Lumen® Managed SIEM Frequently Asked Questions

Get answers to the most frequently asked questions about our Lumen Managed SIEM service

Overview

Q **What is Lumen Managed SIEM?**

Adopting trends such as work-from-anywhere and cloud computing have increased vulnerabilities to cyber-attacks and data breaches. SIEM platforms provide visibility and control to organizations allowing them to identify who connects to their network. However, several management challenges could jeopardize optimal platform performance.

Lumen Managed SIEM service provides customers with a team of SIEM experts who will provide 24/7/365 system administration, monitoring, and maintenance of their SIEM software. Our SIEM team has the proper skill set required to get your SIEM up and running quickly and optimize your time-to-value so you can start seeing results in the short term.

Q **What is Lumen Managed SIEM used for?**

Configuring, maintaining, and optimizing the SIEM platform could be an overwhelming task for security teams and an expensive decision for organizations. Lumen Managed SIEM grants you access to seasoned security experts with the right skill set to help you deploy and provide 24/7/365 system administration, monitoring, and maintenance of your SIEM platform.

Q **What is included in Lumen Managed SIEM?**

Lumen Managed SIEM empowers your organization by removing the management burden from your internal staff. The service features include:

- 24/7/365 SIEM system monitoring and maintenance
  - Setup and Configuration of SIEM software
  - Patching SIEM software
  - Upgrading SIEM software
  - Monitoring SIEM availability and performance

LUMEN®

- Log Management
  - Enable log ingestion from customer defined log sources
  - Verify that log feeds from all expected log sources are being received as expected
  - Configure and manage log retention and backup per customer policy
  - Recommend changes to log policy to improve efficiency
- Project and Service Reporting
  - Project reporting during onboarding process
  - SIEM Dashboard and Report Creation and Maintenance
  - Quarterly Business Reviews

Q **Which purchasing options are available?**

Lumen Managed SIEM is available in two purchasing options:

- Our experts can leverage the SIEM you already invested (platforms supported IBM QRadar, Splunk, LogRhythm, Microsoft Sentinel, and FortiSIEM)
- Lumen can supply SIEM as part of the service (platform supported IBM QRadar)

Q **Which SIEM platforms are supported by Lumen Managed SIEM?**

Lumen security experts can leverage your existing SIEM platform. Supported platforms include IBM QRadar, Splunk, Microsoft Sentinel, LogRhythm, and FortiSiem.

User Experience

Q **How is Lumen Managed SIEM delivered?**

During the transition phase, Lumen security experts will work with you to gather relevant information including internal operations processes, network architecture, infrastructure configurations, and log management required to transition Customer SIEM system administration functions to Lumen's security engineers.

During the managed operations phase, our team will monitor the SIEM system for availability and performance. If the SIEM becomes unavailable or SIEM performance is degraded, Lumen will use reasonable business efforts to restore availability and performance.

Lumen will monitor log ingestion, including evaluation of log format and verbosity from log sources, loss of visibility, reduction in visible traffic from log sources, and quality of network flow ingestion. Our team will notify the Customer of SIEM upgrade availability or patching and advise on the impact on the service of upgrade installation. Lumen will perform SIEM software upgrades and install patches approved by the customer per the customer's change management process.

Q **Who will deliver the service?**

Managed SIEM is delivered by Lumen's security team, which is formed by seasoned on-shore U.S. based resources with years of experience.

LUMEN®

What happens once I order?

A kickoff meeting will occur after the contract signature to scope out project deliverables and timing. Our team will work with you to develop a project plan to guide and track progress. Regular reviews and progress reporting will occur during the onboarding process.

Additional questions

Do I need a SIEM platform before getting Managed SIEM?

Lumen Managed SIEM has two purchasing options. Our security team can leverage your existing SIEM platform, or Lumen can also supply the SIEM as part of the service (check available platforms per option listed before in this document).

What is the difference between Lumen Managed SIEM and Lumen Virtual SOC?

Managed SIEM and Virtual SOC are closely related services, covering different areas of the threat intelligence, detection, and response ecosystem and complementing each other. Managed SIEM is focused on the platform, such as deployment, health, optimization, and log configuration, and Virtual SOC is centered on event monitoring, alert management, and incident handling.