

Lumen Virtual SOC

Around-the-clock SIEM monitoring and expert incident handling by top security experts

Lumen Virtual Security Operations Center (VSOC) provides 24/7/365 security monitoring and expert incident handling for quick response and resolution. Avoid insourced SOC expenses and leverage Lumen's security expertise to augment your detection and response strategy and receive remediation recommendations that go beyond just notification actions.

Improve your security posture

Develop your custom runbook and get 24/7/365 SIEM monitoring and incident handling to detect, analyze, and quickly respond to cyber threats. Our security experts augment your detection and response strategy and help you focus on actual events by identifying and closing out false positives and tuning use cases in your SIEM platform. They will also perform deep-dive analytics and treat hunting to provide remediation recommendations.

Cost-effective security support

Lumen Virtual SOC provides expert around-the-clock SIEM monitoring while minimizing labor and CAPEX expenses. We leverage existing SIEM investments made by your organization and have three standard packages available to help mature your security strategy and fit your business and budget needs.

Top security expertise

Lumen's seasoned security experts log into your environment and apply years of solid security expertise to deliver the Service. Our team has unique access to threat intelligence through Black Lotus Labs®, and lessons learned from protecting Lumen's extensive network to provide you with remediation recommendations that go beyond standard notification actions.



Features and Specs

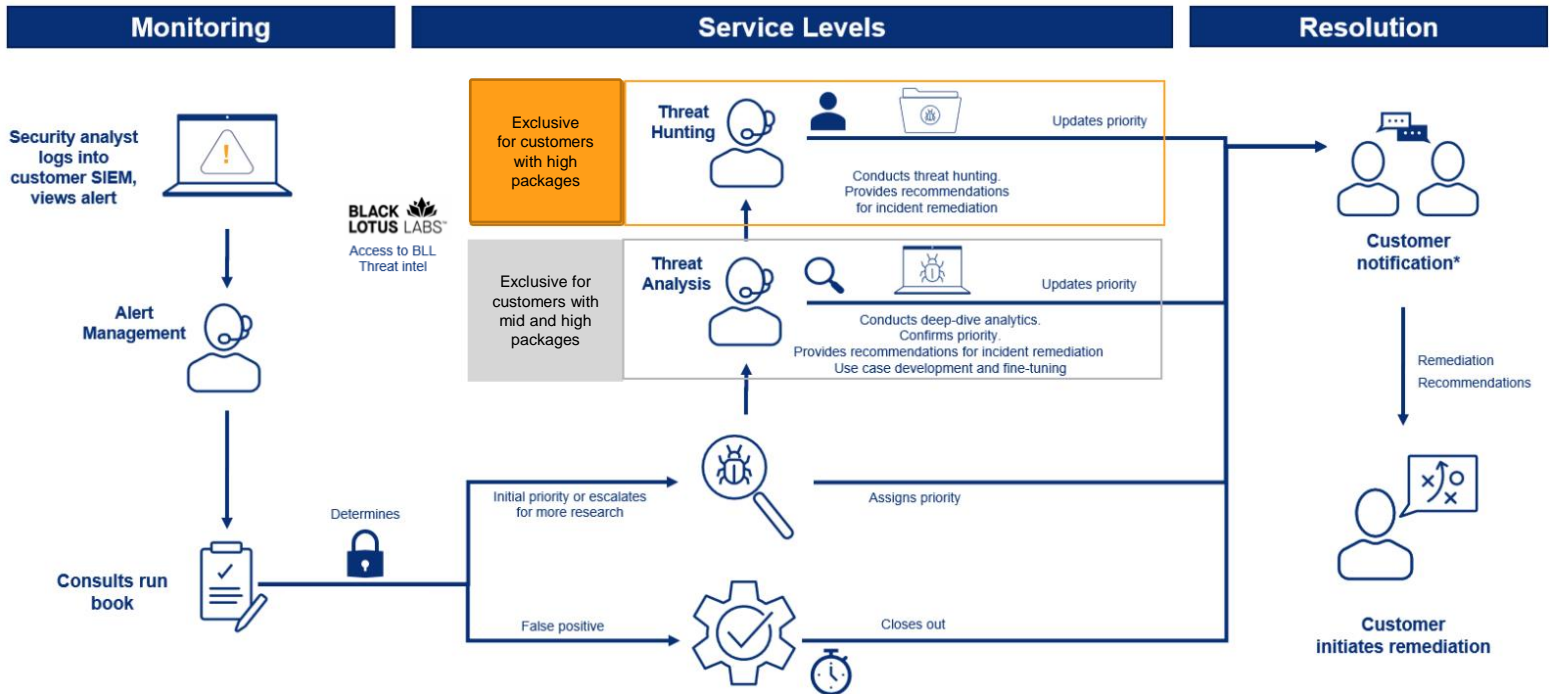
Standard Virtual SOC packages*

- 24/7/365 SIEM monitoring and notification
- Use Case development and tuning
- Runbook development and maintenance
- Deep-dive Analytics
- Incident Handling
- Use Case advanced tuning
- Threat Hunting

| | Entry | Mid | High |
|---|-------|-----|------|
| 24/7/365 SIEM monitoring and notification | ✓ | ✓ | ✓ |
| Use Case development and tuning | ✓ | ✓ | ✓ |
| Runbook development and maintenance | ✓ | ✓ | ✓ |
| Deep-dive Analytics | | ✓ | ✓ |
| Incident Handling | | ✓ | ✓ |
| Use Case advanced tuning | | ✓ | ✓ |
| Threat Hunting | | | ✓ |

*Requires customer to provide SIEM or purchase a Lumen Managed SIEM Service.

SOC workflow



*Any security events, correlations, or suspect event trends will be escalated per custom run book

Why Lumen?

Lumen is your single provider to enable digital transformation. Our security experts leverage their vast experience and unique access to Black Lotus Labs threat intelligence to provide secure event monitoring, support, and advanced remediation recommendations you need to respond to events quickly and with positive results. Partner with Lumen on Professional Security Services to obtain resources for consulting and advisory services, risk and compliance management, and security device and operations management.