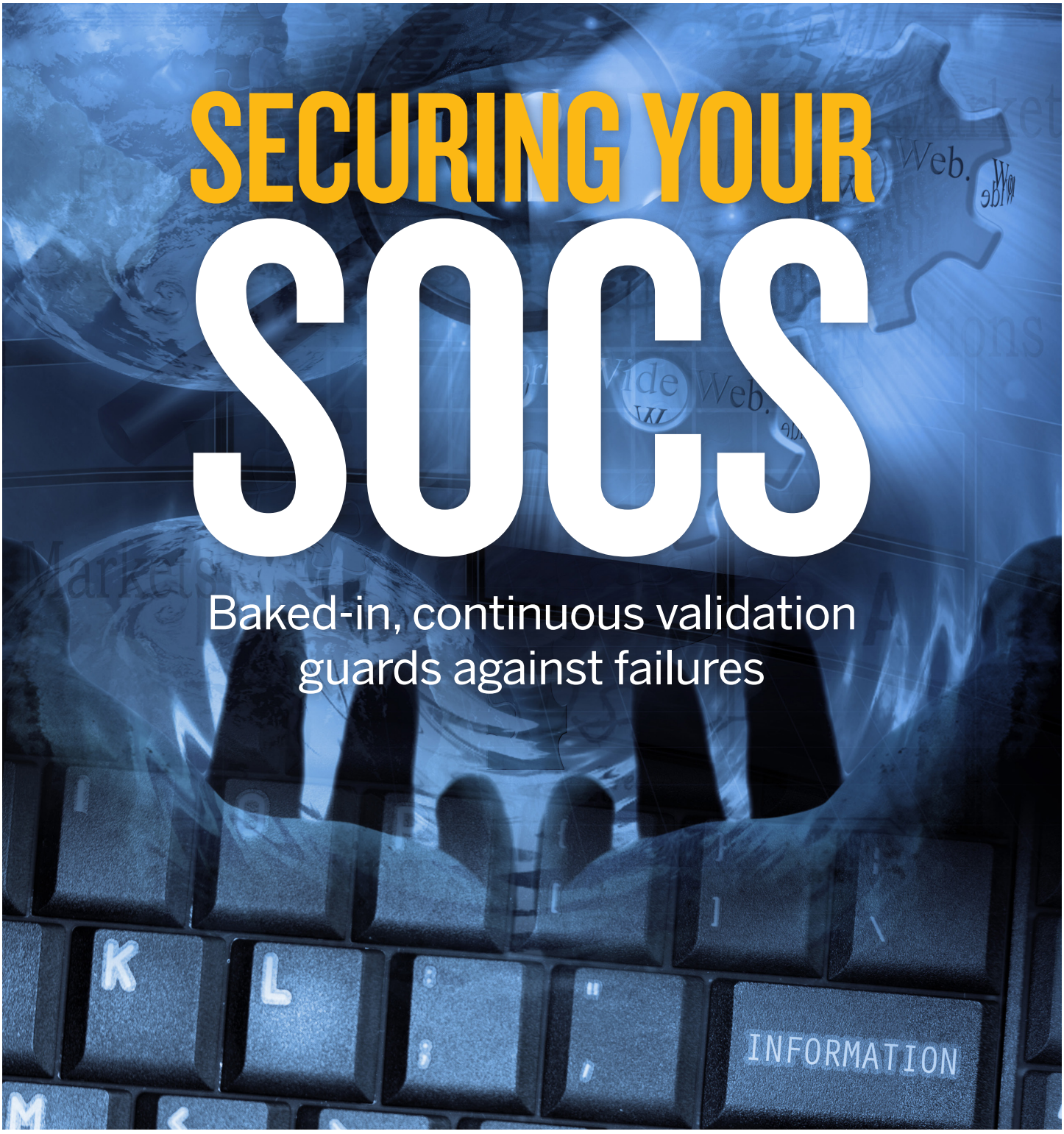

SECURING YOUR SOCS

Baked-in, continuous validation guards against failures

ebook

An SC Media publication

Sponsored by

Cymulate

Maintaining constant vigilance with continuous validation

Cyber resilience is key to maintaining attack and compliance readiness. How that all works in the SOC is where the magic occurs. Melisa Bleasdale reports.

Merely having a security operations center (SOC) is not enough to guard against catastrophic attacks given the nature and magnitude of today's security breaches. Protecting an organization requires constant vigilance coupled with controls and cross-functional education.

