Get Maximum Value from Your SIEM

WITH TRUSTWAVE CO-MANAGED SOC

Trustwave®

Security controls, network infrastructure, applications, and cloud platforms all provide a plethora of logs and telemetry that can be key to identifying and understanding cyber-attacks. These logs and alerts come in fast and furious, and many organizations have chosen a security information and event management (SIEM) system as their central tool for collecting, analyzing, and driving the operational side of detecting threats. But a SIEM is only truly effective if it's well-configured, managed, and monitored 24×7.

It's rare that an organization has enough security expertise on hand to dedicate to SIEM operations. To augment their internal staff, most look to partner with a security service provider. But it can quickly become overwhelming trying to decide which sort of provider, and which specific service, is the best bet for getting the most value out of a SIEM investment.

This guide will help you navigate the various SIEM management provider options, including a newer entrant, the Co-Managed SOC service. Read on to learn how a Co-Managed SOC will help you maximize your SIEM investment, eliminate active cyber threats, and improve the productivity of your in-house security team.

Defining a SOC

Before diving in, let's establish up front what we mean by a SOC, or Security Operations Center. A SOC may or may not refer to a physical center where security personnel work 24×7. Few companies have the resources required to fund such an operation, especially given experienced security personnel are in such short supply.

What a SOC does include is a set of security capabilities, generally including the mission of detecting and responding to cyber threats to the organization. Other security elements may well feed into that core mission, including vulnerability management, antivirus, and the like. But at its core, the SOC is charged with cyber threat detection and response.

SIEM discussion

The core tool SOC personnel rely on in that effort is a SIEM. SIEMs are powerful tools for solving a complex security problem: collecting the right telemetry from your infrastructure, including cloud applications, to effectively monitor for cyber threats.

The complexity of that security problem extends to the SIEM itself. No SIEM is plug and play, or "set it and forget it." To be effective, the SIEM must be properly configured, targeting the most appropriate use cases for your specific organization. A SIEM that simply collects every possible alert will quickly overwhelm those charged with monitoring it, causing runaway operational costs without effective outcomes. Given that, most organizations benefit from having third party security consultants help with the initial configuration.

Even after it's properly configured, a SIEM requires constant attention, including maintaining the health of data feeds, tuning use cases, and investigating the outcome of those use cases. Many organizations will want or need to do all of this 24×7.

Here again, not every company has the resources to take on that job, but it's a crucial one. A partially implemented SIEM can be more of a liability than a benefit because it's just constantly churning out threat alerts. With no one to ferret out the false positives you are in constant fire drill mode, left chasing a series of harmless alerts, or worse, ignoring impactful ones.

Gartner makes the case for managed SIEM services

While companies clearly need a SIEM, most typically don't have the expertise in-house to effectively deploy and manage them. The solution: hiring that expertise, in some form of managed SIEM service.

In its 2022 "Market Guide for Managed SIEM Services," Gartner nicely laid out the case for such services, saying: "Buyers who have invested in SIEM technology use Managed SIEM services to derive more value. They can use Managed SIEM services to get assistance with decisions around strategy, architecture, maintenance, development, or support. This approach leads to better security operations results."

Gartner also noted: "Security teams have a wide range of complex responsibilities and benefits. Outsourcing certain elements of security delivery helps ease the workload of the security teams and provides resources so the team can focus on operational requirements."

I've Got SIEM. Do I Need Managed Detection and Response (MDR)?

If you've already got a SIEM, and are considering a Co-Managed SOC service, you may be wondering whether you need to be concerned about adding a Managed Detection and Response service as well. It's an excellent question, but the short answer is yes, MDR can enhance your response capabilities and overall cyber threat protection.

MDR is great at detecting high-confidence threats, because the endpoint detection and response (EDR) technologies MDR works with give you good visibility into what's happening on an endpoint. You can quickly see the various layers of the attack and their impact. In short, MDR provides a great immediate improvement in your security posture. It's one of the first services Trustwave recommends customers implement.

