Lumen Defender℠ Advanced Managed Detection and Response (AMDR) for Palo Alto Cortex XSIAM

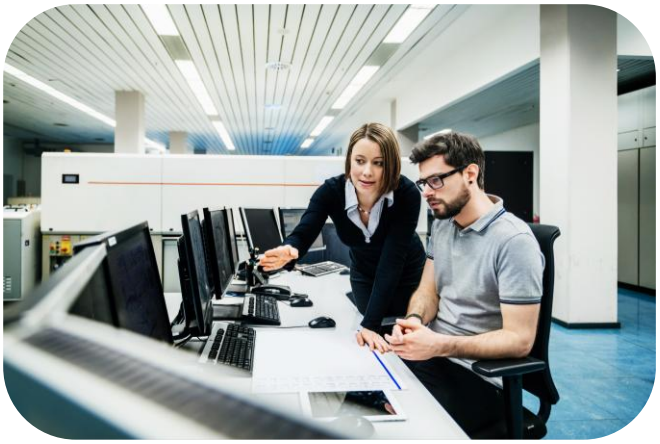
See threat activity earlier. Help reduce the burden of running a modern SOC.

Security operations are falling behind attacker speed. Threat activity is increasingly occurring earlier in the attack lifecycle, while alert volume, tool sprawl, and staffing constraints limit the ability of traditional SOC models to detect and respond effectively.

Lumen Defender AMDR for Palo Alto Cortex XSIAM delivers intelligence-led security operations through Lumen Defender℠ Threat Feed, powered by Black Lotus Labs® intelligence, combined with SOC-led detection and response operated by Lumen on the Cortex XSIAM platform.

Built on Cortex XSIAM's agentic AI capabilities, where the platform can investigate activity and initiate response actions, this approach helps reduce manual effort while actions are guided and validated by Lumen analysts.

The service supports both fully managed and co-managed SOC models, helping organizations modernize security operations, improve response consistency, and reduce the cost and operational burden of legacy SOC environments without high internal staffing.



Detect threats beyond endpoint and log signals

Lumen Defender Threat Feed provides network-embedded threat intelligence informed by attacker infrastructure and behavior outside the customer environment. This helps surface higher-confidence signals earlier in the attack lifecycle.

Provide response consistency with SOC-led execution

Detection, investigation, and response are operated by Lumen's global SOC, helping standardize how threats are handled, enhancing consistency over time.

Move from alert handling to intelligence-led operations

Threat intelligence is applied directly within detection and response workflows, shaping how threats are prioritized, investigated, and acted upon.

Minimize the burden of running a modern SOC

Lumen delivers fully managed or co-managed SOC operations, helping organizations scale detection and response without the cost and complexity of traditional SOC models.

Common use cases

- Earlier detection of emerging and infrastructure-based threats
- SOC modernization through or co-managed operations
- Can help reduce alert volume and investigation fatigue

LUMEN® TECHNOLOGIES

Visibility and reporting

- Near real-time dashboards and Lumen-provided service reviews provide visibility into security activity, incident trends, and key performance metrics
- They can help teams understand outcomes, align priorities, and improve security posture

Features and Specs

Intelligence-led detection

- Threat intelligence applied directly within detection workflows
- Higher-confidence signals and reduced false positives
- Visibility into attacker infrastructure and behavior

Automated investigation and response

- Automated workflows investigate alerts and initiate response actions
- Analyst oversight helps ensure actions are validated and appropriate
- Designed to reduce manual effort in triage and investigation

SOC-led operations

- 24×7 detection, investigation, and response by Lumen SOC
- Consistent execution across environments and incidents
- No requirement to staff or operate an internal SOC

Platform integration

- Unified detection and response through Palo Alto Cortex XSIAM
- Supports complex, hybrid, and distributed environments
- Scales with organizational growth and security needs

Why Lumen?

Lumen Defender AMDR combines network-embedded threat intelligence, SOC-led detection and response, and platform-integrated analytics to deliver a more effective and consistent security operations model. By operationalizing intelligence directly within detection and response workflows and supporting those workflows with Lumen's global SOC, the service helps organizations detect threats earlier, respond with greater consistency, and can help reduce the complexity and cost associated with running a modern SOC.

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

LUMEN® TECHNOLOGIES