Managed SIEM service.

Solutions brief

verizon

The benefits of Managed SIEM.

In recent years, the adoption of new technologies has changed the way organizations work. Companies are generating and protecting more data than ever, and storing it in the cloud and across multiple devices. This is fundamentally changing the IT security requirements of organizations. Monitoring the security compliance of systems and devices is no longer sufficient – enterprises require comprehensive cyber detection capabilities and intelligence to recognize and mitigate potential threats.

Traditional Security Information and Event Management (SIEM) tools are used to collect event data generated by your organization's IT infrastructure. This information is then interpreted in an enterprise context by correlating event data with other sources of contextual information, to identify anticipated and unanticipated actions that might indicate misuse of business assets, or result in a potential business risk.

With Verizon's Managed SIEM services, your organization will benefit from our intelligence gained from providing security services for 25 years, while still retaining the advantages that a dedicated SIEM solution offers in terms of data control. This combination helps you to quickly establish an operational SIEM service and achieve a level of security monitoring that goes beyond what you can provide in-house.

Why choose Verizon's Managed SIEM?

- The presence of dedicated SIEM technology on your premises allows for seamless integration and flexibility.
- A tailored security monitoring rule base, focused on your organization's threat landscape.
- Continuous monitoring of your security events and incidents by our experienced team of experts.
- Extensive intelligence gathering and application beyond the boundaries of your environment.
- Security operations expertise from a leading provider, facilitating and managing the people and processes.
- 24x7 health and device management, and security incident escalation.

A proactive approach to security.

Managed SIEM is a continuous security monitoring solution for rapidly identifying security threats, helping you respond to potential compromises before they materialize into serious data breaches or cause major harm to your critical business infrastructure. Our service provides a fast response, expert incident management, access to comprehensive security intelligence and detailed reporting capabilities.

We actively gather and digest security threat intelligence from both internal and external sources, to proactively identify, analyze and assess possible impacts on your IT infrastructure. These findings will be made available to you through the Managed SIEM Content Library, empowering you with the knowledge and tools you need to stay secure.

Security monitoring and incident escalation.

Our Managed SIEM service includes 24x7 monitoring of your SIEM alerts. Verizon's Security Operations Center (SOC) analysts will interpret the information generated in relation to your business context and assess the potential impact on your environment. If they determine that these alerts are valid, they will escalate them according to their classification within the Service Level Agreement (SLA).

Our 24x7 health monitoring and device management service will help to keep your log management and security monitoring architecture up and running, and collect and analyze log evidence on a continuous basis.

Our commitment to you.

We understand that you expect a predictable and measurable quality of service. Our SLAs clearly specify what you can expect from our Managed SIEM services and by when. We also publish quality metrics, fully document escalation procedures and define the responsibilities of each party.

Read the next page to learn more about the specific components of our Managed SIEM service.

Managed SIEM Intelligence and Improvement Services.

Managed SIEM Intelligence and Improvement Services provide you with access to a body of knowledge based on our security expertise and intelligence. These insights can be used to maintain, improve or mature your security monitoring capabilities. You'll have access to Verizon's best practices, recommended architecture and guidelines for implementing and operating SIEM analytics.

We also evaluate SIEM vendor upgrades and updates, to analyze their impact and determine if they pose any reliability problems. Only after a positive outcome will the patches be released for installation. This testing prior to deployment helps reduce the potential impact to your service availability and performance.

Managed SIEM Content Library.

The Verizon Managed SIEM Content Library serves as the foundation for our Managed SIEM analytics. The library consists of a collection of predefined and proven SIEM content. Each use case is built around a set of event monitoring scenarios that can be implemented on the SIEM infrastructure using one or more correlation rules, filters, report definitions and/or dashboards.

Verizon will provide recommendations to maintain and improve the running SIEM content, as new threats and changes arise in the environment. When this happens, you'll be sent content library update notifications. These contain recommendations and internet links with additional information, to aid your understanding of the risks and mitigation strategies.

Security Services Advisor.

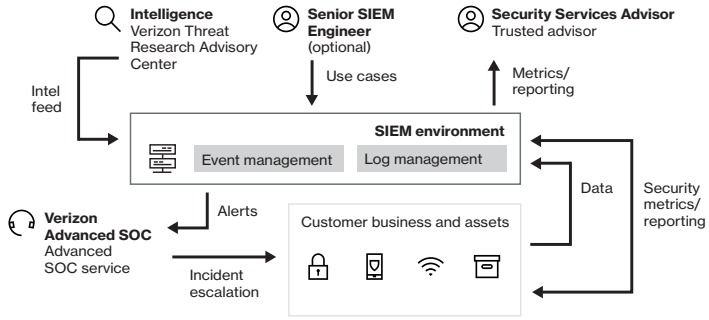
We'll appoint you with a trusted Security Services Advisor, who will host regular security review meetings. All customers have access to security advisors who work across several accounts, but your own dedicated advisor can be contracted at an additional charge.

Your advisor will provide you with:

- Training on the customer portal
- Communications and security advisories
- Help with service issues and service credit requests
- Updates on release and service features, if applicable
- Recommendations for improving your security posture

Senior SIEM Engineer (optional).

A Senior SIEM Engineer can work with your organization to review your platform configuration and running content set, and provide recommendations on use case creation as well as dashboards, tuning and log source tuning. They can also implement any changes to the running SIEM content after impact analysis and validation.



Verizon's Managed SIEM service collects and correlates event data to identify potential security threats to your business.

Verizon Security Operation Centers.

Our Managed SIEM services are delivered from our regional SOCs, where our security analysts deliver monitoring and management services on a 24x7 in-region basis.

Our security experts will continuously monitor your SIEM alerts, and escalate any incidents requiring immediate action to your nominated security personnel. They will analyze all SIEM-generated alerts for their potential impact on your business.

They'll also generate and interpret different reports to proactively identify trends and potential anomalous behavior, before they become serious threats or security breaches.

We're also responsible for the lifecycle management of your SIEM content. This will involve interacting with your security teams on a daily basis, to evaluate and help maintain the efficacy and validity of the implemented SIEM content set.

Verizon Threat Research Advisory Center.

The Verizon Threat Research Advisory Center is an additional resource that strengthens our ability to draw conclusions and provide security recommendations to you with confidence. The Verizon Threat Research Advisory Center helps to aggregate sources of threat data, using our expansive IP backbone and extensive forensic caseload. We then normalize this data, analyze it and produce actionable intelligence.

The Verizon Threat Research Advisory Center provides three types of intelligence – strategic, tactical and applied intelligence. Strategic intelligence provides information about attack tactics and methods. Tactical intelligence provides information relating to specific indicators of compromise. Applied intelligence brings these two sources together, to recognize potential threats to your system. Collectively, these three levels of insight help your organization to prepare for, recognize and respond to cyberattacks effectively.