Sponsored by

Google Cloud

Key Elements Enterprises Need to Include in Modern SecOps

Security teams are overwhelmed in the operations center. What will it take to unlock effective threat detection and master data collection and response for modern defense?

Brought to you by

informa tech

INSIDE:

Next

Key Elements Enterprises Need to Include in Modern SecOps

Security teams are overwhelmed in the operations center. What will it take to unlock effective threat detection and master data collection and response for modern defense?

By Evan Schuman, Contributing Writer, Dark Reading

The security operations center (SOC) is the enterprise's first line of defense against an active attack. It is the brain of all security operations, with a team that sifts through threat intelligence, events data, logs, and activity reports from throughout the enterprise and key partners around the world. And, yet, the SOC is as underfunded and understaffed as any other area in security. SOC staff members typically work with antiquated tools, wrangle outdated data, and grapple with massive blockages to the information and systems they need to do their jobs.

Today's enterprise SOC environments are both massively distributed and highly localized. An enterprise often has more than a dozen authorized global cloud providers — on top of an untold number of shadow IT cloud deployments. Some of these clouds are designed to work with others, but many are not. Then there are the issues related to IoT, remote offices, and third-party systems.

How can CISOs realistically give SOCs the tools needed to effectively manage all of that?

Overwhelmed by Data and Noise

It all starts — or doesn't — with access. Many enterprise SOCs have insufficient access to their own employer's NAT IP addresses and — critically — its many cloud environments. Visibility requires not only credentials and internal URLs, but also the names of all relevant personnel on file with the cloud provider, which would need to be notified in the event of an active attack.

"The oceans of data have become a tidal wave leaving SOCs drowning in mostly useless data and noise. For some reason, we as a security community continue to enable the notion that collecting 'all the data' will prevent attacks, but that has proven to be false time and time again," says Tyler Young, CISO at security data vendor BigID. "The assumption that we can simply plug data into our SIEM to overlay known threat data and our internal telemetry and magically find threat actors in our environment is just wrong." Indeed, much of the data currently gathered by SOCs is useless by the time it reaches stakeholders, Young says. One reason is that private sector organizations often hesitate to share details about incidents. Another challenge is that a dearth of context and details around incidents makes it more difficult for SOC staffers to make use of the information they do have.

Threat Intel Must Be Actionable

Brian Bell, the global head of cybersecurity and risk services at consulting firm Wipro, says that what many vendors — and quite a few enterprise SOC teams — consider to be threat intelligence actually is not. What people sometimes forget, he says, is that threat intelligence needs to be

Previous Next

actionable and usable.

"Threat intelligence is a term that sees a lot of abuse in the industry," Bell says. "The threat feeds you receive, whether paid or open source, are not intelligence; they are information at best and usually just data — never intelligence." Bell notes that a threat feed that consists of a list of bad IPs or domains with no context is simply data. Without proper curation, such a list is difficult to use effectively. "Information is much more useful than data but is still not intelligence," he says.

A threat feed that provides a minimum of context — as in, "This IP is associated with Dridex" — is on the border between data and information, Bell says. A threat feed that gives a list of bad IPs, along with the exact observed activity — as in "Dridex C2 communication on port 8043" — and the time the activity was observed has applied sufficient context to the data to produce information.

"Threat intelligence will be produced internally — not by reading blogs and repackaging the information but by applying a critical eye to what the security operations center and the incident response team are seeing in the wild," Bell adds. "What is currently actively targeting my organization? What context can I apply to this data? What intention can I direct it with?"

What Is the SOC's Material Business Impact?

Connected assets are the lifeblood of businesses, but it's often unclear how each asset is being used, says Curtis Simpson, CISO of asset intelligence platform vendor Armis. "The individual tools in the security stack are unclear of how each asset registering malicious or suspicious activity relates to the business. This limits the ability to effectively establish severity based on business impact and, in turn, leads to the prioritization of alerts based on only very limited technical context," he says.

When each tool has been configured to over-alert so that nothing is missed, and prioritization is based on limited technical context, the SOC is faced with an overwhelming list of conflicting priorities. The recommended approach to modernizing and optimizing the SOC focuses on asset intelligence. The first and most foundational step is to adopt a modern continuous asset discovery, identification,

"Threat intelligence will be produced internally — not by reading blogs and repackaging the information but by applying a critical eye to what the security operations center and the incident response team are seeing in the wild." —Brian Bell, Wipro

and intelligence platform that augments or replaces existing asset discovery and inventory software. This enables organizations to move from static, incomplete configuration management database (CMDB) data with limited contextual value to continuously consumable asset intelligence that guides prioritization.

Simpson suggests that this approach not only benefits the enterprise more effectively but also positions the SOC as essential and strategic.

