Lumifi MDR with Microsoft Sentinel

Why Lumifi?

Lumifi was one of the first MDR providers to adopt Microsoft Sentinel as a leading SIEM tool. With considerable operational experience on the platform, Lumifi has been able to provide premier white-glove MDR service to customers.

The Lumifi Advantage

Ready to Deploy Content

Increased coverage on Day 1 with content aligned with the MITRE ATT&CK framework and tested by red-team experts.

Examples:

- Data Exfiltration
- Lateral Movement
- Account Compromise
- Command and Control
- Execution

Mature Threat Intelligence

Mature, MISP-driven threat intelligence program, curated by Lumifi and brought into Microsoft Sentinel.

Dozens of sources curated and pruned for false positives:

- DHS
- Infragard
- OSINT
- Closed/Paid Sources
- Lumifi Developed & Researched

Custom Use Case Development

Fully prepared to develop custom content based in unique or previously unseen log sources.

Tailored to your environment:
No two environments are the same, which is why our MDR service includes custom use case development to ensure the right detections are applied to the right log sources.

Experienced Analysts

Lumifi's analyst are already experienced with the platform. No spin up time required.

Extensive operational experience in large enterprise environments.

Lumifi already has customers on Microsoft Sentinel and are effective the day analysts get access to the SIEM.

1475 N Scottsdale Rd STE 410
Scottsdale, AZ 85257

877.388.4984
lumificyber.com