Lumen Service Guide

Lumen Managed SIEM Service

Version: February 15, 2023

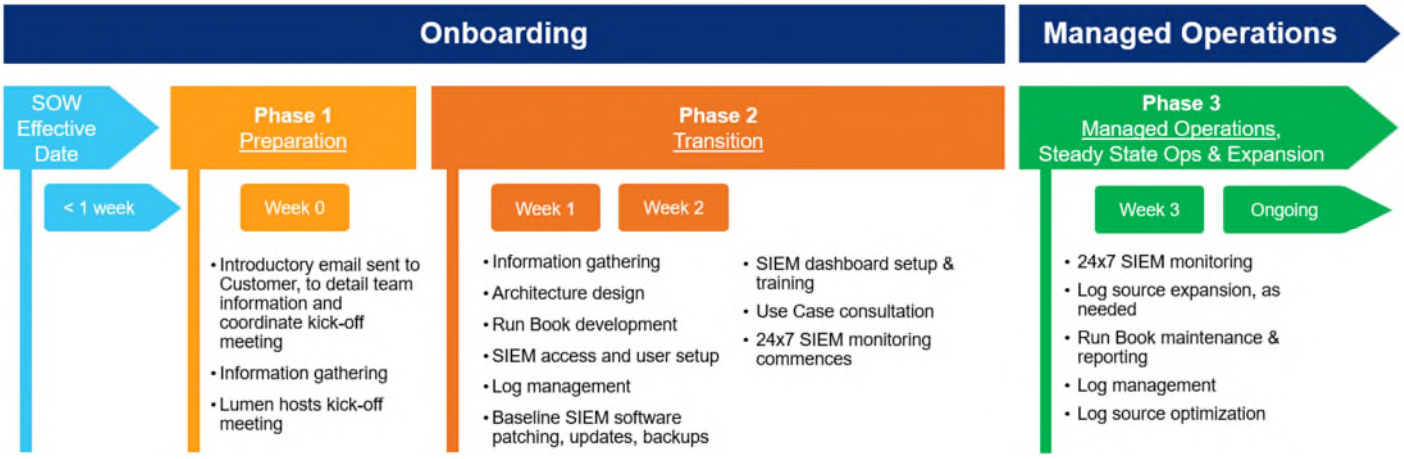
This Lumen Service Guide ("SG") sets forth a description of Managed Security Information and Event Management ("SIEM") – Customer-owned Service ("Service") offered by Lumen, including technical details and additional requirements or terms. The Managed SIEM Service is Lumen's Professional Security Services managed security service offering for SIEM system administration, log aggregation and analysis. "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 Managed SIEM – Customer-owned Services. The specific details of the Service ordered by Customer will be set forth in the SOW.

1. Service.

1.1 Supported SIEM Platforms. Supported Customer SIEM platforms currently include IBM QRadar, Splunk, Sentinel, LogRhythm, and FortiSiem. Other SIEM platforms may be supported through a custom professional services engagement and are outside the scope of this Service.

1.2 Onboarding of Service.

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



1.2.1 Phase 1 – Preparation.
Lumen will send an introductory email to outline next steps, and will work with the Customer to schedule a kick-off meeting. Lumen 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 confirm that all information required from the Customer to begin the transition is available and understood, and will work with Customer to jointly develop an onboarding project plan.

1.2.2 Phase 2 – Transition.

Lumen will perform the following activities.

Reporting – Lumen will develop a dashboard and individual reports within the SIEM that depict network activity for Customer Use Cases. Lumen will provide training to Customer to assist with accessing and using these dashboard reports. During the Transition Phase, Lumen will conduct weekly status meetings to monitor and report on progress, and will provide weekly transition status reports via email.

Run Book – Lumen will work with Customer to create a new, or update an existing Run Book that includes escalation procedures for SIEM related issues requiring Customer action.

SIEM patching – Lumen will notify Customer of SIEM patch availability and advise on patch application. Lumen will install patches approved by Customer per Customer's change management process once Service transition to Phase 3.

