

Lumen[®] SOC as a Service for Public Sector

Keeping pace with today's threat landscape

Public Sector IT leaders are facing considerable challenges and significant pressures in keeping pace with today's threat landscape and preparing for future threats. They require 24/7 visibility yet building their own Security Operations Center (SOC) does not fit into their budgets. Recruiting and retaining talent and updating the latest technology tools brings even more challenges.

Lumen SOC as a Service for Public Sector offers a simplified strategic approach, that meets the strict compliance requirements set forth by the Federal government. SOCaaS offers visibility into cyber vulnerabilities and provides fully managed cybersecurity threat detection, incident management, and support for Public Sector customers.

Common Use Cases

- Consolidation of multiple SOC's into one solution for a holistic view across the entire agency or organization
- Lowering operational costs by leveraging highly trained, certified, U.S. based security analysts that are experienced in cyber security threat detection and available 24/7
- Enhancing overall security posture and agile risk response by integrating cutting-edge threat intelligence and data analysis.

Features and Specs

Facilities and personnel

- 24/7 security operations centers are geographically diverse, located in Herndon, VA and Dallas, TX
- SOC's are highly available and audited annually for FISMA high compliance
- Support for agency suitability requirements available
- U.S. persons with experience supporting government agency needs

Minimize operational costs

- Leverage highly skilled, U.S. based analysts and the latest technology without having to recruit and retain staff or manage the lifecycle of products. The fully managed service offers predictable monthly service rates to plan budgets accordingly.

Agile risk response

- Achieve greater visibility and situational awareness by continuously monitoring your devices. With 24/7 monitoring, the analyst team can ingest and analyze the data to quickly detect and prioritize cyber threats and events.

Enhance overall security posture

- Utilize Lumen's highly available, FISMA high operations, and federally compliant SOC services for a fully managed offering that can help improve your agency's overall security



877-453-8353 | lumen.com | info@lumen.com

Features and Specs (Cont.)

Federally compliant SOC services

- The SOCaaS SIEM ingests security-related event logs, sourced from an agencies' network and security devices for data analysis and event correlation.
- Threat detection analysts monitor customer networks for suspicious activity and proactively alert customers of notable security events of known or suspected malicious activity.
- Timely reaction to events in accordance with the SLA
 - Known malicious events are prioritized and notifications are sent to customers in near-real time
 - Benign events are suppressed minimizing alert noise for customers
 - Suspicious events are triaged, investigated, and escalated to the customer, if needed

Technology

- Ongoing development of filter/rules continuously improves our operations by adapting the system for future responses to defined threats
- Consolidated telemetry feed for agency's use
- Self-service portal for tickets and notifications
- Dashboard to review log data, visualize trends, retrieve standard reports include ticketing metrics and SLA performance
- Support for government furnished equipment (GFE)
- Data retention in alignment with National Archives and Records Administration (NARA) requirements
- Available via GSA Enterprise Infrastructure Services (EIS) contract, GSA Multi-Award Schedule (MAS) contract, and open market procurement vehicles

Why Lumen?

Lumen has a long history collaborating with government and industry partners to tackle the most pervasive security threats with a cross organizational approach. Our analysts have a deep level of expertise, integrated with the latest technologies and threat intelligence, so that agencies facing limited resources can refocus their specialized security staff on the most critical aspects of their mission.