LTI

Let's Solve

Case Study

Alert Monitoring using Captive SIEM

A Larsen & Toubro Group Company

Client

American Multinational Energy Co

Challenges

The client faced following challenges

- Absence of actionable intelligence & 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

LTI 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 Delivered

- 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

info@Lntinfotech.com