www.pipelinepub.com
Volume 18, Issue 2

Going Beyond the SOC

By: Sam Jones

According to the FBI, the number of cyberattacks reported to its Cyber Division is up 400 percent compared to pre-pandemic levels, and attacks are getting worse. From financial sites to healthcare sites to government sites to supply chain industries, no one is safe from these attacks. The traditional defense against these threats is the Security Operations Center (SOC)—a room full of analysts watching for security alerts on TV screens—but this defense isn't working very well. For proof, just ask the cybersecurity teams at Continental Pipeline, Target, TransUnion, or any of hundreds of other companies that have experienced significant attacks.

How a SOC works (and doesn't)

The operating theory behind a SOC is that if you collect enough data across the enterprise through various IT and security tools, then use analysis platforms to rank and visualize the alerts from different tools, then finally deploy a tiered analyst team to manage and respond to the alerts, then surely, most or all cyberattacks will be spotted quickly and handled before they cause real damage. Real-world experience tells us otherwise.

There are several reasons why the SOC model is broken. In the first place, all those security tools issue lots of alerts—thousands of them, many of which are benign. For example, a user who's typically in the office logging in from a remote location could trigger an alert, or a user logging in outside of business hours could trigger an alert. Security analysts must deal with hundreds or thousands of these "false positive" alerts each day.

Figure 1: A SOC in action

Another reason why SOCs fail is that each of the discrete cybersecurity tools in use has its own data format and often, its own console, and ultimately only depicts a single aspect of the organization's security posture. In today's world, many complex cyberattacks occur through two or more vectors. It's not just somebody banging against a firewall; it could be a phishing attack through email, or a virus downloaded during a routine program update (as with the SolarWinds attack). The problem is that in a SOC, nobody natively sees the whole picture—that picture must be manually correlated across thousands of alerts by teams of analysts. Because this process is manual, it does not allow for robust automation, nor does it allow every alert to get attention.

So, there are too many alerts, too many tools, and not enough automatic data correlation among tools. But there's also another problem: not enough analysts. A global study of cybersecurity professionals by Information Systems Security Association (ISSA) and industry analyst firm Enterprise Strategy Group (ESG) reports that under-investment in cybersecurity tools, combined with the challenge of additional workloads for analysts, is causing a skills shortage that's leading to unfilled jobs and high burnout among information security staff. And that also drives analyst costs up: a top-tier cybersecurity analyst can earn $200,000 per year.

Of course, all of this is happening in a world where cyberattacks are growing more sophisticated and numerous by the month.

SOCless—another way

But what if companies abandoned the SOC idea? What if they distributed their cyber-defenses geographically and to a team of infrastructure experts? What if a platform automated away the mundane work of responding to low-priority alerts and the complex work of correlating across all IT and security tools? What if analysts spent their time proactively looking for threats and implementing best practice policies? What if alert fatigue didn't exist? Is this possible?

It is. We can look to software development teams for an example of how it might work. In DevOps, a modern approach to software development, the best software companies in the world don't line up their developers in rows in one room. They have systems that allow asynchronous

collaborations from distributed people around the world. But there's a lot more to it than just where people sit.

In DevOps, innovation and bug-fixing is an ongoing, 24/7 operation built on top of continuous integration and continuous delivery (CI/CD) systems. Modern CI/CD allows developers to focus on building and enables the smallest of teams to build market-defining products. Mundane and complex tasks are fully automated in CI/CD, and developers are required to emplace proactive testing for all features they roll out. This significantly reduces errors and bugs in the systems, which allows developers to focus on what matters most.

The traditional work of a SOC is pitting a dedicated team of humans against thousands of alerts. But premier technology companies have adopted a new model: trusted, well-documented, high-fidelity alerts get attention, but most alerts can be ignored because of automation. The most advanced cybersecurity platforms automatically send routine alerts to the infrastructure or application owner responsible for that particular area—whether it's a firewall, an end user, an application or a server—along with a set of recommended responses. As Alex Maestretti (current CISO at Remily, former engineering manager at Netflix, where the SecOps team is SOCless) put it, this is what is meant by SOCless: decentralizing alert triage to system experts. The solution to alert fatigue isn't more humans or more data, it's robust autonomous systems with decentralized processes.

