



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

LTI (NSE: LTI, BSE: 540005) is a global technology consulting and digital solutions company helping more than 300 clients succeed in a converging world. With operations in 29 countries, we go the extra mile for our clients and accelerate their digital transformation with LTI's Mosaic platform enabling their mobile, social, analytics, IoT and cloud journeys. Founded in 1997 as a subsidiary of Larsen & Toubro Limited, our unique heritage gives us unrivaled real-world expertise to solve the most complex challenges of enterprises across all industries. Each day, our team of more than 25,000 LTItes enable our clients to improve the effectiveness of their business and technology operations, and deliver value to their customers, employees and shareholders. Find more at www.Ltinfotech.com or follow us at @LTI_Global