



Trustwave Co-Managed SOC Service

REDUCE ALERT NOISE BY UP TO 90%. TAKE BACK CONTROL OF YOUR SECURITY OPERATIONS.

Benefits

- Reduce alert noise by up to 90%
- Identify active threats with 24x7 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, 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, although a "collect everything" strategy for the SIEM does produce more alerts, it also comes with a high rate of noise which in turn requires a human to investigate to separate out 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 may 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.

For some, without the proper resources and operational processes in place, realizing the promised benefits of a SIEM investment becomes elusive, at best.

Trustwave Co-Managed SOC

To address these challenges, organizations are turning to Co-Managed Security Monitoring Services, as [defined by Gartner](#), to augment their resources.

Trustwave Co-Managed SOC service provides 24x7 real-time global threat monitoring and a unique end-to-end consultative approach to help your organization maximize the value from your SIEM 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 and security operations. We know how to accelerate your SecOps 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 approach that ensures your SIEM is implemented and deployed appropriately, with use cases that make sense and work effectively to defend against threats to your organization.

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, or build custom use cases if required, to align to the goals of your organization and security operations.

You'll have a better view of your cost expectations, and a road map for ongoing use case improvements. More importantly, you retain ownership of all improvements we make in your SIEM 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 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 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 24x7 global, real-time threat monitoring. We also manage your SIEM 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, threat hunts, to improve detection content, and reduce false positives while 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, unlimited remote threat response, and more.

Trustwave MDR gives security analysts the ability to investigate and respond to threats directly. Analysts are able to investigate the impact, and blast radius, of a threat more completely leveraging XDR/EDRs, and allowing for faster responses with higher confidence.

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

Security Colony

As part of the Trustwave Co-Managed SOC services, you'll gain instant access to Trustwave Security Colony, a powerful resource with tools to help proactively improve your security maturity at your own pace.

Security Colony is a unique cybersecurity collaboration platform which gives you access to dynamic assessments and daily reports of your Vendor Risk, Ransomware Readiness, Security Maturity, Breach Monitoring, and more, with actionable guidance that tracks your progress over time.

You'll have access to millions of dollars of Trustwave consulting output from years of real client engagements to help you solve the most common security challenges. Additionally, you'll have access to the Security Forum where you can engage with active members or directly ask Trustwave experts a question.

Support for Best of Breed Technology



Get started today:

<https://www.trustwave.com/en-us/services/co-managed-soc>

