LevelBlue

Co-Managed SOC Service

Reduce alert noise by up to 90% and take back control of your security operations.

A SIEM, or security information and event management system, is a core tool for many security operations teams and security operations centers (SOC). While SIEMs offer significant advantages, it quickly becomes clear that they are far from turnkey solutions.

Faced with a relentless onslaught of potential threats, security teams are often tempted to send increasing volumes of telemetry and logs to the SIEM, assuming that collecting and correlating more data will automatically improve visibility and threat detection.

In practice, a “collect everything” strategy generates more alerts but also significantly increases noise. Each alert requires human investigation to distinguish true threats from false positives, which can quickly overwhelm security operations teams and place downward pressure on productivity. As alert fatigue sets in, many alerts go unresolved, increasing organizational risk exposure. At the same time, higher log volumes directly drive up SIEM operating costs.

SIEMs are complex and require ongoing maintenance and optimization by highly skilled security engineers to ensure security analysts can interpret output effectively and avoid alert overload.

Without the proper resources and operational processes in place, realizing the full value of a SIEM investment can be elusive at best.

LevelBlue Co-Managed SOC

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

LevelBlue Co-Managed SOC service provides 24×7 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 unrivaled results for our clients.

A proven approach for unrivaled results

We know what excellence looks like in SIEM and security operations. We help accelerate your security operations to that level, regardless of your current capabilities, operational readiness, or maturity.

Benefits

- Reduce alert noise by up to 90%
- Identify active threats with 24×7 real-time global threat monitoring
- Minimize the complexity of SIEM management
- Avoid alert fatigue by removing noise and increasing alert fidelity
- Augment your team with tenured SIEM and SOC experts
- Accelerate security operations productivity
- Extract greater value from your SIEM investments
- Retain ownership of all improvements to your SIEM

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

Consult and Plan

The first phase of our engagement begins with a mature, consultative approach to ensure your SIEM is implemented and deployed appropriately, with use cases that that are practical, effective, and aligned to defending your organization against real threats.

We work with you to assess whether you are at risk of runaway costs caused by unnecessary telemetry sent to the SIEM or from excessive storage policies. We also personalize use cases from our extensive library, or build custom use cases when needed, to align with the goals of your organization and security operations.

You’ll gain greater visibility into your cost expectations and a road-map for ongoing use case improvements. More importantly, you retain full ownership of every improvement we make to your SIEM on your behalf. We don’t hold your SIEM or data hostage, unlike most providers.

Build and Onboard

During this phase, we guide you through implementation, resource alignment, and plans for ongoing testing. You’ll begin developing the documentation your organization needs, including security policies, playbooks, and incident response plans aligned to detection output from your newly tuned SIEM.

We’ll also introduce you to the LevelBlue Cyber Success Team – tenured and highly experienced SIEM and SOC experts – who’ll work with you for the life of the service term.

Manage and Monitor

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

The LevelBlue security analysts and investigators monitoring your environment are equipped with LevelBlue SpiderLabs-curated threat intelligence to identify known threats, conduct proactive threat hunting, 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 and Tune

As established, SIEM platforms are complex and require highly skilled expertise to operate and perform as expected. As part of steady-state operations, LevelBlue provides ongoing advisory support and continuous tuning.

Your LevelBlue Cyber Success Team security advisor is a named expert who is deeply familiar with your organization and brings an industry-wide perspective on the cyber threats that may impact your business.

With this perspective, your advisor conducts ongoing use case tuning and optimization, reviews changes to your architecture, recommends updates to security policy, delivers custom reporting, and collaborates with you regularly to asses the state of your operations.

During critical incidents, your advisor can draw on a global network of peers to force-multiply response efforts , delivering a comprehensive and personalized approach to resolving the most complex cyber challenges.

Comprehensive threat response with MDR

In addition to LevelBlue Co-Managed SOC services, clients often include LevelBlue Managed Detection and Response (MDR) services for comprehensive threat response, unlimited remote response capabilities, and added operational value.

LevelBlue MDR enables security analysts to investigate and respond to threats directly. Analysts can more fully assess impact and blast radius by leveraging XDR and EDR technologies, resulting in faster response times and higher confidence outcomes.

Ask us about the additional benefits of combining LevelBlue MDR with LevelBlue Co-Managed SOC.

Security Colony

As part of LevelBlue Co-Managed SOC services, you gain immediate access to LevelBlue Security Colony, a powerful platform designed with tools to help you proactively improve your security maturity at your own pace.

Security Colony is a collaborative cybersecurity resource that provides dynamic assessments and daily reporting across vendor risk, ransomware readiness, security maturity, and breach monitoring, along with actionable guidance that tracks your progress over time.

You’ll also benefit from millions of dollars in LevelBlue consulting output drawn from years of real client engagements, helping you address common security challenges more efficiently. In addition, the Security Forum enables you to engage with active members and directly ask questions of LevelBlue security experts.

Support for best-of-breed technology

Microsoft paloalto NETWORKS splunk> LogRhythm