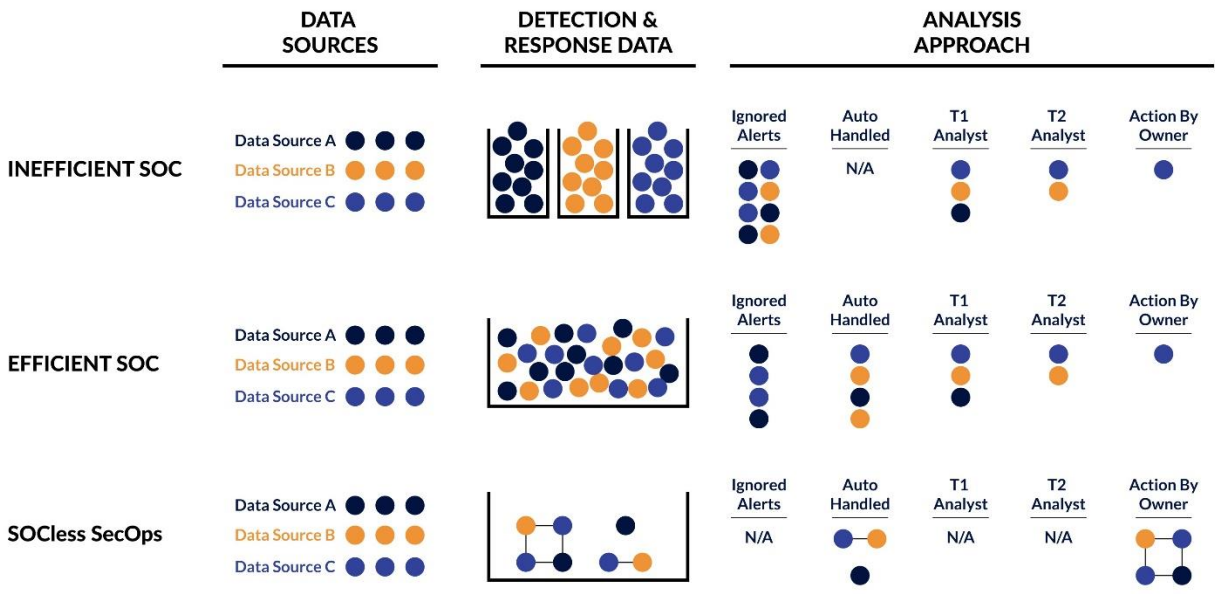

Figure 2: SOCless in practice compared to SOC-based approaches to SecOps
click to enlarge

Migrating to SOCLess

To make this SecOps model work, the security department needs people continuously contributing meaningful policy changes, detection strategies and playbooks, not staring at monitors looking for alerts. It takes work and commitment to get to that state, but if analysts are always monitoring alerts, they'll never get ahead of the problem. To enable proactiveness, security teams need the CI/CD equivalent for security infrastructure.

The first requirement is to have core risk management controls with hygiene best practices easily applied. One prime example of this is the thorough implementation of zero trust; this not only improves your security posture but also reduces alerts and noise, thereby simplifying the data problem. The second requirement is a cybersecurity detection and response platform where strategies and playbooks can be rapidly deployed. Rapid deployment and configuration are paramount: the time from detection and response idea to production deployment should be as close to zero as possible. Any detection and response platform that supports this will be easy to use and have significant out-of-the-box content, including AI- and machine learning-based detections, because rules don't cut it.

Going SOCless takes more than technology, however. It takes a committed team and reimagined processes—getting comfortable with significant automation, having infrastructure owners receive relevant alerts directly, and dedicating majority time to proactive security work. There will always be a need for people, however, and for many enterprises, augmenting internal personnel with a managed security service provider is a cost-effective way to stay proactive. An enterprise does need people to ensure that the right strategies are continuously deployed, and an MSSP with a co-managed deployment of a detection and response platform enables enterprises to scale up support as needed. Like enterprises have turned to the cloud for as-a-service offerings, they can turn to MSSPs for SOC-as-a-service offerings. This will aid many in completing the internal SOCless transition.

By taking a good look at distributed DevOps functions and mapping that to distributed security operations (SecOps), companies can start to get ahead of the hackers in terms of spotting and remediating complex attacks. It takes a real change in perception to pull it off, but many of the biggest and most advanced companies on the planet have already gone SOCless. Maybe it's time every other company did, too.