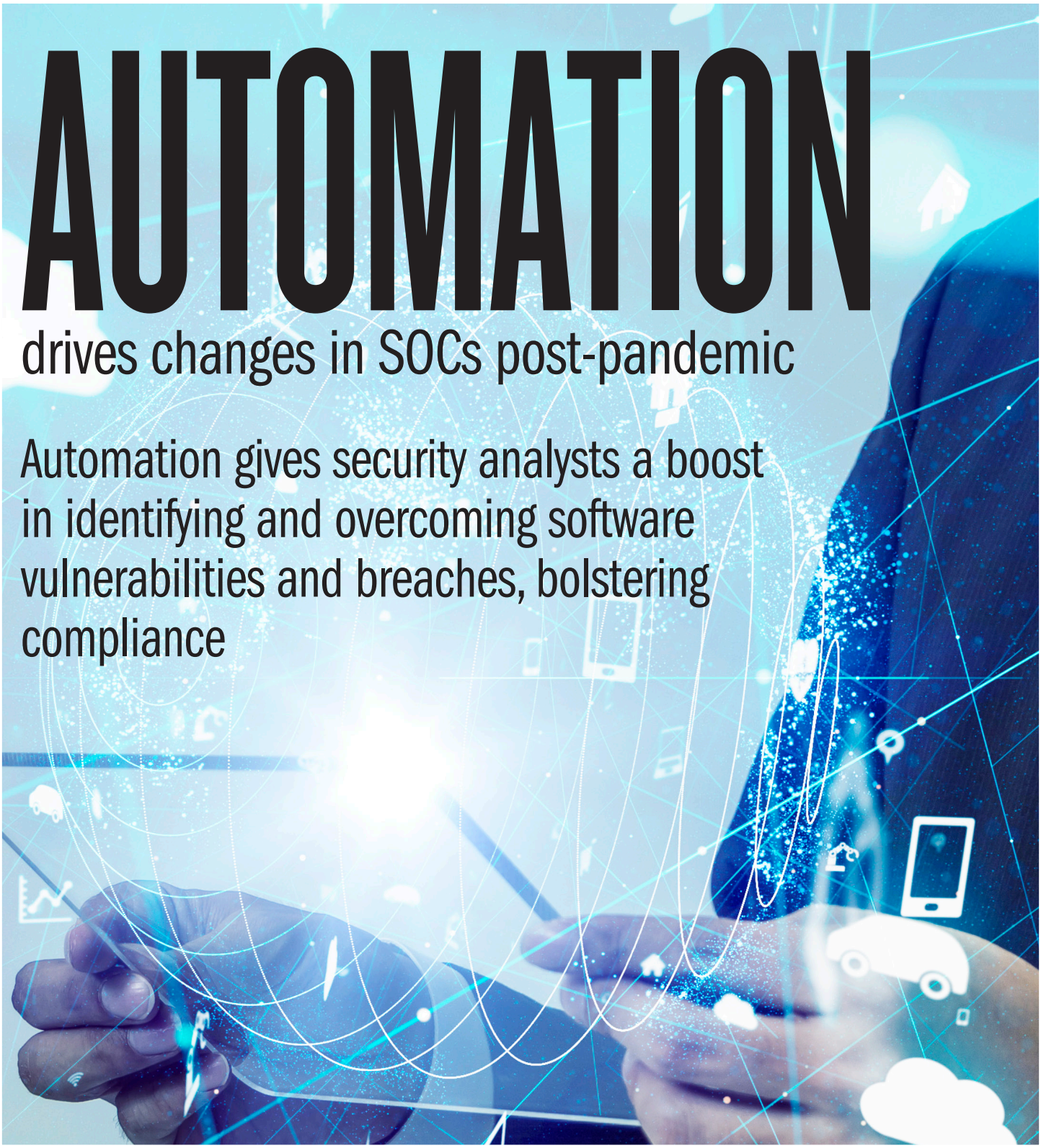
October 2020

Brought to you by Swimlane

AUTOMATION

drives changes in SOCs post-pandemic

Automation gives security analysts a boost in identifying and overcoming software vulnerabilities and breaches, bolstering compliance



Automating the network without borders

In today's new normal, employees are working from home, extending the company perimeter and stretching the attack surface. Automating cybersecurity and the security operations center are playing a vital role in keeping companies and their cloud-based assets and operations protected. Ed Tittel reports.

