LUNAVI

SIEM Services with Azure Sentinel

Monitor and Respond to Security Events - Anywhere

Our team of information security experts stand ready to implement Security Information and Event Management (SIEM) for your cloud-hosted, colocated, or on-premises infrastructure, applications, and data, using the power of Azure Sentinel.

SIEM Services from Lunavi include monitoring of your systems for anomalies, analyzing the risk of any identified threats, and responding to security threats with incident response protocols to minimize and eliminate security incidents and breaches.

By using Azure Sentinel, we can ingest and analyze data from any source, including Lunavi's gBlock Cloud, Microsoft Azure hosted environments, and even your on-prem data center.

This completely managed SIEM solution includes:

- Identification of attacks before they turn into a full-blown security incident or breach
- Mitigation of any identified attacks
- Rectifying misconfigured security resources such as firewalls
- Reduced time to remediation when incidents and breaches occur
- 24/7/365 network security monitoring (NSM) and endpoint detection and response (EDR)
- Threat intelligence and incident response services
- Custom SIEM dashboards displaying security data, events, and status of all endpoints across your managed environments.

Gold
Microsoft Partner
Microsoft

Azure
Expert
MSP

Lunavi manages an Azure Sentinel instance on your behalf, delivering managed SIEM services that include:

Data Collection

Sentinel scans, aggregates, and reports on information from all your users, applications, and infrastructure, regardless of where they are hosted.

Threat Detection

Analytics and Artificial Intelligence features built into Sentinel enables the detection of known threats and minimization of false positives, so you can focus on remediation.

Forensics and Investigation

Dig into security reporting on your environment to discover suspicious activities, threat vectors, and audit trails.

Cloud-Scale Security

Gain unprecedented platform scalability, enabling comprehensive querying and storage of security data even in the largest cloud environments, while simultaneously right-sizing your security environment and only paying for what you need.

Incident Response

Rapid response to security events is facilitated with orchestration and automation tools, quickly removing threats and protecting your sensitive apps and data.

Office 365 Integration

Connect your Microsoft products quickly and easily, including complimentary importing of Office 365 or Microsoft 365 data.

SEIM Optimization

Lunavi is intimately familiar with both Sentinel and Azure services at large, enabling cost optimizations including reservation tiers and audits that can dramatically reduce your monthly spend.

Additional Services

Need a comprehensive infosec solution? Lunavi can help with endpoint protection, DAST, phishing training, vulnerability assessments, and more.

LUNAVI

www.lunavi.com