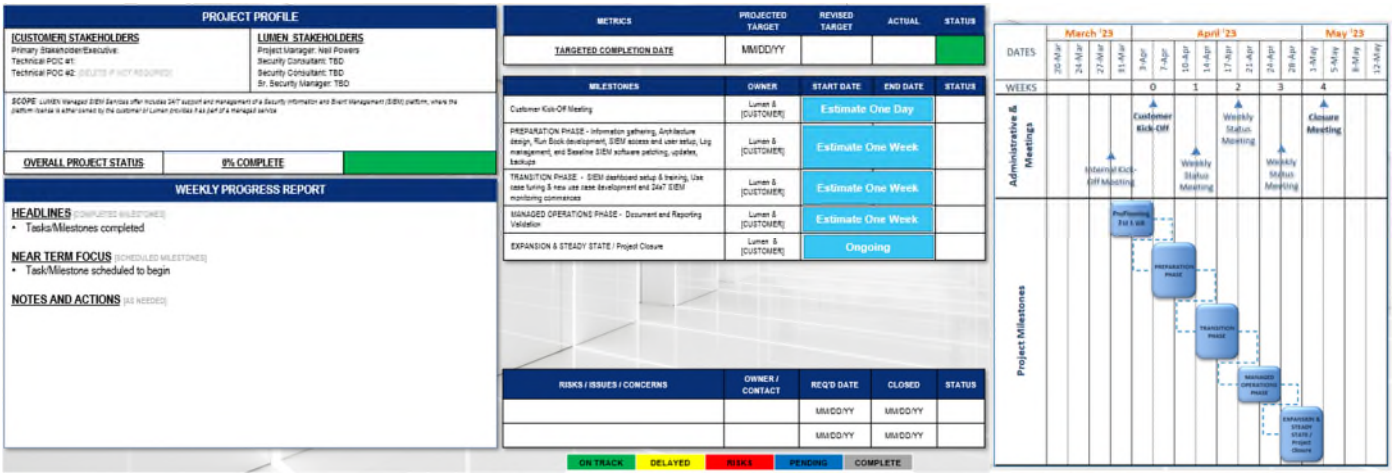
SIEM backup – Lumen will configure SIEM backup parameters per Customer provided policy and Customer controlled backup target location. Customer will provide Lumen with SIEM backup policy and Customer controlled backup target location. Configuration and implementation of Customer's backup policy will occur during Phase 3.

Log management – Lumen will work with Customer to identify and prioritize Logs, validate network connectivity between Log sources and SIEM, onboard and configure ingestion for Logs, and create the Lumen base build configuration.

User assignment – Lumen will work with Customer to define or update user access role types that will be configured in the SIEM. Lumen will then create or update SIEM users and assign them to those access roles within the SIEM.

Use Case consultation – Lumen will enter and activate Customer provided Use Cases, and Customer provided Use Case changes, into the SIEM. Customer is responsible for Use Case development, testing and verification. Lumen will make reasonable business efforts to assist Customer in Use Case development, testing and verification.

- *Representative example of **Weekly Transition Project Status Report and Gantt Chart.***



Lumen will hold an operational acceptance meeting with Customer to validate completion of Transition Phase activities, and commencement of the Managed Operations Phase.

1.3 Phase 3 - Managed Operations.

The Managed Operations Phase represents the *ongoing* SIEM system administration activities, including monitoring the SIEM on a 24x7x365 basis for health, availability and performance.

Log management – Lumen will monitor log ingestion, including evaluation of log format and verbosity from log sources (the balance between events per second and the different types of events), loss of visibility, reduction in visible traffic from log sources and quality of network flow ingestion. Should the cause of any loss of visibility, reduction in visible traffic from log sources or decrease in the quality of network flow ingestion be outside of Lumen's control, Lumen will notify Customer per agreed upon Run Book.

SIEM patching – Lumen will verify that known SIEM system vulnerabilities are identified and patched. Lumen will install patches approved by Customer per the Run Book.

SIEM upgrading – Lumen will notify Customer of SIEM upgrade availability and advise on impact to service of upgrade installation. Lumen will perform SIEM software upgrades approved by Customer per Customer's change management process.

SIEM backup – Lumen will maintain SIEM backup configuration per Customer provided backup policy and target location.

