

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

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 84,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit <https://www.ltimindtree.com/>

