Lumen Service Guide

Virtual Security Operations Center ("vSOC") Service

Updated: October 21, 2022

This Lumen Service Guide ("SG") sets forth a description of the vSOC Service ("Service") offered by Lumen, including technical details and additional requirements or terms. vSOC, is Lumen's Professional Security Services managed security service offering for Security Operations Center ("SOC") security information event management ("SIEM") monitoring and Incident Handling. "Lumen" is defined as CenturyLink Communications, LLC d/b/a Lumen Technologies Group or its affiliated entities. This Service Guide is subject to and incorporated into the Statement of Work ("SOW") for vSOC Services. The specific details of the Service ordered by Customer will be set forth in the SOW.

Service Description.

The Lumen vSOC Service provides 24x7x365 monitoring and Incident notification leveraging the Customer's SIEM (Security Information Event Management) platform. Lumen SOC security experts correlate Alerts with threat intelligence and professional experience to interpret and classify Events, identifying impacting threats for quicker resolution.

Lumen will supply a virtual SOC comprised of geographically separated security analysts located in the United States.

The vSOC Service pricing is based on the defined service package and the Customer's anticipated maximum monthly Incident rate, priced as a monthly recurring charge (MRC). Incident rate can be estimated based on Customer's SIEM ingestion rate or events/messages per second.

The standard vSOC offering is provided in the three service packages (Basic, Advanced, Premium) and as further illustrated in the table and descriptions below.

Task/Role	Entry (Basic)	Mid (Advanced)	High (Premium)
24/7/365 SIEM monitoring and Incident notification	✓	✓	✓
Use Case development and Tuning	✓	✓	✓
Run Book development and maintenance	✓	✓	✓
Deep-Dive Analytics		✓	✓
Incident Handling		✓	✓
Use Case Advanced tuning		✓	✓
Threat Hunting			✓

- vSOC Basic - The Basic Service package includes:
  - Run Book development, including notification process and procedures for handling Alerts and Incidents.
  - 24x7x365 SIEM monitoring and notification: confirm the validity of SIEM Alerts, perform prescriptive analysis (classify Event and gather contextual information according to Run Book), and provide notification according to Run Book.
  - 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. Lumen will perform rule/offense tuning and testing of use case logic (signatures) to trigger Alerts. Lumen will fine tune the Use Cases to improve fidelity (fewer false negatives and false positives) based on reviews of Incidents, new Threat intelligence from Black Lotus Labs, and additional research performed by senior vSOC security analysts.

- vSOC Advanced - The Advanced Service package of service includes the features of Basic with the following additional Services:
  - 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.) will be included in the Ticket to the Customer.
    - Threat analysis considers the patching and version status of affected victims, checking for zero-day vulnerabilities, and determining the actual risk of a threat taking into consideration information Black Lotus Labs intelligence and comparing it against Events within the customer's SIEM.

- Incident mining assists with improving overall operations by identifying recurring incidents and lessons learned to recommend process or environment improvements.
- Incident Handling - This feature identifies cause of incidents by conducting analysis of Logs, validates priority and recommends remediation actions to be taken by the Customer.

- vSOC Premium - The Premium Service package includes the features of Basic and Advanced plus:

  - Threat Hunting: proactive function conducted by a Lumen security analyst who reviews Logs and configurations outside of the SIEM, taking into account current trends, outside of established use cases with the goal of discovering anomalies related to current events.

    Threat Hunting is an activity conducted during Business Hours. Threat Hunting is performed on a regular basis or may be done on an ad-hoc basis if it's initiated via a Customer request or as a result of a new high priority security advisory being released; Ad-hoc Threat Hunt activity may cause planned Threat Hunts to pause until the ad-hoc Threat Hunt has been completed.