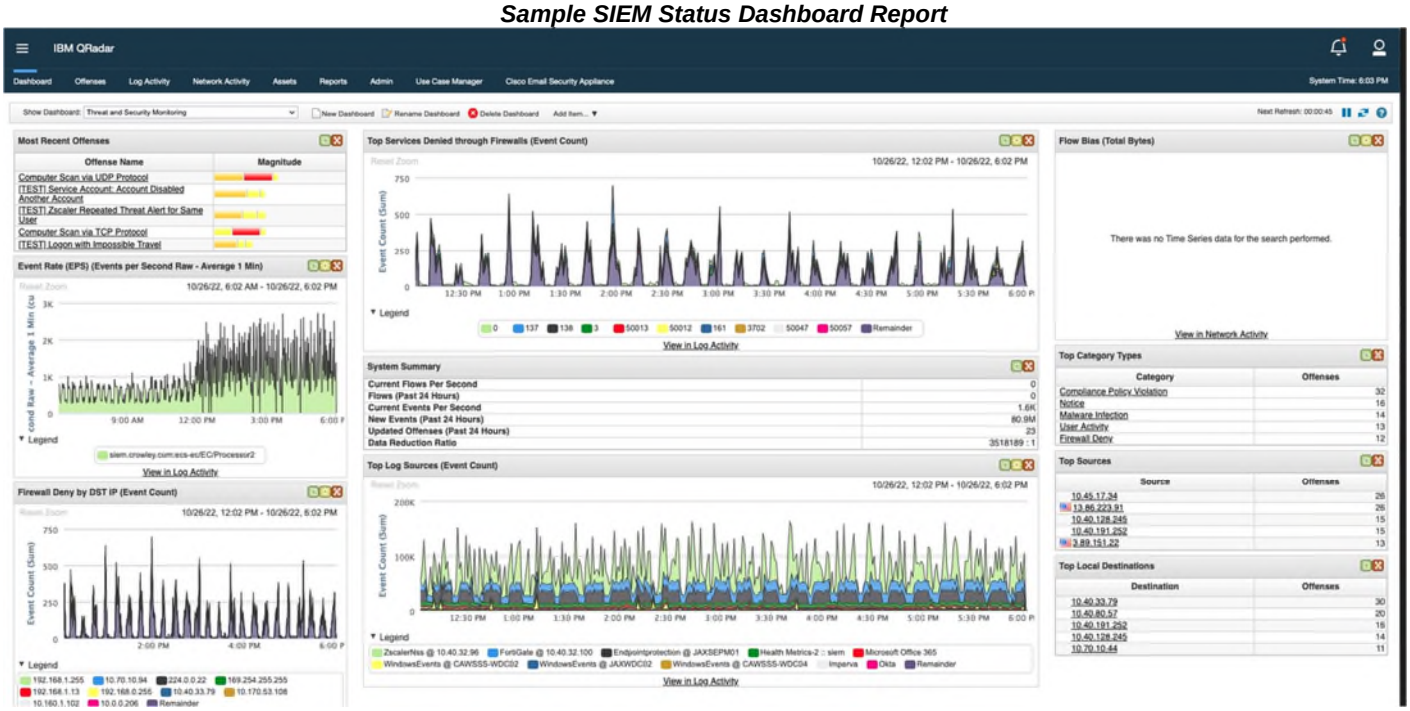
SIEM Log source onboarding– Customer may request that Lumen configure the SIEM to ingest additional log sources. Lumen will work with Customer resources responsible for newly requested log sources to facilitate onboarding of new log sources. Customer is responsible for making all required changes on Log sources and network to enable the logs to be forwarded to the SIEM.

SIEM monitoring - Lumen will monitor SIEM platform health, availability, and performance 24x7x365. If the SIEM becomes unavailable or SIEM performance is degraded, Lumen will use reasonable efforts to restore availability and/or performance. Should the cause of any outage or performance degradation be outside of Lumen's control, Lumen will notify Customer per agreed upon Run Book.

Use Case consultation – Lumen will enter and activate Customer provided Use Cases, and Customer provided Use Case changes, into the SIEM.

Reporting – Lumen will schedule and conduct quarterly business reviews ("QBR") during which Lumen will report on the quarterly actions (patching, upgrading, etc.), performance metrics (ingestion, alerts, downtime, etc.), overall service status (performance against SLAs and other expectations), as well as provide recommendations for improvement. Additionally, Lumen will maintain SIEM dashboards and reporting (as agreed upon with Customer) available to Customer for online viewing.

Sample SIEM Status Dashboard Report



Sample Use Case Dashboard Report

Sample Individual Use Case Report