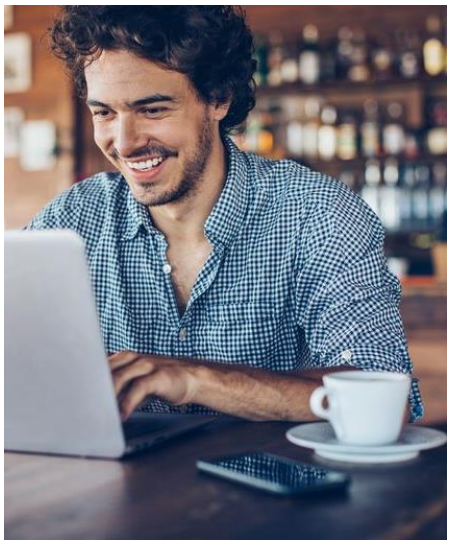
Lumen Virtual SOC Frequently Asked Questions

Get answers to the most frequently asked questions about our Lumen Virtual Security Operation Center service

Overview

Q What is Lumen Virtual SOC?



Cyberattacks are multiplying year after year, and no enterprise is immune. Building and maintaining a Security Operation Center is expensive, not to mention the effort you need to find, train, and retain the right security talent to monitor the tools and trigger threat responses.

Lumen Virtual Security Operations Center services provide 24/7/365 SIEM monitoring and incident handling to detect and analyze cybersecurity threats and incidents. Lumen SOC security experts quickly identify and triage events, fine-tune use cases, apply Lumen's extensive experience learned protecting its network, and take threat intelligence from our Black Lotus Labs® for outstanding incident handling.

Q What is Lumen Virtual SOC used for?

Today's organizations need 24/7/365 SIEM monitoring to detect suspicious incidents and intruders in their network; however, the required resources and effort to perform this in-house are cost-prohibited for most organizations. With Lumen Virtual SOC, our security expert team augments your threat and response strategy and provides around-the-clock SIEM monitoring to help you improve your security posture and align with regulatory compliance requirements without the financial burden of insourced SOC units.

Q What is included in Lumen Virtual SOC?

Lumen provides 24/7/365 SIEM monitoring and incident handling leveraging your SIEM platform. The service features include:

- Supported SIEM standard platforms are IBM QRadar, Splunk, Sentinel, LogRhythm, and FortiSiem.
- 24/7/365 SIEM monitoring and notification: confirm the validity of SIEM Alerts, perform prescriptive analysis, and provide notification according to Run Book.

LUMEN® TECHNOLOGIES

- Use case development and tuning - Lumen has a default set of templated use cases that adhere to the MITRE ATT&CK® framework. These use cases are customized for a Customer environment and applied within the Customer's SIEM platform.
- Run book development and maintenance – including notification process and procedures for handling Alerts and Incidents.
- Deep-dive analytics – Analysis of trends, threats, incident mining and lessons learned, resulting in additional information about the Incident (such as causes and impacts) and expanded remediation recommendations (such as addressing impacted systems, etc.) to be included in the ticket (available in plus and premium packages).
- Incident handling – Identify cause of incidents by conducting analysis of logs, validates priority and recommends remediation actions (available in plus and premium packages).
- Use case Advanced tuning. (available in plus and premium packages).
- Threat hunting – proactive function conducted by a Lumen security analyst who reviews Logs and configurations outside of your SIEM, taking into account current trends, outside of established use cases with the goal of discovering anomalies related to current events (available in premium package).

Lumen Virtual SOC is offered in three package options, with pricing based on maximum amount of monthly incidents and packaged selected by the customer. Standard features vary based on the package selected.

Q Which package options are available?

Lumen Virtual SOC is available in three packages:

- **Essentials:** Includes 24/7/365 SIEM monitoring and notification, use case development and tuning, and run book development and maintenance.
- **Plus:** includes features in essentials package plus deep-dive analytics service, incident handling and use case advanced tuning.
- **Premium:** includes features in plus package plus threat hunting.

Q Which SIEM platforms are supported by Lumen Virtual SOC?

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

User Experience

Q How is Lumen Virtual SOC delivered?

During the transition phase, the Lumen security experts, a team of seasoned U.S.-based resources, will work with you to collect the information required to develop the run book and identify critical use cases. Our security team will log in daily to your SIEM

LUMEN® TECHNOLOGIES

platform and monitor it 24/7/365 for security events. Once an incident is identified, the SOC analyst classifies, triages, and analyzes the event to validate if it is a false positive. True events are prioritized and notified to customers. Our SOC experts analyze logs to isolate incidents and provide deep-dive analytic analysis (trends analysis, threats, ticket mining, and lessons learned) and remediation recommendations that will enhance your response. Lumen can also offer proactive threat hunting (exclusive for the Premium package), where the expert reviews your system based on current trends outside of established use cases to discover anomalies related to current events.

Q Who will deliver the service?

Lumen Virtual SOC is delivered by our security team, which is formed by seasoned on-shore U.S. based resources with years of experience

Q 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 will occur during deployment and post-deployment periods.

Q How much time before the Virtual SOC is fully operational?

The first step in the deployment process is estimated to take two weeks and includes information gathering, access to your security and operational environment (SIEM, ticketing system, etc.), critical use case identification and initial run book creation and approval. Lumen Virtual SOC can begin 24/7/365 operations after the deployment process is complete. Over the next two to three weeks, our SOC experts will continue with use case tuning and development. Then, they expand and optimize log sources and start runbook maintenance and reporting.

Additional questions

Q Do I still need a SIEM platform if I have Virtual SOC?

Yes. Lumen Virtual SOC does not cover SIEM platform management or log ingest configuration. SIEM platform issues could impact our SOC expert analysis. For better results, a managed SIEM service like Lumen Managed SIEM is recommended.

Q Does Lumen Virtual SOC provide SLA for incident notification?

Yes. Lumen Virtual SOC provides SLA based on incident priority: P1 (urgent), P2 (high), P3 (medium), and P4 (low).

LUMEN® TECHNOLOGIES