Lumen Service Guide

Lumen Defender Advanced Managed Service Detection and Response (AMDR) For Sentinel

Version: February 18, 2026

This Lumen Service Guide ("SG") sets forth a description of the Lumen Defender Advanced Managed Detection and Response for Microsoft Sentinel (AMDR) Service ("Service") offered by Lumen, including technical details and additional requirements or terms. AMDR 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 AMDR Services.

The specific details of the Service ordered by Customer will be set forth in the SOW.

1. Service Description.

1.1 The Lumen AMDR Service provides security operations center functions using Lumen provided resources and technology to monitor the Microsoft Sentinel Security Information Event Management (SIEM) platform provided by Lumen or Customer.

1.2 The supported Customer SIEM platform for this service is limited to Microsoft Sentinel. Lumen will provide the Microsoft Sentinel platform. Customer provided Microsoft Sentinel is available per the guidelines in this Service Guide.

1.3 **Threat Hunting.** If Customer has purchased the Premium package including Threat Hunting, the following additional service features will apply. Lumen analysts will conduct proactive reviews of the Log Sources Customer elects to connect to the SIEM and provide Lumen access to. Threat Hunting activities will be reported to Customer weekly and quarterly. Threat hunting is specific to each environment requested to be analyzed by the Customer. Lumen's core threat hunting techniques utilize a five-stage framework in order 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, recommendations to modify the Logs that are ingested into the SIEM, and/or recommendations for patching, updating, or upgrading. The key five stages include:

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

- **Threat Hunting Stage 3.** Identifying logging and data sources to search for evidence. Threat Hunt analysts need to understand the Customer environment and logging to identify potential gaps in coverage. These gaps in coverage will be documented and reported to the Customer. 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. 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.

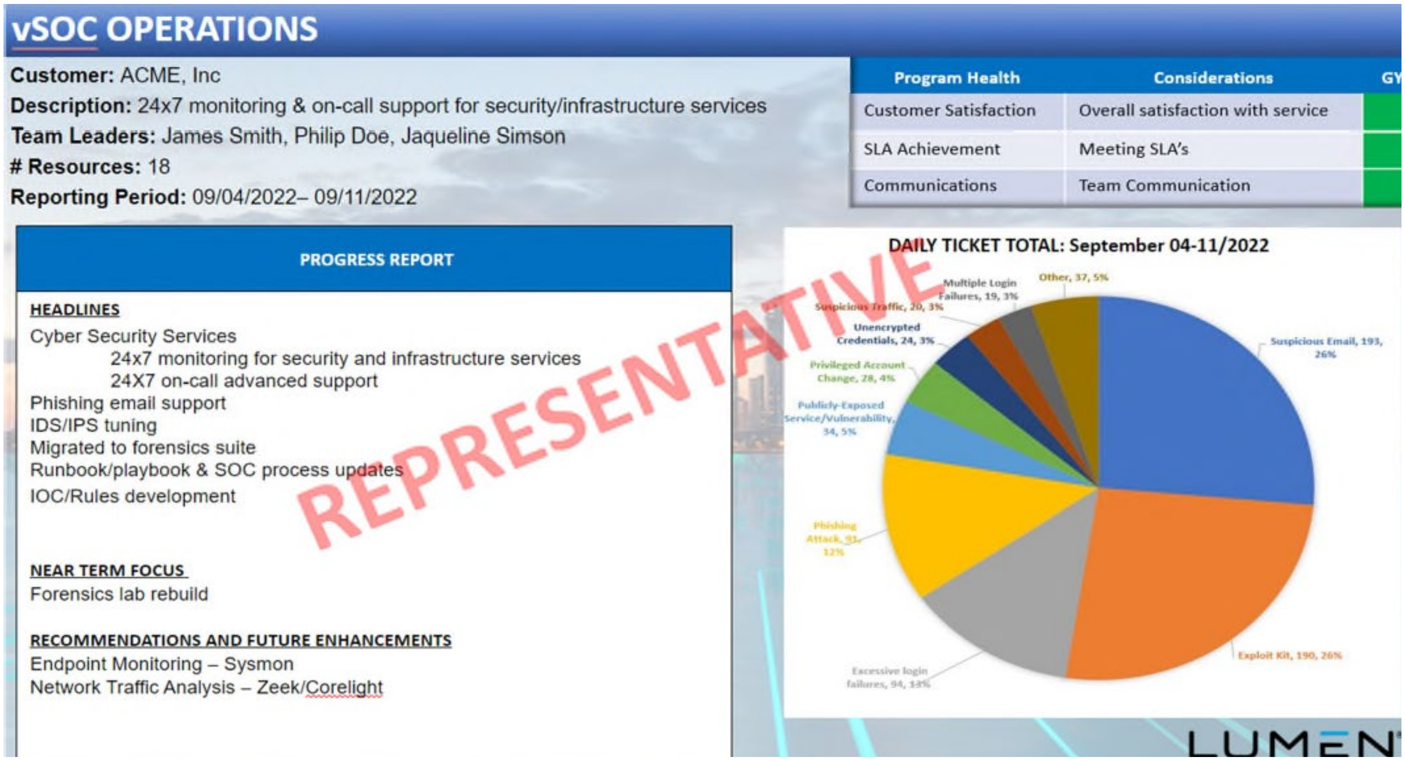
2. Transition Phase. Lumen will work with Customer to collect information to develop the Run Book. Lumen will initially develop the Run Book with (i) standard SIEM platform security use cases, (ii) the critical information provided by Customer as noted below; (iii) priority levels (based on critical 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).

