LTIMindtree

Case Study

Alert Monitoring Using Captive SIEM

Client

The client American multinational energy company

Challenges

The client faced the following challenges:

- Absence of actionable intelligence and structured response mechanisms for cyber threats due to unavailability of monitoring support personnel
- Lack of visibility in the coverage of the monitoring scope, giving rise to unmonitored pockets that were susceptible to cyber attacks

LTIMindtree Solution

- Reviewed SIEM configuration and integrated additional systems for alert monitoring
- Established standard operating procedures and automated run-books for response to cyber security incidents
- Performed threat investigation, triaging, and remediation involving various asset owners

Business Benefits

- Optimized 150+ rules and 60,000+ false positives leading to 9000 actionable alerts per day
- Enhanced coverage/visibility in monitoring through expanded scope of devices with well defined, SLA-based processes for response to cyber Incidents