

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

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/>