"At the highest level, SOCs should position the intelligence platform between the rest of the security stack and the SIEM/SOAR [security information and event management/ security orchestration, automation, and response] to validate and triage every incident for suppression or response," Simpson says. At the same time, he acknowledges, many teams face resource constraints. "The team is already overwhelmed and undertaking optimization projects to address long-term challenges and position the SOC for the future when simply attempting to keep their head above water can make it challenging to even get started, let alone continuously optimize."

Making Complexity Simple

There are some who argue that the very nature of the SOC, along with how most enterprises leverage SOCs, is flawed and needs to be significantly reworked. Complexity is one of the biggest challenges facing the SOC, says Steve Winterfeld, the advisory CISO at Akamai.

"When I became a CISO, I didn't realize how much time would be consumed with vendor management," Winterfeld says. "But having a large number of security capabilities can lead to multiple issues. You have one engineer trying to maintain and optimize multiple systems, so none of them are up to date. Next, you have one analyst trying to respond to feeds from multiple systems and, in some cases, multiple dashboards. This leads to missed alerts that could have prevented an incident from becoming a major crisis."

The global attack surface has gotten exponentially more complex in the last few years. The attack surface is compounded by remote workers, customer access capabilities, growth of apps and APIs, the move to hybrid cloud infrastructure, BYOD, and SaaS, leaving security teams with multiple environments to protect, Winterfeld says. The clouds themselves are so large and numerous that they thwart efficient and cost-effective management. "Today, I am paying more to monitor my cloud infrastructure than I am paying for the cloud infrastructure," says Ken Westin, field CISO at Panther Labs, pointing to the need to have salaried specialists for each cloud platform. "When the cloud platforms make a change to their APIs or their log format, all of the data pipelines and detections break as a result."

"When that orphan tool comes up for renewal, you need to ask yourself, 'Is there a chance here for me to move to a single vendor that is perhaps an improvement for integration?' Treat every renewal as an opportunity to reduce the complexity." —Steve Winterfeld, Akamai

Take a Zero-Budget Approach

Winterfeld suggests that CISOs take a zero-budget approach to SOC security tools. For example, consider whether SOC operations will be affected if the vendor of a tool is acquired.

"It's all part of our third-party risk analysis," he says. "When that orphan tool comes up for renewal, you need to ask yourself, 'Is there a chance here for me to move to a single vendor that is perhaps an improvement for integration?' Treat every renewal as an opportunity to reduce the complexity."

As with other enterprise technology tools, SOC tools originate from many different places. For example, some tools may have been purchased directly a decade ago, while others may have ended up in the SOC via a company acquisition or when a team member downloaded software in shadow IT mode. Then there are the tools used by various cloud platforms that have become part of the SOC tool collection.

Previous Next

Having More Tools Is Never Better

Westin says an accumulation of tools can become a waste of license fees. Worse, he adds, in a SOC environment, security tools can fight each other, resulting in missed information, duplicate information, or a slew of false positives or false negatives as tools react to other tools with which they were not designed to interact

vast amounts of data in the typical enterprise SOC today. Of the countless petabytes and sometimes exabytes of log data that is being stored, he says, the vast majority has zero value. Further, he adds, nothing of use will be gained through a more granular view of the data, which becomes less valuable with each passing moment. Logs are great for forensics, but time and money being spent on storing logs

There are many tweaks and small fixes that can be put into place to improve enterprise SOCs, but fundamental and long-lasting improvements require addressing a problem that drives personnel shortages and the use of outdated and ineffective tools: budget.

In addition, many organizations are using tools designed for network architectures and threats that are at least a decade old. And enterprises are paying a lot of money for tools that can't handle an exponential increase in data volume, let alone keep up with newer threats targeting identity and cloud environments. For example, a SIEM that was designed for on-premises environments and legacy data centers requires major retooling and configuration to handle today's cloud workloads.

Organizations should focus on leveraging cheaper cloud-native options instead of trying to salvage expensive tools, and they should focus on outcomes, not the tools themselves.

John Gunn, CEO of wearable biometric authentication firm Token, laments the accuracy problems associated with the should be reprioritized and spent on analytics that would be far more effective, such as robust authentication, Gunn says.

"People are underestimating how dynamic attack mechanisms have become, especially with the integration of AI into attack methods," he adds.

SOC as a Value-Added Driver

Automation will prove essential to SOC operations and efficiencies, but only if deployed strategically, says Rob Boyce, global cyber resilience lead at consulting firm Accenture. Many organizations instead take an intelligence feed or a list of indicators of compromise (IoCs) and then try to automate the process of working with the data.

Boyce cites as an example the Log4j vulnerability. Log4j

was initially disclosed in December 2021, but it took many organizations months to find and patch affected systems because they didn't know which systems in their environment were affected.