Today's new normal is nothing at all like how things were in the ancient times – say, back in January when people went to work in offices, dined in restaurants and went to theaters or beaches for a bit of entertainment. That was then; this is now. Today workers are at home on networks with questionable security; companies rushed digital transformations to move data and assets to the cloud; and corporate automation is being fast-tracked for those without operations already in place.

A pandemic can wreak havoc with corporate policies and procedures; in this case it provoked changes in how companies manage network security – local and in the cloud – and forced them to view their networks as borderless. Their assets are highly distributed and security automation is essential. The processes used before the pandemic simply are insufficient.

The effects of the pandemic are widespread and impact organizations of all kinds and sizes. As organizations identify and implement methods to cope with the security situation that today's work-from-home (WFH) model presents, they recognize that the future of the workplace post-pandemic will see new security rules focusing on remote users, endpoint management and asset management, wherever those assets are.

This puts the security operations center (SOC) in a challenging position by placing a heavy load on security teams that need to respond to potential threats faster, in more places and often with fewer resources.

Networks without borders

In particular, organizations must deal with borderless networks whose periphery is wherever remote employees are working at any given time. From a personnel standpoint, organizations must avoid the employee burnout that the always-on, always-available WFH virtual workplace produces. The economic downturn and continued economic uncertainty also means IT and thus the SOC, must cope with staff shortages and constant pressure to "do more with less." While understaffing is an ongoing challenge for security teams, the pandemic intensifies the issue as companies need more security staff and IT resources while budgets, built on 2019 expectations, fall short.

Cybersecurity is one of the few employment areas subject to what Nick Tausek, security research engineer at Swimlane, calls "negative unemployment." This seeming contradiction describes the circumstance, currently present in many SOCs, where there are more jobs to fill than there are people to fill them. Tausek observes further "any of my security analysts could quit his or her job today and find another job tomorrow. That makes staff retention a major priority in our SOC and for most SOCs at all the companies I know."

"Automation helps security analysts get their jobs done. It doesn't get distracted, it doesn't lose focus and it reacts immediately to events and incoming information."

– Cody Cornell, co-founder and CEO, Swimlane

Cody Cornell, co-founder and CEO of Swimlane, explains today's security situation as a "super distributed workforce with an equally distributed security center." Despite the challenges the pandemic is placing on companies with both office workers and security staffers working remotely, companies still need the kind of easy interaction and sharing of information that people working in a physical SOC might normally obtain by looking over each other's shoulders or talking to a colleague at a nearby desk. "Unfortunately," Cornell continues, "security teams can too easily lose that immediacy in a remote WFH scenario."

One approach to improving response time while reducing the impediments of a distributed security team is implementing a security orchestration, automation and response (SOAR) solution. SOAR helps organizations cope with this newly fragmented and scattered workplace through automation, especially by automating repetitive, manual tasks, which can take the form of IP address and domain lookups, copying and pasting data, ticket creation and the like.

Cornell says, "Automation helps security analysts get their jobs done. It doesn't get distracted, it doesn't lose focus and it reacts immediately to events and incoming information."

Hitesh Sheth, President and CEO at Vectra, a California-based provider of network detection and response (NDR) products and services, observes that the scattered nature of WFH leads to "an accelerated drive to secure connectivity." Vectra uses network telemetry and metadata to feed its machine learning algorithms, serving near real-time detection that recognizes and prioritizes events and incidents. This information integrates directly into Swimlane to help guide handling of incidents, including automated responses.

Vectra uses its understanding of security workflows and security analyst needs to deliver relevant inputs into Swimlane's playbooks that utilize "the kinds of data that we can – and do – provide for automation purposes." Sheth continues, "This automation is used internally, with strong tie-ins to our EDR (endpoint detection and response) and SIEM systems."

Speaking to the power of automation, he goes on: "We have 360 employees at Vectra, but only two of them work in our SOC. Automation makes our security workload manageable and gives us the agility to respond to high-speed attacks."

Companies see automation as a key ingredient for keeping SOCs working, if not the key ingredient in certain sets of circumstances. To further understand the why, here is how automation works in the SOC and what it can do to improve the security team's capabilities.

