LevelBlue

Customized SIEM Optimization Program

Enhance SIEM detection capabilities to stay ahead of evolving cyber threats.

SIEMs are only as effective as their analytic rules. Without well-defined rules, security teams face alert overload and false positives, while real threats can slip through the cracks.

A strategic, use case-driven approach helps security teams focus on what truly matters, ensuring that detections align with real-world attack patterns and organizational risk priorities.

The LevelBlue Customized SIEM Optimization Program (CSOP) helps you maximize the value of your SIEM platform by aligning detection content with real-world threats, business priorities, and operational risk. CSOP provides structured, custom use case and analytic rule ("use case") development and implementation, enabling proactive threat detection tailored to your unique environment.

Designed to drive continuous SIEM improvement, CSOP helps advance the maturity of your SIEM environment by keeping content aligned with emerging threats, evolving attack techniques, and changes in your infrastructure or operations.

The importance of custom SIEM use cases

Every organization has a unique threat landscape, yet many rely on out-of-the-box SIEM uses cases that may not reflect their specific risks, environment, or compliance requirements. Custom use cases bridge this gap by tailoring detections to industry threats, business processes, and attacker tactics, reducing noise and improving response times. By continuously refining use cases and aligning them with evolving threats, security teams can maximize their SIEM's value – transforming raw data into actionable intelligence that drives faster, more effective threat detection and response.

However, developing and maintaining custom use cases comes with challenges. Many organizations struggle with a lack of expertise in mapping specific business risk to relevant detections or with the ongoing effort needed to fine-tune and update use cases as new threats emerge. Furthermore, aligning SIEM use cases with frameworks such as MITRE ATT&CK requires both technical depth and a solid understanding of evolving attack tactics, which can be a hurdle for teams that are already stretched thin with day-to-day operations. As a result, organizations fail to fully leverage their SIEM's potential, leaving them vulnerable to undetected threats.

LevelBlue can help you navigate the challenges of SIEM use case development and effective threat detection and response.

Benefits

- Access team of LevelBlue consultants with deep subject matter expertise in SIEM use case development, threat detection, and security analytics.
- Identify and address specific threats to your organization's environment.
- Reduce noise and alert fatigue by focusing on high-fidelity alerts tied to real risks.
- Quickly deploy use cases to counter emerging threats and attack patterns.
- Tailor use cases to align with security policies, priorities, and compliance needs.
- Gain strategic guidance to continuously refine detection use cases.
- Layer detection with unique threat intelligence and research from LevelBlue SpiderLabs.

The approach

LevelBlue develops, implements, and fine-tunes SIEM use cases tailored to your environment:

- **Discovery and Planning:** Understand your specific security objectives and existing SIEM environment. This includes facilitating a kick-off meeting, establishing the project governance and oversight process, and collecting relevant information on SIEM capabilities.
- **Use Case Analysis and Development:** Design and develop use cases aligned with your security monitoring requirements. This includes analyzing the SIEM and threat monitoring environment (e.g., existing use cases), designing custom use cases, and conducting feedback sessions to ensure alignment.
- **Use Case Implementation:** Implement use cases and tune configurations to optimize effectiveness. This includes implementing use cases in the SIEM environment, tuning alerting to within prescribed thresholds, and documenting use cases for integration into operational workflows.
- **Threat Monitoring Advisory:** Assess SIEM capabilities to provide recommendations for continuous improvement. This includes supporting updates to the use case catalogue, outlining recommendations for future improvements, and facilitating workshops on topics of interest.

Flexible engagement options

LevelBlue provides a tailored approach to developing use cases and enhancing threat detection – on your terms.

Base Package: Maximize your SIEM's value with tailored solutions that evolve with your business. It includes:

- 3-month term
- 80 hours of consulting support
- 10 hours of project management support

LevelBlue will collaborate with your team to align SIEM capabilities with your security goals and priorities. CSOP can be extended beyond 3 months as required, and additional hours may be purchased to support evolving requirements.

Support leading SIEM platforms

LevelBlue supports a range of industry-leading SIEM platforms – including Microsoft Sentinel, Devo, and Splunk – and delivers value through tailored use case engineering, expert insights, and efficient onboarding.

LevelBlue's goal is to enhance threat detection, streamline response, and maximize the value of your SIEM investment.

LevelBlue Managed Security Services

CSOP focuses on complementary, yet distinct areas compared to the Information Security Advisor (ISA) you may have access to as part of LevelBlue Managed Security Services. The ISA ensures that the SIEM remains healthy, operational, and up to date, providing the essential baseline stability that enables you to trust the SIEM for reliable and effective monitoring. This could include developing and implementing tactical uses cases, such as in response to an immediate threat requiring rapid detection. CSOP extends the capabilities of the ISA by providing structured, ongoing enhancement of SIEM threat monitoring analytics through tailored use case development and implementation.

Ultimately, CSOP provides a proactive approach to threat monitoring customization.