Introducing Lumifi + ShieldVision
Get to know our platform

Lumifi has leveraged more than a decade and a half of security operations expertise to design a platform that can be priced per employee, per month. It gives small security teams and large, mature IT organizations a head-start on effectiveness, enabling endpoint, network, and cloud responses out of the box, but enabling customization for unique business use cases.

Lumifi is a Managed Detection and Response (MDR) provider with 15 years of security operations expertise and a security operations center (SOC) fully based in the US. As one of the most tenured MDR providers in the space, Lumifi combines top industry talent with proprietary technology, enabling organizations to detect threats across the Gartner Triad, via logs, endpoints, and network traffic. Lumifi scales these efforts with ShieldVision, an internally developed SOC automation suite that is purpose-built for the MDR use case, threat detection and response at a massive scale across the entire customer base, improving awareness and reducing response times without sacrificing detection fidelity.

ShieldVision empowers security teams to build use cases and response flows for SIEM, EDR, NDR technologies, and more. Out of the box, it includes more than 1,000 pieces of content including searches, automated response Threat Flows, and prebuilt reports. This enables endpoint, network, and cloud responses using specific queries to customize workflows for your individual business needs. It also grants users the ability to control alert noise granularly by implementing exclusions at a global or per-alert level, in addition to dynamic enrichment and exclusions in Threat Flow.

New Features:

Investigate with repeatable clarity and precision using Composer

- Design investigations once using Composer templates, leveraging hundreds of prebuilt queries, or use your own.
- Templatize Composer investigations and run them ad-hoc, or as part of Threat Flow.
- Rich export options, including omission of certain results, in-line visualizations, and reordering of individual Composer elements as you see fit.

Design, export, and modify reports

- Address compliance needs with templatized reports that drive clear, presentable visualizations
- On-demand support for custom visualizations and data relationships. Don’t see what you need? Let us build it for you.

MSP-ready, out-of-the-box

- Multi-tenant MSP dashboard with data relationships specifically designed for the MSP use case, aiding your team in understanding your clients' activity from a single control plane.
- Click-in functionality to see the platform as a client would, work investigations, and assist with configuration.
- Leverage global visibility and access with multi-tenant content deployment, cross-client incident management, and threat hunting.
- On-demand provisioning and client setup.

Incident Management

- Seamlessly interact with findings produced by ShieldVision, observe Lumifi's actions and responses, and coordinate your team's efforts.
- Pull incident and event data directly into your ticketing system of choice via API and/or webhook.
- Escalate existing or create new cases across all three Lumifi SOC Teams; Analysts, Content, and Engineering.

A single, cohesive SaaS platform for SOC service and cybersecurity technology

- Manage, detect, and respond to threats within a consumable, digestible interface
- Automate common security tasks and tackle challenging orchestration use cases with ease
- Configure endpoint security policies, log ingestion, and data integrations
- Interact with Lumifi's industry-leading SOC service across multiple teams

Fully customizable dashboards

- Design, templatize, and modify dashboards for different audiences with a broad set of available visualizations.
- See in real time the same metrics and data relationships available in the Report Designer.

Flexible means of data ingestion

- "Ride-along": retrieve alerts and other criteria-driven data snippets to form the basis for alerting, investigation, and response.
- "Single-point": Bulk ingestion of data directly into ShieldVision, enabling comprehensive data search and maximizing ShieldVision's means of contextualization.
- "Hybrid": Combine ride-along and single-point, allowing ShieldVision to selectively query external services while storing other data sets of your choosing within ShieldVision itself.

Lumifi Security Operations Center

- Full SOC personnel, headquartered in Scottsdale, Arizona.
- See for yourself – meet the team, visit with technical leadership, and understand how one of the most tenured players in the space operates on a day-to-day basis.