Force multiplier

Cornell sees automation in the SOC as a kind of "force multiplier or people multiplier, because it helps to retrieve or deliver the nitty-gritty details that security analysts need to get their work done."

One of the biggest savings that automation provides in the SOC comes in the form of time. Cornell observes that, without automation, "analysts need to open anywhere upwards of a half-dozen applications, feeds and tools to assemble the information they need to assess and evaluate a security threat or security incident. At Swimlane," he continues, "our automation delivers

"Automation makes our security workload manageable and gives us the agility to respond to high-speed attacks."

– Hitesh Sheth, president and CEO, Vectra

all that information either directly or as links so that analysts can get right to work without spending time on putting all the puzzle pieces together first."

There is another advantage to be gained when the right automation is in play. Cornell observes that "security automation is a special bonus when in the presence of an active adversary" while an attack is underway. He also asserts that "some kinds of attacks happen so fast that without effective automation to counter them — think 'smash and grab' — the attack is over before human security analysts can recognize and respond to what's going on. In such situations," says Cornell, "the right automation is your only hope to counter and fend off such attacks."

Indeed, real-time, event-driven automation can respond to attacks within milliseconds — less time than it takes the human eye to recognize that an alert has come in and action might be required. Of course, such automated responses require sophisticated recognition capabilities and advanced threat intelligence to drive them. They also require extensive testing and the ability to establish priorities so that clear and present dangers are handled expeditiously, while potential threats with no relevance to the organization can be ignored safely.

Cornell adds that his company sees all security information as content. "We can visualize data, provide reporting and trending, convey intelligence information and make it all easily visible and storable in our platform using a common set of representations and tools," he notes.

Cornell observes that, "we learn more from our customers than we ever learn by ourselves," explaining that most new feature requests come from their customers and get shaped by them as they react to Swimlane's capabilities and visualizations. Swimlane takes a collegial and collaborative approach to SOAR development understanding. As Cornell puts it, "Security is in large part a crowdsourcing and community effort and improves as more and different insights and points of view are incorporated."

Ratcheting up automation

Swimlane's Tausek says, "Automation tools improve and speed up security operations because they help to eliminate or avoid the time-consuming parts of the security analyst's job. Automation handles the bulk efforts and the heavy lifting."

In turn, this opens the door for security analysts to set priorities, improve detections, speed responses and spend time formulating (and even automating) remediation actions and workarounds to begin closing the incident response loop.

For example, an alert from a security information and event management (SIEM) system or a phishing email can first be subject to automation to create a case file for delivery to a security analyst.

"The automation checks links, reports on known bad IP addresses or domains, submits code to VirusTotal and presents its result," says Tausek. This lets analysts concentrate on matters of severity and priority, to establish the need for and urgency of a response and to understand not only if remediation is needed but also what would be required.

"Once the tool is configured, there's little or no cut-and-paste activity required from analysts to work with case files," he notes. Further, this means the SOAR solution can scan incoming security feeds automatically and use automation to generate case files and materials,

"Before security automation, security process comes first."

– Mike Lyborg, vice president of professional services, Swimlane

issue alarms and alerts, as well as track trends and severity levels.

Swimlane uses such data to build a content record, taking a feed, against which it can implement a variety of automatable tasks and responses. Integrations with all the security technologies present in an organization's environment such as endpoint security, identity and access management and cloud security allow SOC teams to essentially manage and orchestrate their security stack from one workbench.

Tausek works for Swimlane's internal labs team, developing innovative new use cases and staying abreast of customer needs. He says that customers like the customizability of the platform and while coding skills are not a requirement, many look for security analysts with basic Python programming skills to create ever more customized automations for the platform as needed.

He identifies detailed security configurations and off-boarding scripts as particularly popular with customers. The latter starts monitoring employee activity two weeks before their separation date and pays special attention to use of privileges, file copies across the organizational boundary and administrative actions and continues for several weeks beyond the separation date as well. Tausek has also seen numerous detailed use cases built around cloud services, customer applications and related toolsets. "The more you put into understanding and using our automation," he opines, "the more you'll get out of it and the happier your security analysts will be."

The process to security

Mike Lyborg, Swimlane vice president of professional services, runs post-sales support for customers, including a consulting services operation. As such, he pays attention to how automation is used and what value it provides, rather than dwelling on the details inherent to scripting, testing and deploying automation.