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

3. **Start Operations.** AMDR Service includes an initial two-week test period. During this two-week period Lumen will confirm that SIEM Use Cases are functioning as expected, that the Run Book is accurate, and that all tools and processes used by Lumen SOC are documented and functioning as expected. No SLAs apply during this test period.

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

5. **Reporting.** Lumen will provide regular Sentinel Incident reporting. Lumen will leverage SIEM reporting to provide details within SIEM platform reports. Examples of dashboard items may include system notifications, most severe offenses, top attack categories, system summary and top alarm signatures. Lumen will provide regular reports of Sentinel 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).



vSOC OPERATIONS

Customer: ACME, Inc
Description: 24x7 monitoring & on-call support for security/infrastructure services
Team Leaders: James Smith, Philip Doe, Jaqueline Simson
# Resources: 18
Reporting Period: 09/04/2022– 09/11/2022

Program Health	Considerations	GY
Customer Satisfaction	Overall satisfaction with service	🟩
SLA Achievement	Meeting SLA's	🟩
Communications	Team Communication	🟩

PROGRESS REPORT

HEADLINES

Cyber Security Services
- 24x7 monitoring for security and infrastructure services
- 24X7 on-call advanced support

Phishing email support
IDS/IPS tuning
Migrated to forensics suite
Runbook/playbook & SOC process updates
IOC/Rules development

NEAR TERM FOCUS

Forensics lab rebuild

RECOMMENDATIONS AND FUTURE ENHANCEMENTS

Endpoint Monitoring – Sysmon
Network Traffic Analysis – Zeek/Corelight

DAILY TICKET TOTAL: September 04-11/2022

Multiple Login Failures, 19, 3%
Other, 37, 5%
Suspicious Traffic, 20, 3%
Unencrypted Credentials, 24, 3%
Privileged Account Change, 28, 4%
Publicly-Exposed Service/Vulnerability, 34, 5%
Suspicious Email, 193, 26%
Phishing Attack, 91, 12%
Exploit Kit, 190, 26%
Excessive login failures, 94, 13%

6. **Managed Operations.**

Managed Operations 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 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.

Quarterly Business Reviews– 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 and referenced above) available to Customer for online viewing.