vSOC analysts conduct proactive reviews of the specific device or customer network environment that Customer provides Lumen access to. Threat Hunting activities will be reported to Customer both weekly and quarterly. The Lumen analysts reviews are based on trends outside of established use cases to discover anomalies. Threat hunting is specific to each environment requested to be analyzed by the Customer, but some techniques can be applied to almost any environment. Lumen's core threat hunting techniques utilize a five-stage framework. A five-stage framework is utilized to provide structured analysis and focus on each threat hunting activity. The reporting of findings may result in, by way example, new use case development and recommendations to modify the Logs that are ingested into the SIEM, and recommendations for patching or updating or upgrading recommendations. The key five stages include:

- **Threat Hunting Stage 1.** Determining the potential Attack scenario involves clearly defining the specific Threat that could be active in the environment. This stage includes identifying overall techniques that current detections may not identify and identifying valid targets and vulnerabilities that exist in the environment to be reviewed by Lumen.

- **Threat Hunting Stage 2.** Mapping the potential paths builds on the previous stage and is based on how an adversary might execute the intrusion and which key kill chain steps would have to occur. This results in areas the hunt should focus on searching for evidence of an Attack. Lumen may utilize the MITRE ATT&CK® framework for mapping potential intrusion paths and providing context and log sources needed for each step.

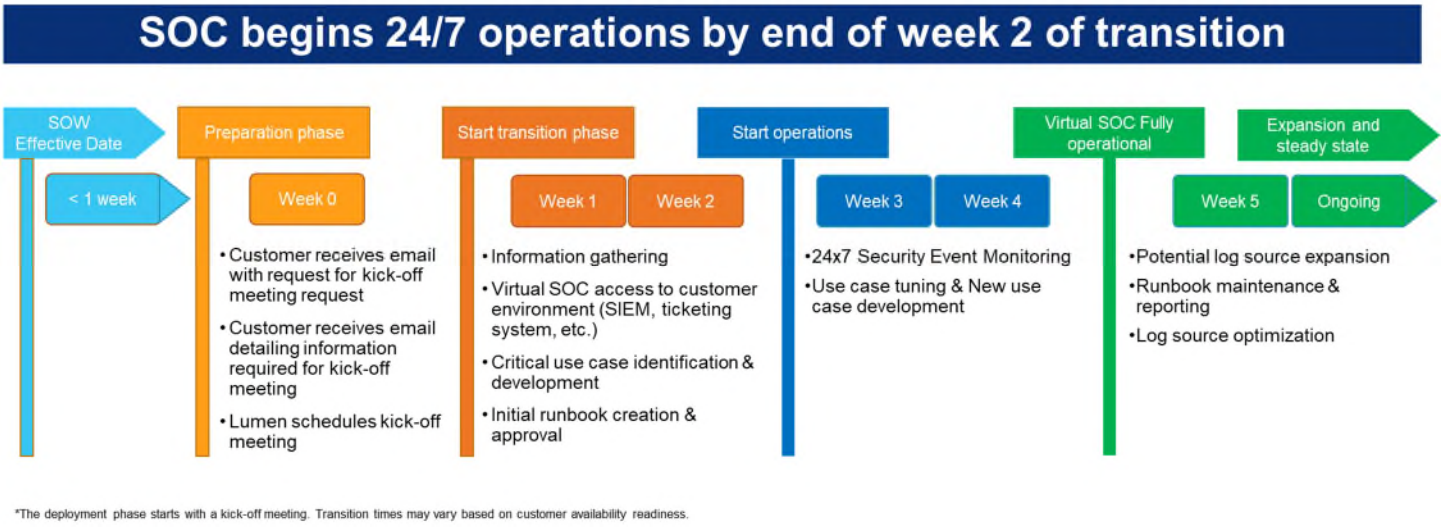
- **Threat Hunting Stage 3.** Identifying necessary logging and data sources to search for evidence. Threat Hunt analysts need to understand the client environment and logging to identify potential gaps in coverage. These gaps in coverage will be documented and reported to the customer while other approaches would need to be developed for hunting. During this stage, the threat hunt analyst searches for indicators of compromise and adversary TTPS.

- **Threat Hunting Stage 4.** Conducting analysis to identify patterns. The evidence from searches will be correlated and reviewed to determine if the activity is related to adversary actions or is normal expected traffic in the environment. Findings may result in additional searches to look for further evidence of compromise.