"Before security automation, security process comes first," he says. His team works closely with a customer's SOC and its security team to understand prevailing security policies and processes.

"Our consulting process works with the customer to help them reverse engineer how things work already," he notes. As an important aside, he also observes that "customers who already have and use written security policies and processes generally do best."

But written policies and procedures alone are not always enough. "Even for those with good written materials, we often find that processes as practiced do occasionally diverge from processes as written," he continues. He recommends that customers build playbooks with script collections to match, adding that "very often, we are able to improve the customer's security processes while we're automating them. This may make things faster, more reliable, or easier to use – if not all three."

In putting automation playbooks together, Swimlane finds that working backwards from actions, inputs and outputs is extremely helpful. Says Lyborg: "We try to look at everything as we begin to automate. This includes tickets and ticketing mechanisms; SMS, email and other messages and alerts sent and received; account handling and job roles; firewall and proxy rules; DNS services and sinkholes and more."

It is a big job but if done well, it helps customers get more productivity from their SOCs and staff

> "We don't believe in automating our way to fewer security analysts or reducing staff. We use automation for block-and-tackle tasks to make our analysts more productive."
>
> *– Jarret Raim, senior director, managed services, Bitdefender*

members, including creating a capabilities cushion if budget reductions for staffing and technology outlays occur. Lyborg also emphasizes that "improved and faster responses" are key to increasing ROI from SOAR investments, particularly from automation.

Bitdefender real-life example

As a leading purveyor of endpoint security software and other security solutions and services, Bitdefender leverages Swimlane in its internal operations and managed detection and response (MDR) service. Bitdefender's Jarret Raim, senior director of managed services, built a SOC at the company after moving over in 2019 from Rackspace. At his former employer he was director of Rackspace Managed Security and built that company's managed security business.

Romania-based Bitdefender has been largely locked down during the pandemic with most employees working from home since March. Raim, based in Texas, says Bitdefender was lucky to have had a fully planned-out WFH strategy in place when the pandemic struck. Its U.S.-based MDR operation is completely cloud-based. All its capabilities are virtualized, accessed through virtual machines (VMs) or Software-as-a-Service (SaaS) capabilities. Its infrastructure uses an Azure-based Microsoft 365 suite and Azure Active Directory with two-factor authentication for identity, authorization and access control services.

"Anybody with Internet access, a laptop — and the right credentials — can get into the SOC. We have a separate level of authorization and access control for our organizational unit, which provides MDR services and guidance to our customers," he says.

In terms of staff composition, Raim relays that most of the staff fills one of two roles: security analyst or threat intelligence analyst. Other job roles include defensive infrastructure specialists, customer briefing center staff and security operations specialists.

Automation comes into the picture in easing the "grunt work" for security staff, he notes. "We don't believe in automating our way to fewer security analysts or reducing staff. We use automation for block-and-tackle tasks to make our analysts more productive. We're always looking for ways to scale what the security staff can do so we can take care of more customers and more endpoints. That's how we succeed."

When asked how active a role his security analysts take in building automation, Raim admits that "analysts hack their Python scripts at a basic level. We're not talking full-blown Python application development, that's for sure. We have software engineering resources at Bitdefender for that kind of thing."

But analysts can and do create basic Python scripts and "massage existing scripts" to bring in threat intelligence data and remediation advice to get the job done, he notes.

To understand what drives security automation at Bitdefender, Raim says, "It's all about workflow. You must understand what you should automate, especially where analysts spend their time, to get the best results. We find that tasks involved in collecting data, assembling information and delivering case packages gives us a boost. We also find that building in staff involvement trees and escalation graphs really helps expedite workflow and leads to speedy case resolutions."

Security operations at McAfee

Mandar Pargunde, McAfee's director of security operations, explains

"Our endpoint security and endpoint detection and response (EDR) tools let us maintain visibility and detect suspicious activities. Given the volumes of data this generates, we've used Swimlane effectively to automate triage for and respond to such activities."

– Mandar Pargunde, director of security operations, McAfee

the role of the SOC at McAfee as "responsible for detecting and responding to suspicious events across our global IT environment. To accomplish this goal," he continues, "the SOC utilizes various McAfee technologies and works with a number of stakeholders ranging from the service desk to our engineering departments."