SOCs vary in size, scope and staffing across various industries, with the common thread being that they exist to monitor, detect, and respond to evolving threats to their respective organizations. Guarding against failures in security architecture has as much to do with constantly testing its capabilities as it does ensuring the right people and tools are in place to do the job.

Adding increasingly advanced security products to your arsenal might seem like a good course of action, yet in the absence of continuous validation it is an unsustainable and unrealistic approach. The question becomes whether security processes should be driven by validation or vice versa.

John Roman, CIO of the Bonadio Group, a Rochester, N.Y.-based top 50 CPA firm servicing multinational clients, says his company built a risk management-based security process with continuous validation baked in, not bolted on. It is never a question of whether a company is going to be attacked, but when, he says, adding that organizations must anticipate being a target, building their programs based on how they will respond to attacks.

The security team practices incident response tabletops and regularly tests its disaster recovery plans and other related exercises. Noting that there is always room for improvement in every organization's approach to security, Roman feels that if you are not in the habit of testing your systems continuously, it is effectively like learning to drive in the middle of a car accident.

"Not validating your defenses as a regular exercise will have you trying to defend yourself during an active attack, when it is already too late. The bad people out there are not taking breaks," he says. "Their attack process is continuous. We have to keep up with them by continuously validating our security systems. Hackers aren't rusty and we shouldn't be either."

Jill Knesek, CTO of Chicago-based Cheetah Digital, an independent, cross-channel marketing services provider, agrees, stating that there is always a smarter hacker trying to breach your defenses.

"The larger your brand, the larger your threat vectors and your ability to be compromised. You really have to be on your game. We are constantly trying to make sure we know what the hackers see externally as a perimeter, and then, if they do somehow get through that exterior, what options do they have internally? How many break points can I have to keep them in a small area that is not going to expose us so that we can create a length of time for identification and detection so that we can quickly unplug, remediate, block, whatever we have to do?"

For Knesek, validation testing is composed

OUR EXPERTS: Validation

Mansoor Alam, founder & CTO, Memoir Health
Deron Grzetich, managing director, KPMG
Tim Hickman, partner, White & Case LLP
Jill Knesek, CTO, Cheetah Digital
John Roman, CIO, Bonadio Group
Rob Suárez, VP & CISO, Becton Dickinson

Validation

67%

Percentage of cybersecurity professionals who believe cyberadversaries have a big advantage over cyber-defenders, up from 59% the prior year

– ESG

of multiple layers. Some actions are done weekly, monthly or annually, but stresses the point that validation is ongoing. In order to know how you improved your security systems, she explains, you have to know where you were previously. If during your validation testing you find that your company is not improving or is getting worse, you clearly are not putting enough resources into that area of your business, she notes.

Mansoor Alam, founder & CTO, Memoir Health

"Companies should be asking themselves whether the controls they have in place are enough, and continuous validation can answer that question," says Rob Suárez, vice president and CISO at Becton Dickinson, a global medical technology company headquartered in Franklin, N.J.

Becton Dickinson has a specialized team of penetration testers, people who wake up in the morning with the singular goal of finding vulnerabilities, performing security assessments, evaluations and hands-on testing of their applications and medical devices, he says. They also engage with outside vendors to further strengthen their capabilities and broaden their focus on security readiness.

Mansoor Alam, founder and chief technology officer of Memoir Health, a health care services company for chronic pain patients based in San Francisco, agrees with Knesek. He says that the variance in adoption of security processes, such as validation, is largely a result of changing perspectives in how organizations prioritize risk.

"Traditionally, we invested at the systems level, taking a top-down approach that focuses on protecting our most sensitive assets. For obvious reasons this makes sense, but I believe that we need to rethink and expand our definition of sensitive assets."

What you don't know ...

Knowing your current vulnerabilities provides you with a baseline for mapping your immediate security priorities. Ongoing validation shows whether you are focused on the right areas and whether your controls and implementations are working, Knesek says. If vulnerability scans keep coming back showing no improvement after repeated tests and implementations, you need to consider whether the point of failure is your team, tools or process, or all the above. And, you need to ask what it is that you are doing or trying to accomplish with the scan. If no improvements are identified, perhaps the controls being implemented should be reevaluated.