- **Threat Hunting Stage 5.** Documenting the findings of the threat hunt. The threat hunt is completed by documenting the results of the analysis, the logic used, and the assessment of the activity. The hunt will also document any gaps in logging and recommendations for detection logic. If evidence of a separate intrusion is found, the analyst will report the finding to the customer and conduct a separate hunt. Documentation is provided at the end of each Threat Hunt; however, the duration of each Threat Hunt is variable.

SIEM Platform Access requirements. The Customer must provide vSOC resources secure access to the SIEM platform no later than 30 days from the Effective Date of the SOW. Supported customer SIEM platforms include IBM QRadar, Splunk, Sentinel, LogRhythm, and FortiSiem. Other SIEM platforms may be supported through a custom professional services engagement**.**

Representative example of vSOC Onboarding Process. Each Customer onboarding process and timeline may vary.



SOW Effective Date. Once the SOW has been signed by both parties (the Effective Date), an email will be sent to the Customer thanking them for their order and outlining the next step; a kick-off meeting which begins the Preparation Phase.

Preparation Phase. Lumen will work with the Customer to schedule a kick-off meeting and will provide the Customer with a list of information that the Customer should have available at the kick-off meeting. During this phase Lumen will ensure that all information required from the Customer to begin the transition is available and understood.

Transition Phase. Lumen will confirm that the vSOC has secure access to the Customer SIEM. Lumen will develop and activate an initial set of SIEM Use Cases.

Lumen will work with Customer to collect information to develop the Run Book. Lumen will initially develop the Run Book with (i) standard SIEM platform security use cases, (ii) the critical information provided by Customer as noted below; (iii) priority levels (based on critical assets list, compliance requirements, etc.) agreed with Customer; and (iv) a ticketing process and/or communications plan (e.g., email, Customer ticketing system, written report format).

Critical Information. Customer will provide the following information to assist Lumen in the Run Book development: critical assets list, compliance requirements, internal policies (e.g., Acceptable Use Policy, remote access policy, bring your own device policy), geographical limitations, key escalation and project contacts.

Once the initial Use Cases have been activated in the SIEM, and the initial Run Book has been completed, the vSOC will begin monitoring the SIEM. This process typically occurs approximately 2 weeks after the SOW Effective Date.

Start Operations. vSOC Service include an initial two-week test period. During this two-week period Lumen will ensure that SIEM Use Cases are functioning as expected, that the Run Book is accurate, and that all tools and processes used by vSOC are properly documented and functioning as expected. No SLOs apply during this test period.