"I think there's a huge way for automation to play a big role there to be able to fast-track the assessment of intelligence and the applicability of that intelligence within an environment," Boyce says.

Another key element with SOCs is active attack defense strategies and the role that triage should or should not play.

One school of thought is that SOCs have very limited resources, so the most valuable assets and the access points most likely to be attacked get the bulk of budget and attention.

Another school of thought suggests that professional attackers — regardless of whether they are state actors, identity thieves, ransomware extortionists, or cyber saboteurs intent on harming operations — are, by nature, contrarian. They prefer to gain access via low-priority paths that have minimal protections. Rather than directly attacking a high-value asset such as payroll records, these attackers try to gain access via a low-level asset — for example, a smart printer with its own IP address — and then quietly and slowly escalate privileges and move through the system to get to a higher-value target. For those who embrace this school of thought, identifying a path as low risk is painting a target on its back for cyberthieves.

Taking the Threat out of Threat Intel

There are many tweaks and small fixes that can be put into place to improve enterprise SOCs, but fundamental and long-lasting improvements require addressing a problem that drives personnel shortages and the use of outdated and ineffective tools: budget.

The best way to start the process, according to Accenture's Boyce, is to grab the CEO's and CFO's attention. How? Focus on business intelligence instead of threat intelligence. In other words, Boyce suggests, demonstrate to the leaders in charge of non-security lines of business how the SOC can help maintain or increase revenue. If you can do this, the CEO and CFO will be much more likely to invest more into security.

"Today, they are not showing senior management how the SOC is enabling the enterprise. No one is being shown the strategic value of the SOC in a way that informs business decisions. That is a huge opportunity," Boyce says.

For example, in the first hours after Russia attacked Ukraine in February 2022, management executives at a large multinational corporation were ordered to report to the board any likely impacts on the enterprise from the war.

The CEO believed there wasn't any meaningful direct exposure because the company did not have employees or major customers in Ukraine. However, the SOC staff carefully reviewed logs and discovered that several key partners conducted extensive data transfers with Ukraine. SOC staff prepared a report indicating that the war might cause problems with those partners, which could, in theory, impact the enterprise's operations.

"[SOC staff] moved from threat intelligence to just intelligence. In doing so, they showed the SOC to be a value-added driver," Boyce says. "Many organizations did not understand fully if they had third parties that may have operations within Ukraine. You can use AI and GenAI capabilities to scrape through even publicly available information about your third parties and find out if they did or did not have operations within Ukraine to be able to ensure that you're making appropriate contingency strategies."

The SOC's ROI

Perhaps the most popular SOC improvement advice involves contextualizing vulnerability data and prioritizing patching and remediation.

For Fred Rica, partner, advisory, for accounting firm BPM, that contextualization is where he encourages enterprise CISOs to start their SOC strategy thinking.

"There are more alerts than ever, point products litter the environment, thousands of vulnerabilities are disclosed yearly, systems produce conflicting data, and analysts can only see what the tools produce. So, what happens

Previous Next

is qualitative arguments win over quantitative, the loudest voice tends to win, and, as a result, the outcomes aren't always those desired," Rica says.

Britive CEO Art Poghosyan fears that many enterprise CISOs have not sufficiently adapted their processes to factor in today's threat landscape. "CISOs are not seeing the opportunity to understand the new ways that the environment is getting exposed," he says.

Poghosyan describes an organization where developers created a new polling API that pushes updates submitted by clients via a Web app to a new database. Unfortunately, the security or cloud operations team have no knowledge of this API or the newly created database. Sometime later, the person behind the account is compromised by a threat actor. Security and cloud operations teams won't see the intrusion initially because they are not aware of the new database or API. Far worse, the account used to access it looks normal because there is no way on the surface to know the account is bad because it was set up initially for a legit purpose.

Poghosyan's suggested fix is to leverage just-in-time access. "With a JIT cloud access management tool in place, the developers could have set up access profiles for the account that stood up these cloud-based resources. It could detect the unusual queries to the database by a developer account that was provisioned to a contractor but from an IP address range outside of the corporate network."

None of these suggestions will — on their own — convert SOCs into the security saviors that enterprise CISOs need them to be. However, they are a start.

SOCs need to be given access to everything in their global environments, and that means that the SOC must overcome the objections of other line-of-business executives. The SOC will remain the enterprise's first line of defense against attacks. The question enterprises must properly answer is whether the SOC team will be given what it needs to do its job.

About the Author: Evan Schuman has tracked cybersecurity issues for enterprise B2B audiences for far longer than he will admit. His byline has appeared in The New York Times, Associated Press, Reuters, SCMagazine/SCMedia, VentureBeat, TechCrunch, eWEEK, Computerworld, and other technology titles. He has also repeatedly guest lectured on cybersecurity issues for graduate classes at Columbia University and New York University.