> "Traditionally, we invested at the systems level, taking a top-down approach that focuses on protecting our most sensitive assets. For obvious reasons this makes sense, but I believe that we need to rethink and expand our definition of sensitive assets."
>
> *– Mansoor Alam, founder & CTO, Memoir Health*

"Why are you scanning just to find out that you have vulnerabilities?" she asks. "You need to take the information and bring it back into the organization and make sure that if there are any vulnerabilities that the systems teams are patching them properly or shutting down ports or even creating more secure coding [if you are developing new technologies or applications]. Then you scan and validate again. You should constantly be improving."

64%

Almost two thirds of organizations believe they either definitely or possibly had a breach due to employee access

– BeyondTrust Research

In 2002, then Secretary of Defense Donald Rumsfeld said "…there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns — the ones we don't know we don't know." While he was talking about terrorism during a press conference at the time, the sentiments certainly could be true of cybersecurity today. Learning what you do not know is a key responsibility for cybersecurity teams.

Deron Grzetich, managing director, KPMG

Deron Grzetich, managing director at KPMG, a global network of professional firms providing audit, tax and advisory services, headquartered in Amstelveen, the Netherlands, recounts an experience he had in early 2007 helping to build the security program for a global law firm in Chicago. Security in the legal industry was still in its infancy but the company understood that it was likely to be the subject of attack as part of the supply chain since it held valuable information on its clients, he says.

"At the time, a friend of mine said, 'You've been at this for a year and you guys are doing some basic blocking and tackling. How do you sleep at night?' I answered that I was sleeping really well because we had not fully implemented our monitoring function," says Grzetich. "That it was next on the list and I knew I would not sleep once I realized what was happening inside and outside of my organization. I told him, 'Right now I'm dumb, blind and happy. Once I see it all, I am going to see the bad stuff.'"

He said that the "bad stuff" was legion and included everything from poorly implemented IT processes and general security hygiene to malicious things internal users were doing on a daily basis that put the company in a dangerous position. Adding that organizations are being tested every day by internal and external threat actors, performing continuous validation will allow you to quickly find those instances and remediate them, he notes.

Grzetich underscores that thought, reiterating that organizations are being tested every day by external threat actors and their own employees. He says that whether you monitor for that activity or not is when you realize the benefit of continuous validation. One cannot defend themselves against Rumsfeld's unknown unknowns.

Augmenting your team

Among security professionals there are differing opinions on whether continuous validation practices, such as penetration testing, threat hunting and attack surface management, should be kept in-house to minimize external sources gaining access to their security architectures. The security professionals interviewed here see working with qualified outside vendors as an opportunity to further bolster their teams. While they understandably would not go into depth about their company-confidential approach to validating their own company's defenses, all agreed that they are stronger because of their relationships with trusted firms such as external SOCs.

> "Not validating your defenses as a regular exercise will have you trying to defend yourself during an active attack, when it is already too late."
>
> *– John Roman, CIO, Bonadio Group*

#2

Q4 2020 ranked as the security-biggest quarter for funding of cybersecurity companies over the past three years

– CB Insights

Small to medium-sized businesses are often better served by specialized outside partnerships. As Knesek explains, smaller organizations are like small-town fire departments. Lacking enough ongoing emergencies to have a full-time staff of firefighters, they call in reinforcements from larger cities when necessary. Having employed external SOCs at nearly every organization where she has worked, Knesek says she feels that these external teams offer a deep level of expertise that is hard to find in an average SOC.

Jill Knesek, CTO, Cheetah Digital

Partnering with external experts is not limited to smaller companies, however. Large, multinational firms often contract out penetration testing and other exercises as a means of confirming their teams' results.

Suárez adds that this is a hot topic in the security industry. Having spoken to multiple professionals and peers in the financial services and critical manufacturing industries who have gone through a security journey, he says that it comes down to maturing your practices.

"It is important to engage external partners as well, because you are never going to have all of the competencies within your individual organization unless you do security as a business," Suárez says. "We are a medical technology company, not a cybersecurity company. Working with outside partners to support and augment our capabilities pressure tests our own penetration testing practices with our full-time staff as well, so we use a combination of internal and external teams."

What should you look for when engaging with an external SOC? Knesek says it is all about building relationships and that starts by no longer calling them a vendor. She prefers the word "partner." She looks to see that they are well regarded in the industry, and that they have achieved a Type 2 compliance certification such as SOC2 or ISO2701, something she feels that demonstrates their competence. Once she has established a level of confidence in them, she knows that when the inevitable happens that strong relationship comes into play.

