LTIMindtree

Case Study

Network Behavior Anomaly Detection

Client

The client is an IT service provider from India

Challenges

The challenges client faced:

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

LTIMindtree Solution

- Deployment of cyber analytics platform along with data collectors near key networking switches and configuration to detect behavioral anomalies based upon rules and 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

- Effective anomalies detection based upon user risk profile, assets accessed by the user, network sessions and external threat intelligence