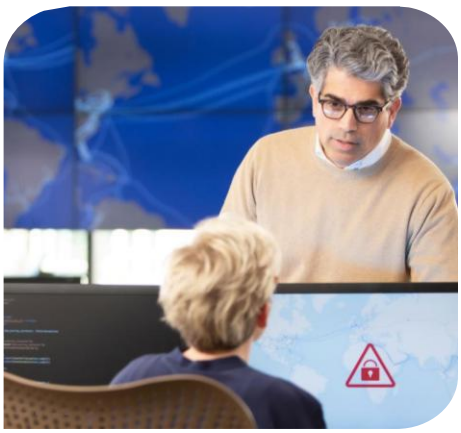
Lumen Defender℠ Advanced Managed Detection & Response (AMDR) with Microsoft Sentinel

Lumen Defender℠ Advanced Managed Detection & Response (AMDR) with Microsoft Sentinel is a fully managed 24/7 Security Operations Center (SOC) offering comprehensive cybersecurity coverage across event monitoring, incident response and threat hunting. Designed to meet the evolving threat landscape, Lumen Defender ADMR combines advanced security technologies with highly skilled analysts and integrated threat intelligence to deliver proactive and responsive protection for enterprise environments. Lumen helps organizations mitigate risk, contain threats, and maintain operational continuity by continuously monitoring, analyzing, and responding to security events. The service enables a consistent, rapid, and effective response to security incidents through automated and analyst-driven playbooks.

Common use cases

Full management: Lumen delivers end-to-end security operations, fully managing event detection, incident response, and threat hunting. This model is ideal for organizations that require comprehensive coverage without maintaining internal SOC capabilities.

Shared management: Lumen works alongside the customer's internal security team to provide flexible, scalable support across core SOC functions. Lumen can handle alert triage, shift coverage, and backup SOC operations, allowing the customer to retain control over sensitive investigations while offloading routine monitoring and escalation.



Why Lumen Defender ADMR?

Unmatched network visibility - Backed by a 340,000-route-mile global fiber platform, Lumen combines deep network infrastructure expertise with comprehensive threat visibility, enabling early detection of advanced persistent threats (APTs) and sophisticated cyberattacks across hybrid environments.

Elite threat intelligence from Black Lotus Labs - Lumen's proprietary threat intelligence team, Black Lotus Labs, enhances SOC operations with real-time monitoring of ~46,000 command-and-control (C2) infrastructures and over 200 billion NetFlow sessions daily, disrupting threats before they reach customer environments.

Integrated, scalable security portfolio - Lumen delivers a full spectrum of managed and Professional security services—including DDoS Mitigation, MTIPS, Security Assessments, Managed SASE, ZTNA and Managed Firewalls—designed to work together as part of a unified, automated, and network-integrated defense strategy.

Flexible SIEM integration - Lumen supports both customer-provided and Lumen-managed SIEM platforms, enabling organizations to retain their existing investments or streamline with a managed solution.

LUMEN® TECHNOLOGIES

Features and Specs

SOC monitoring

- Continuous 24/7 monitoring, detection, triage, and case creation for cybersecurity events across the enterprise.
- Event correlation and alert prioritization using behavioral analytics and threat intelligence.

Event management

- Comprehensive security event handling, from alert triage to escalation and coordination.
- Playbook-driven workflows for consistent event response and customer communication.

Threat hunting

- Proactive threat detection through hypothesis-based analysis and anomaly hunting.
- Identify adversary tactics, techniques, and procedures (TTPs) within enterprise environments.

SIEM flexibility

- Customers can bring their own Sentinel environment or Lumen will provide.
- Implementation, setup, and integration services
- Ongoing SIEM tuning, management, and maintenance.

Reporting

- On-demand and scheduled reporting with self-service access to threat, compliance, and operational metrics.
- Includes executive summaries and detailed technical reports for incident review and audit purposes.

Shared access

- Customer portal access, consolidated threat dashboard, and mobile notifications.

Security automation

- Integration with SOAR tools to enable automated triage, enrichment, and response workflows.
- Enhances SOC efficiency through reduced manual workload and consistent response execution.

Why Lumen?

Lumen combines world-class threat intelligence, deep network visibility, and proven cybersecurity expertise to deliver a powerful, scalable Lumen Defender ADMR solution. With integrated support for leading SIEM platforms, 24/7 monitoring, and a full suite of managed security services. Lumen enables organizations to strengthen their cyber defense without overextending internal resources. Backed by the award-winning Black Lotus Labs and a robust global network, Lumen is the trusted partner for enterprises seeking to modernize and secure their operations.

866-352-0291 I lumen.com I info@lumen.com

LUMEN® TECHNOLOGIES