The McAfee SOC seeks "to identify repetitive, time-consuming tasks and find out innovative ways to automate them." Thus, for example, as part of its "detect and respond functions, the SOC takes on a variety of tasks that range from something as simple as data enrichment to something complex such as including the right systems to be involved in an investigation. Our McAfee tools integrated with Swimlane allow us to automate mundane or time-consuming tasks and saves a lot time for our analysts."

Since the pandemic struck, McAfee focused its monitoring efforts on "all the hosts that have moved outside our castle walls. Thus, prevention and detection logic has shifted to host-based tools for the most part," Pargunde says. "Our endpoint security and endpoint detection and response (EDR) tools let us maintain visibility and detect suspicious activities. Given the volumes of data this generates, we've used Swimlane effectively to automate triage for and respond to such activities."

In terms of automation's changing role, McAfee's initial challenge was to determine which "security controls we have in place to measure our prevention, detection and response capabilities," he continues. "Given answers in terms of McAfee products deployed on our hosts, we made sure we had the right alerting and triggering mechanisms in Swimlane to handle the caseload. Swimlane does good work to triage and enrich data and that saves lots of time for our analysts."

From a benefits perspective, Pargunde says, "The number one benefit is the ability to detect and respond on time [using automation]."

In addition, automation means McAfee can "take on high volume and adapt quickly as compared to traditional approaches that are both time consuming and not scalable," he adds.

In general, McAfee finds that automation enables it to track how much of its environment it is monitoring, determine how many detections it can review and respond to, empower analysts with improved tools, workflows and playbooks, speed the detection and response cycle and measure its ability to meet key performance indicator (KPI) targets and improve its performance on those that come up short.

As Swimlane and its partners and customers attest, security automation brings tangible benefits to those who put it to work, especially in the pandemic and post-pandemic SOC. It shortens the incident response cycle; offers lightning-fast response to high-speed attacks; relieves security analysts of tedious, time-consuming make-work; and generally, helps make SOCs more productive. Today's new normal looks to change tomorrow's SOC for the foreseeable future. ■

ExpertFocus

Swimlane is at the forefront of the security orchestration, automation and response (SOAR) solution market and was founded to deliver scalable security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages.

For more information, visit swimlane.com

ADVERTORIAL

Staying ahead of pandemic-related cybersecurity threats with automation

The COVID-19 pandemic has impacted organizations worldwide. Many were forced to transition their entire workforce to remote environments seemingly overnight, while others had to scale down their workforces through furloughs or layoffs. These changes have led to numerous challenges for security operations centers (SOCs). Additionally, today's SOC is faced with a growing cybersecurity skills shortage and an amount of alerts that no single team can hope to keep up with manually. To help mitigate these issues, while also dealing with budget cuts and other business challenges, many are turning to security orchestration, automation and response (SOAR) solutions.

According to a recent Enterprise Management Associates (EMA) report, "...IT security teams are relying on the automation delivered through SOAR and other security technologies like never before... 94% [of respondents] reported that their SOAR platforms were either very or extremely valuable in enabling security teams working remotely to coordinate security workflows." In fact, with the dramatic increase in remote working, this study highlighted the fact that it's taking SOC teams significantly longer and making it much more difficult to perform vulnerability scanning on endpoints and deploy patches and updates.

Although phishing is one of the most common use cases for automation—and typically one of the first completed during a SOAR implementation—the report identified many other ways that automation is being used in organizations during the rise of remote work. Leading responses include automating vulnerability remediation and automating patch management.

Swimlane customers and partners have also indicated that these two use cases are increasingly popular right now, as unpatched and misconfigured hardware, applications, security stacks, systems, endpoints and cloud services can result in massive security breaches via open ports, configuration settings and unpatched vulnerabilities. A SOAR solution like Swimlane can automatically add important contextual data by leveraging prior scan results, analysts' notes, and known and accepted risk elements. This provides your SOC with a more efficient way to proactively see, prioritize and remediate vulnerabilities across your IT ecosystem.

To learn more about how automation can enhance your SOC during these unpredictable times, download EMA's *How Automation and Orchestration can Help Bridge the IT Security Skills Gap* report today.

SWIMLANE

1-844-SWIMLANE | swimlane.com