Employing MDR takes your security program to the next level because it gets telemetry from hundreds of sources throughout your environment as well as in the cloud. MDR can quickly integrate third party technologies through bi-directional APIs, incorporate additional intelligence sources for higher fidelity threat detection, conduct threat hunting and response at the endpoint, and more.

Layering MDR and a managed SIEM service together gives you a broader, complementary picture of the security landscape with real-time endpoint threat containment and response capability.

Types of Managed SIEM Services

With interest high in managed SIEM, it stands to reason providers are coming up with variations on the theme. To date, they tend to fall into one of two camps: Managed SIEM and SOC-as-a-Service (SOCaaS).

Managed SIEM

Managed SIEM services help organizations operate and manage the complexities of their SIEM. Like similar services for firewall or endpoint detection and response (EDR) tools, it helps customers manage their SIEM and may include alert monitoring and light investigation of security incidents. While the exact mix of services will vary by provider, most managed SIEM services include SIEM licensing, deployment and configuration, maintenance of the SIEM platform, and perhaps ongoing optimization and tuning. Notably, managed SIEM offerings often do not include 24×7 alert monitoring.

SOC-as-a-Service

SOC-as-a-Service (SOCaaS) typically means the vendor assumes ownership of the SIEM infrastructure and product licensing. This can be a turn-key solution for smaller organizations that have neither a SIEM nor a security operations center (SOC). Companies simply direct all SIEM data to their provider, who assumes responsibility for correlating alerts, interpreting the data, and identifying security problems amid the numerous false positives. In many cases, SOCaaS refers to a traditional MSSP model, where the provider monitors its own threat detection software.

Co-managed SOC

Another approach to managed SIEM is one that's intended to help customers derive more value from their SIEM investments over time. That is the intent behind the Trustwave Co-Managed SOC offering.

With Trustwave, you'll start your Co-managed SOC experience with a consultative transition and transformation project. SIEM and SOC consultants with decades of collective experience will work hand-in-hand with your team under the coordination of a Trustwave Project Manager to assess your current capabilities and priorities, build a plan for transition and transformation, and tune and advance your SIEM use cases based on Trustwave's extensive library of field-proven and industry-aligned use cases.

As the service approaches steady-state operations, you'll begin working with one or more named Cyber Success Team experts for the life of the service. These experts work with you to understand your business needs and operational context. They will continuously tune your SIEM for optimal performance and tailor it for the specific use cases that are most important to your organization. They seamlessly integrate with your security operations team, increasing their productivity and freeing up resources.

You'll also benefit from Trustwave's 24×7 global threat monitoring, which performs alert triage, investigations, and response prioritization, to help you quickly address and eradicate actual threats instead of chasing false positives.

Trustwave uses a closed loop method to SIEM management. It's an iterative approach to constantly learn from the alerts your SIEM produces and tune it to become increasingly effective at homing in on the most important ones. What's more, whatever improvements we make are yours to keep, even in the (unlikely!) event you choose to end your engagement with Trustwave.

4 Steps to Improved SIEM Management

In short, Trustwave Co-Managed SOC maximizes your SIEM investment with proven processes, use cases, and ongoing experience that address four crucial elements:

- **Consult and Plan:** Your named security experts create a roadmap specifically for your business, create personalize use cases, and provide predictable cost and capacity estimates.
- **Build and Onboard:** Our proven methodology gets you up and running quickly, to accelerate time to value and align resources for hybrid security operations.
- **Manage and Monitor:** Trustwave acts as an extension of your team, providing 24×7 SIEM management and incident monitoring informed by SpiderLabs global threat intelligence
- **Advise and Tune:** Your named experts apply their decades of experience to continuously tune and optimize your SIEM, and your security policies, to improve your cyber resilience.

And Trustwave works with SIEMs most companies already have, namely:

Microsoft Sentinel, LogRhythm SIEM Platform, IBM QRadar, and Splunk Enterprise Security.

To learn more about the Trustwave Co-Managed SIEM offering, visit: **trustwave.com**