Security Posture Priorities

Solution Evaluation

An integral step in creating a resilient cybersecurity platform is to perform an audit of your organizations existing policies and procedures. Lumifi can help with this endeavor during our Asset Criticality Assessment, during client onboarding process, and periodically on a structured timeline.

Here are components we consider when looking at the entire security infrastructure:

Network Security
Malware Prevention
Monitoring
Incident Management
User Education
Configuration and Change Management
User Access and Privileges

Tool Implementation

Once the proper solution or suite of solutions is determined, we help source, install, configure, tune and customize each solution to our customer's needs. If a solution is already in place, we step in and begin management of the existing tool.

The following are just a few of the services we offer in this step of the process:

Cybersecurity Hardware / Software Deployments
Cybersecurity Tool Configuration, Tuning & Customization
SIEM Appliance Administration
Establishing Security Policies & Procedures

We offer managed and co-managed environments that allow our customers to maintain visibility 24/7/365 right alongside our team. Once we are up and running the with the properly deployed solutions constant monitoring through our world-class MDR service is the next step in the process.

Managed Detection & Response (MDR)

Lumifi is a leader in MDR services, recognized on Gartner's Managed Detection and Response Market Guide and by third-party service provider lists. Often, the least considered factor in the security provider selection process in the human element. While technology is an important factor in first-class MDR, Lumifi's biggest differentiator is its expertise. Lumifi provides the experience needed to stand out from the saturated MDR market with leadership and management having decades of experience, stretching back to before MDR was even a term.

Vulnerability Management (VM)

Discovering where you are most vulnerable is a security priority and likely already part of your overall program. The ability to continuously identify threats and monitor unexpected changes in your network before they turn into breaches is common practice.

Security programs often have the challenge of finding and retaining talent along with time restraints for proper cybersecurity processes. Lumifi can help fill those gaps. Our security staff will manage the process and help ensure your security program is successful while saving you time and money.

Email Security

Ransomware, impersonation, spear phishing; standard email-defense systems can't protect against it all. Lumifi deploys leading email security tools to defend against routine spam and targeted threats.
Email security tools combine internally developed and third-party technologies with dozens of internal and external threat-intelligence sources. These tools simplify and automate the process of recovering email and other data within your email environment while ensuring that email systems remain 100% operational, and data is secured within. In addition to L1 and L2 support, Lumifi provides back-end integration into its MDR services to enhance visibility and reporting.

Endpoint Detection & Response (EDR)

EDR solutions take traditional antivirus tools to the next level by allowing security teams to continuously collect, track and store endpoint data. This level of detail provides analysts with the forensic granularity necessary for active threat hunting and proper incident response. Lumifi partners with leading EDR tools such as SentinelOne, Defender for Endpoint and CarbonBlack to provide comprehensive security solutions that secure customer endpoints end-to-end.

Incident Response & Threat Remediation

Cyber resilience includes recovering quickly from an attack. When Lumifi reports a verified incident, our ASOC provides recommended steps for remediation, including step-by-step instructions with procedures and escalation paths to remediate the incident.
The Lumifi Cybersecurity Resilience Platform integrates advanced triage into our MDR services to address email threats quickly and eliminate false positives. Our cybersecurity analysts check and analyze clusters of emails flagged as suspicious, and if an email is deemed dangerous the indicators of compromise are provided to help with mitigation.

Compliance & Reporting Support

Cybersecurity compliance is a key factor in many industries and producing the proper reports and logging protocols necessary can be cumbersome and time consuming for many organizations.
Lumifi helps companies in various industries cover compliance mandates such as HIPPA, HITECH, PCI DSS, Sarbanes-Oxley, EU GDPR, CCPA and more. Our Security Operations Center is certified SSAE 18 SOC 2 Type II and prepared to help clients of all industries meet their cybersecurity compliance requirements.