LTI

Let's Solve

Case Study

Network Behavior Anomaly Detection

A Larsen & Toubro Group Company

Client

An IT Service Provider from India

Challenges

The challenges client faces:

- SIEM in place but finding the alert monitoring mechanisms constrained as it did not lead to deep dive threat hunting on the available logs.

LTI Solution

- Deployment of Cyber Analytics Platform along with data collectors near key networking switches & Configuration to detect behavioral anomalies based upon rules & models
- Monitoring of anomalies and investigation of the alerts generated by the platform
- Kill chain based threat hunting using queries and multi-dimensional analysis

Business Benefits Delivered

- Effective Anomalies Detection based upon User Risk Profile, Assets accessed by the User, Network Sessions & External Threat Intelligence

info@Lntinfotech.com