"I am very fair with my partners. I will do my part to help them through any crisis but at the same time, I demand information so that I can keep my own client base, executive team and corporation apprised so that we can monitor and manage incidents appropriately," she says.

Roman believes that when it comes to external validation of your security implementations, it is a good idea to have an outside company with the requisite expertise to ensure your staff can focus on things like vulnerability, remediation and implementing technical policy.

> "We are constantly trying to make sure we know what the hackers see externally as a perimeter, and then, if they do somehow get through that exterior, what options do they have internally?"
>
> – *Jill Knesek, CTO, Cheetah Digital*

"Too many times we hear, 'We received an alert two months ago that something bad was happening, but there are thousands of alerts to pay attention to,'" he notes. "We all know that IT and information security professionals get alert fatigue, whereas an external SOC gets paid not to get fatigued. It is certainly a lot less expensive outsourcing

48%

Percentage of organizations that knowingly push vulnerable application code into production regularly

– ESG

a SOC to perform validation than hiring an information security professional for a small- to medium-sized business," he adds.

SOCs and the law

In 2020, hundreds of companies of varying sizes were the victims of the SolarWinds breach, the nation's biggest and most worrisome security breach of the year. The fact that it was unleashed from within a major security provider's software underscores the truism that you are never too big to fail — or, at least, be breached.

Rob Suárez, VP & CISO, Becton Dickinson

Not only do security breaches cause major damage to their targets, they also unleash countless compliance problems. Interestingly, it is these very sort of security breaches that trigger new and increasingly stringent regulations. Is it a stretch to believe that if continuous validation and immediate vulnerability remediation were the norm, there would be fewer regulations and less of a need for them? Some might argue that is the case.

> "Compliance is the bottom watermark; it is minimally what will be done. It is not our end goal; it is not the upper tier of what we strive to achieve as a security organization."
>
> – Rob Suárez, VP & CISO, Becton Dickinson

Although there are no guarantees in security, continuous validation can provide a critical layer of risk mitigation that can mean the difference between thwarting a devastating breach and not realizing you've had intruders on your network for months on end.

"We learn through history that if we do not take responsibility [for security failures], somebody is going to force us to do it and that somebody is typically the state or federal government in the form of regulations," remarks Roman. "They are usually created in response to something bad happening more than 3 times. Sometimes companies just cannot self-regulate. A lot of times it takes a compelling event for all of us to change and act differently."

He points out that, unfortunately, what has happened with data breaches over the past 10 years have been significant, compelling events that have affected all of us. The government has indeed stepped in, often at the state level, with each state drafting up its own version of data protection laws, requirements and enforceability.

Compliance is not necessarily the first lens Grzetich's team looks through in building security functions for his clients. They are evaluating threats, the overall landscape, preventative tools and security processes while looking at their client's businesses through a lens of threat management, which as a by-product includes compliance elements, he says, but is not driven by them.

"I think a corporation's security practices should be driven by what is most important to that corporation's customers and more importantly, what is important to society," observes Suárez. "As a medical technology company, what drives our security practices is protecting health care providers, the institution of health care globally and protecting the patients.

"That sets us up with a wide variety of the security controls that we pursue," he says. "Compliance is the bottom watermark; it is minimally what will be done. It is not our end goal; it is not the upper tier of what we strive to achieve as a security organization."

25%

Apple, Netflix, and Yahoo accounted for 25% of brand impersonations in phishing attacks in Q1 2020

– Security Boulevard

Security controls put in place to ensure attack readiness are often the same that provide compliance readiness. In the field of information security, these controls protect the confidentiality, integrity and availability of information and they are more important than many CIOs and CISOs realize.

Tim Hickman, partner, White & Case LLP

Global concerns

Tim Hickman, a partner at White & Case, a New York-based international law firm, notes that SOCs are challenged with the daunting task of maintaining security in their organization while simultaneously monitoring the communications traversing the network. The biggest problem, he emphasizes, is that a lot of that communication involves humans or is about humans and the SOC is going to have personal data to protect that falls under a multitude of complex global regulations.

What works in the U.S. in terms of securing data against a breach and which regulations apply (for example, *California Consumer Privacy Act, California Privacy Rights Act, Graham-Leach-Bliley Act,* and the proposed *New York Privacy Act*), might not be enough under more stringent international requirements such as the *General Data Protection Regulation* (GDPR) and its cross-European Union (EU) variants.

