



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

---

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](http://www.Ltinfotech.com) or follow us at @LTI\_Global