Trustwave®

Trustwave Co-Managed SOC Service

TAKE BACK CONTROL OF YOUR SECURITY OPERATIONS.

Benefits

- Identify active threats with 24×7 real-time global threat monitoring
- Minimize the complexity of managing a SIEM
- Avoid alert fatigue by removing noise for higher fidelity
- Augment your team with tenured SIEM & SOC experts
- Accelerate the productivity of your security operations team
- Extract greater value from your SIEM investments
- Retain ownership of all improvements to your SIEM

A SIEM, or security information and event management system, is a core tool for many security operations teams and security operations centers (SOC). SIEMs have numerous advantages; however, it doesn't take long to realize that it's far from a turn-key solution.

With the relentless onslaught of potential threats to an organization, security teams are often lured to send more telemetry and logs to the SIEM with the assumption that correlating more logs across their environment will produce better visibility and threat detection.

In practice, a "collect everything" strategy for the SIEM does produce more alerts, but it comes with a high rate of noise, which requires human investigations to separate the true threats. This quickly becomes overwhelming for a security operations team to manage, putting downward pressure on productivity levels. As alert fatigue sets in, many alerts often go unresolved, which can result in increased exposure to risk. Additionally, the higher volume of logs you feed your SIEM, the more it will cost you to operate.

SIEMs are complex and require ongoing maintenance and optimization by highly skilled security engineers to help security analysts make sense of the output and avoid a flood of alerts.

Realizing the promised benefits of a SIEM investment—and its close counterpart SOAR (security orchestration automation and response)—becomes elusive, at best, without the proper resources and operational processes in place to make it work as intended.

Managed SIEM vs Trustwave Co-Managed SOC

To address these challenges, organizations are turning to managed security service providers (MSSPs) to augment their resources. SIEM related services are commonly referred to as Managed SIEM, as defined by Gartner.

However, it's not always enough to simply outsource management and monitoring without first considering an internal assessment to help identify any capability gaps, operational constraints, or even current configurations, all of which contribute to the success or failure of your security mission.

Trustwave Co-Managed SOC service includes Managed SIEM (manage & monitor), but also extends to include an end-to-end consultative approach to maximize the value realized from your SIEM and SOAR investments.

Guided by decades of cumulative knowledge from global client engagements, we've sharpened our enterprise-proven processes and operational intelligence to deliver unrivalled results for our clients.

A Proven Approach for Unrivalled Results

We know what great looks like for SIEM, SOAR, and security operations. We know how to accelerate your operations to great, regardless of where you are in terms of current capabilities, operational readiness, and maturity.

We've built flexibility and personalization into our co-managed approach to augment your security team and operations where you need it the most. Our proven end-to-end approach will help you transform your security operations through four major activity areas:

Consult & Plan

The first phase in our engagement starts with a mature, consultative jumpstart activity that ensures your SIEM and SOAR technologies are implemented and deployed appropriately, with use cases that make sense and work effectively.

We work with you to determine if you are at risk of runaway costs from unnecessary telemetry sent to the SIEM and/or cost from excessive storage policies. Furthermore, we'll personalize use cases from our extensive use case library, and build custom use cases, to align to the goals of your organization and security operations.

You'll have a plan with predictable capacity and cost management expectations, and a road map for ongoing use case improvements. More importantly, you retain ownership of all improvements we make in your SIEM and SOAR on your behalf. We don't hold your SIEM or data hostage, unlike most providers.

Build & Onboard

During this phase, we walk you through implementation, resource alignment, and plans for ongoing testing. You'll begin to develop the appropriate documentation for your organization including building the right security policies, playbooks, and incident response plans to go along with the detection output from your newly tuned SIEM.

We'll introduce you to the Trustwave Cyber Success Team—tenured and highly experienced SIEM/SOAR and SOC experts—who'll work with you for the life of the service term.

Manage & Monitor

Once you're in steady state, Trustwave will conduct 24×7 global, real-time threat monitoring. We also manage your SIEM device for security updates, ongoing health, and uptime.

The Trustwave security analysts and investigators monitoring your environment will be armed with SpiderLabs curated threat intelligence to assist them in identifying known threats, reducing false positives, and continuously eliminating noise.

Your security operations team will only receive confirmed, actionable incidents that require immediate response or direct action.

Advise & Tune

As we've established, SIEMs are complex and require highly skilled experts to keep them operating and performing to expectations. As part of steady state operations, Trustwave will provide ongoing advisory and tuning.

Your Trustwave Cyber Success Team security advisor will be a named expert who'll be deeply familiar with your organization and have an industry-wide perspective on the cyber threats that may impact your business.

Armed with this perspective, advisors will conduct ongoing use case tuning and optimization, review changes to your architecture, recommend updates to security policy, provide custom reporting, and collaborate with you frequently to review the state of your operations.

During critical incidents, your advisor can tap a global network of peers to force-multiply response efforts for a comprehensive, personalized solution to the most difficult cyber challenges.

Comprehensive Threat Response with MDR

In addition to Trustwave Co-Managed SOC services, clients often include Trustwave Managed Detection and Response (MDR) service for comprehensive threat response, threat hunting on the endpoint, remote incident response, and more.

Trustwave MDR gives security analysts the ability to investigate and respond to threats directly on endpoints and in multiple security controls. Analysts are able to conduct advanced threat hunting and investigate the impact, or blast radius, of a threat more completely, allowing for faster responses with higher confidence.

Be sure to ask us about the added benefits of Trustwave MDR with Trustwave Co-Managed SOC.

Support for Best of Breed Technology

Microsoft

Get started today:
https://www.trustwave.com/en-us/services/co-managed-soc

Trustwave®

www.trustwave.com

CMS_0922