"The definition of personal data under EU law is so broad, information captured [such as IP addresses] applies as personally identifiable information (PII), but would not be considered PII under U.S. law," Hickman says. "A lot of security measures that companies implement involve the necessity of processing and analyzing information that is considered PII. As soon as that happens, you have a whole raft of GDPR-compliance obligations, which can be exceedingly difficult to satisfy in the SOC context."

Hickman explains that biggest impact to a SOC has to do with questions such as whether what you are doing is monitoring employees and if so, is that monitoring permitted. If it is not, what do you need to do to make it lawful and if it already is, how can it remain that way?

Like so many compliance regulations, GDPR is in a constant state of flux. Adding to that challenge, member states within the EU and countries outside of the EU, such as the U.K., have their own, distinct interpretations and enforcement of the regulation. It seems prudent to engage with outside counsel on how to stay on top of ever-changing and labyrinthine global regulations. It should be noted that while the U.K. has left the EU as a member, its close ties with the EU means that a huge number of British companies that do business in Europe still must comply with GDPR.

> "The definition of personal data under EU law is so broad, information captured [such as IP addresses] applies as personally identifiable information (PII), but would not be considered PII under U.S. law."
>
> *– Tim Hickman, partner, White & Case LLP*

Continuous readiness

Because humans are fallible, Suárez points out, the technology they develop will always contain vulnerabilities. It is a matter of time and attention from different cybercriminals and cyberthreats as to when those vulnerabilities will be found. He believes

36

After a data breach, as many as 36 additional deaths per 10,000 heart attacks occurred annually at hundreds of hospitals examined

– U.S. National Science Foundation

cyber resilience should be a priority for any company because attacks will only continue to grow in ferocity. Suárez then encourages all companies to make continuous threat hunting part of their security process.

He also cites information sharing with fellow industry security leaders, as a critical means of strengthening your security posture.

John Roman, CIO, Bonadio Group

"Through information sharing as a community, we are empowering each other with information that is not readily available to the public. We have to recognize that criminal organizations we are defending against are actively sharing information amongst themselves," he says. "This type of information sharing, in order to match the pace of new cyberthreats, is fundamental."

Knesek opines that having internal controls is important, but having an external validation and testing team, whether it is doing web application scanning or infrastructure penetration testing, is critical to providing insight into areas that need improvement. That is where she feels continuous validation becomes ongoing improvement toward reducing vulnerabilities and increasing time to detection. This is the key element to being successful, she says, and points out that no organization is ever going to be free of security events.

Roman views continuous validation and continuous compliance readiness as critical pursuits for all size organizations.

"I'll go back to the fact that you do not want to practice a response to an incident from a real incident," he explains. "I would say that as IT professionals and information security professionals, we invest in ourselves by having continuous training, especially if you maintain a certification like CISSP, CISSA, etc. Why wouldn't you also apply the same to the organization that you are responsible for protecting?"

Roman views continuous validation as an investment in your organization, with the investment being measured in time spent pursuing a continuously improving state of security and compliance.

"It is not occasional security and compliance, or periodic. It is continuous," he says. ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@cyberriskalliance.com.*

If your company is interested in sponsoring an ebook, please contact Dave Kaye, chief revenue officer, at (917) 613-8460, or via email at dave.kaye@cyberriskalliance.com.

3X

Reported data breaches grew from 56 in Q4 2019 to 154 in Q4 2020

– Department of Health and Human Services

Cymulate

For companies that want to assure their security against the evolving threat landscape. Cymulate SaaS-based Continuous Security Validation automates security risk assessments end-to-end, enabling them to challenge, assess and optimize their cyber-security posture simply and continuously. Because security professionals need to know and control their dynamic environment.

More information is available at Cymulate.com

Masthead

EDITORIAL
SPECIAL PROJECTS EDITORIAL DIRECTOR
Stephen Lawton
stephen.lawton@cyberriskalliance.com
SPECIAL PROJECTS COORDINATOR
Victor Thomas
victor.thomas@cyberriskalliance.com

SALES
CHIEF REVENUE OFFICER Dave Kaye
(917) 613-8460 *dave.kaye@cyberriskalliance.com*
VP, SALES Matthew Allington
(707) 651-9367 *matthew.allington@cyberriskalliance.com*

Determine Security Gaps in Minutes and Remediate them

Cymulate