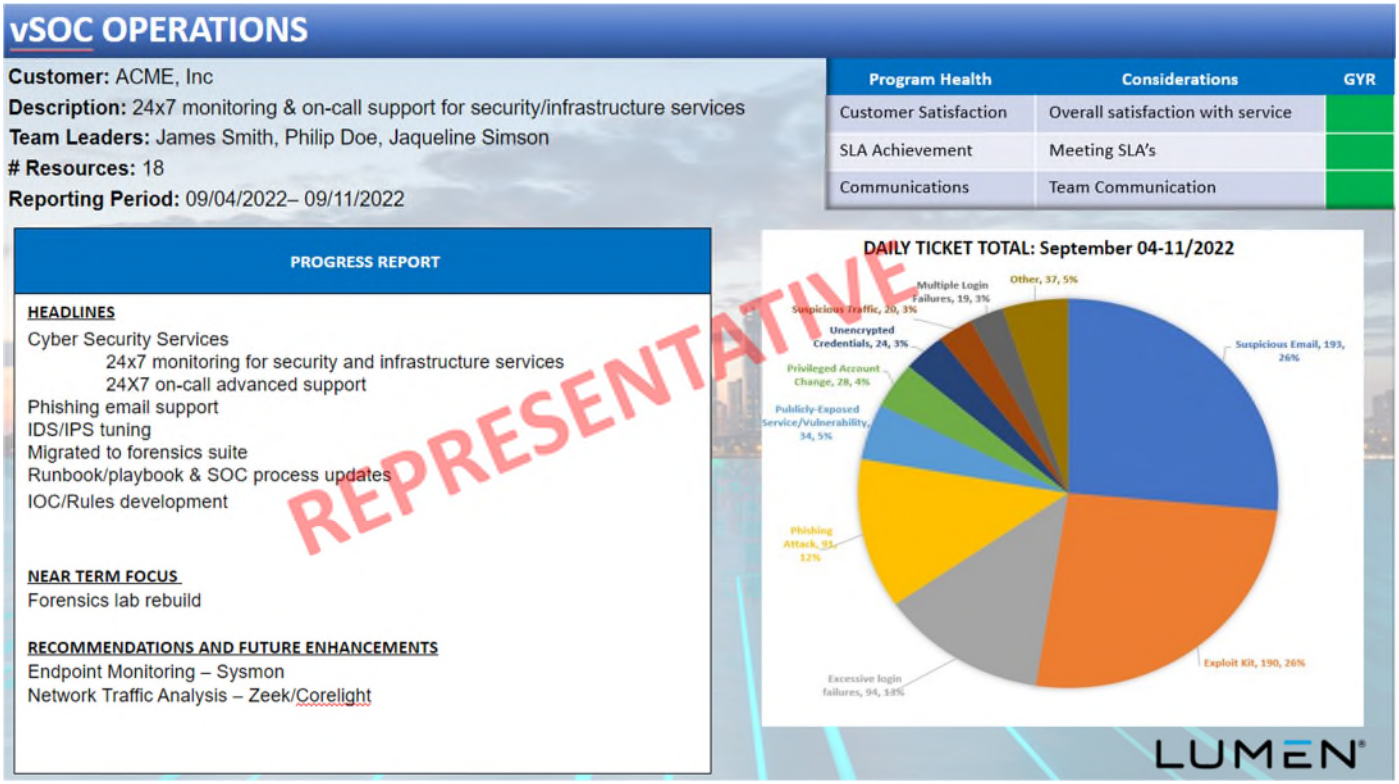
vSOC Operational. Services will be performed in accordance with the Service package selected by Customer.

As part of the vSOC Service Lumen provides classification of Incidents, and triage and impact analysis. Lumen closes out false positives Alerts and assigns Incidents priority levels per the rules established in the Run Book. Lumen will notify Customer of Incidents per method obtained in Run Book. Any Incidents, correlations, or suspect Incident trends will be promptly escalated to the Customer via the agreed communications plan.

Custom Use Case Requests – Lumen will perform custom use case requests for Customer. Lumen will use reasonable efforts to fulfill custom use case requests within three (3) weeks per change request.

Reporting - Lumen will provide weekly incident reporting. Lumen will leverage customer SIEM reporting to provide incident data details within SIEM platform reports. Example dashboard objects include system notifications, most severe offenses, top attack categories, system summary and top alarm signatures. Lumen will provide regular reports of incidents, trends, and resulting security posture as mutually agreed upon. Reports will be provided by email in a mutually agreed format, on a weekly basis (unless otherwise mutually agreed). A sample report is illustrated in the table below.

Sample Report Content



Definitions.

Incident Handling: Analysis and cause identification of Incidents and provide recommended remediation actions, which may include updating use cases and the Run Book. Lumen provides recommendations only. Customer is responsible for taking action and/or implementing any recommended action.

Deep-Dive Analytics: Analysis of trends, threats, historical Incident mining. Any additional information identified and documented by Lumen will be included in the Ticket.

MITRE ATT&CK®: A globally accessible knowledge base of adversary tactics and techniques based on real-world observations maintained and published by The MITRE Corporation (https://www.mitre.org/).

SIEM Policy: SIEM policies define the Log data ingestion, normalization and retention rules for the SIEM based on known Use Cases.

Threat Hunting: Threat Hunting is a proactive function conducted by a Lumen security analyst who reviews Logs and configurations outside of the SIEM, taking into account current trends, outside of established use cases with the goal of discovering anomalies related to current events. The five stages of Threat Hunting are described in the Service Guide.