LTIMindtree

LTIMindtree's Threat Hunting Service

Traditional security monitoring is proving to be insufficient in today's fast-paced digital world of Cloud, Mobile, IoT, and advanced threat landscape. With increasing velocity and volume of data, traditional security monitoring solutions are overwhelmed, and require enormous time and effort to write and maintain rules to detect known threats.

Detection of unknown threats is beyond the capability of traditional security monitoring solutions. Thus, the need of the hour is to identify known and unknown threats as quickly as possible, and contain the spread and impact of the infection. This is also known as Threat Hunting, which is a proactive way of looking for threats, using internal and external threat intelligence, hypothesis-based information mining and analysis, advanced malware analysis and behavior analysis.

LTIMindtree's Threat Hunting Service

LTIMindtree's Threat Hunting service proactively helps to protect the organization's infrastructure and assets from a wide range of threats. Our Threat Hunting Service offerings include:

- **24x7 Threat Hunting**
- **Threat Advisory Services**
- **Advanced Malware Analysis**
- **Advisory & Consulting**

Organizations can maintain continuous threat awareness, enhance and strengthen security monitoring based on the outcome of threat hunting and educate user community with advisories.

Service Features

LTIMindtree's Threat Hunting service analyzes the environment for unknown threats through both User behavior and Network behavior analysis across 50+ behavioral dimensions. Its "Active Learning" feature enables analysts to apply feedback recorded on an anomaly to other similar anomalies automatically, thus increasing the efficiency and reducing false positives. Key features of the Threat Hunting Service include:

User Behavior Analysis

Real-time log enrichment to provide full user behavior analysis for threat detection and search.

Network Behavior Analysis

Predictive Analytics to identify anomalous behavior and assist hunting.

Malware Detection

Perform real-time threat hunting to respond to ransomware and other emerging threats.

Threat Intelligence Feeds

Researches and validates vulnerabilities, applicability of the potential malicious activity and map to client's assets for proactive protection.

Prescriptive Analytics

LTIMindtree's Threat Hunting platform leverages deep learning methods to dynamically baseline normal behaviors as whitelists.

Advanced Malware Analysis

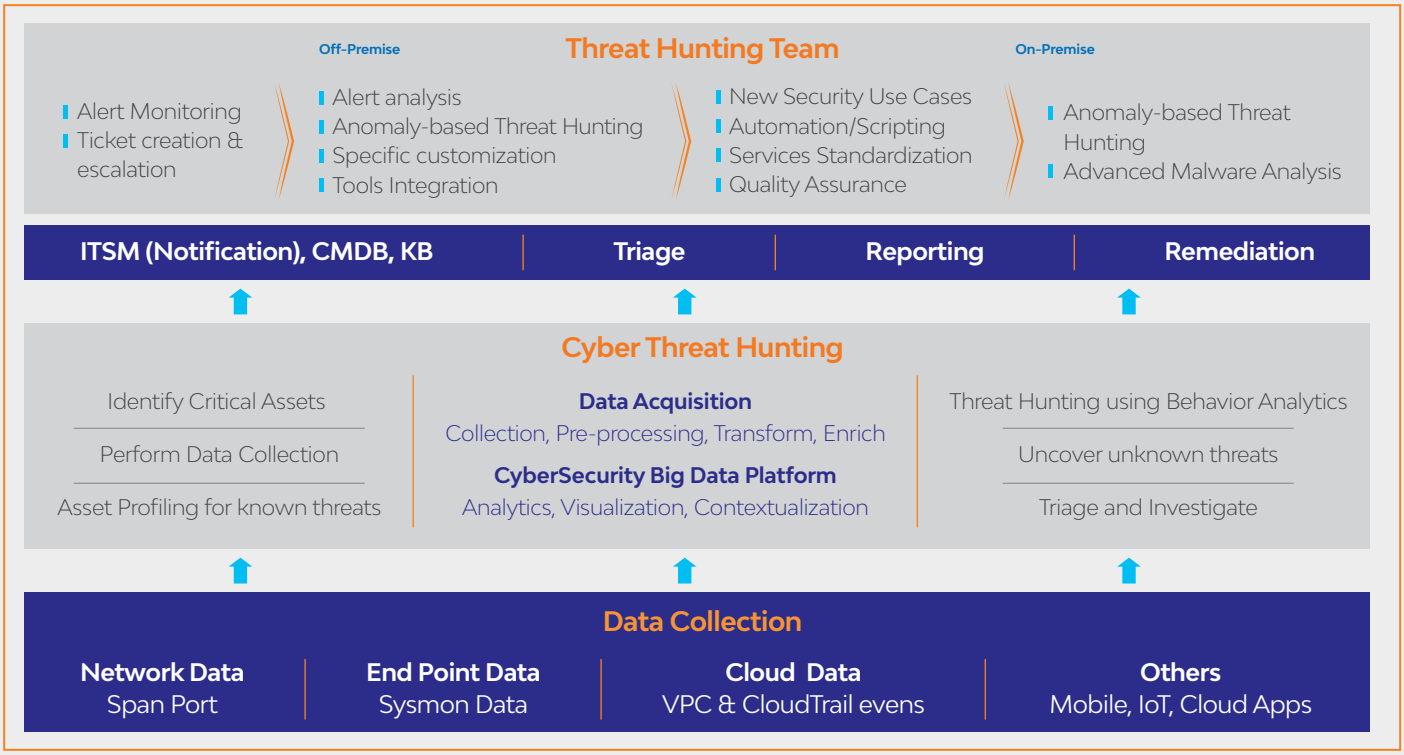
Discovers malicious activity | Determines sophistication level of an intruder | Identifies vulnerability | Catches the "Bad Guy"

Service Delivery Model

LTIMindtree's Threat Hunting service is offered as a Managed Service from Cyber Defense Resiliency Centers (CRDC), located in India and Canada. A specialized team of Threat Hunters monitor the environment on 24x7 basis, who help in identification and detection of both known and unknown threats on real-time basis within the integrated data sources (network span port, sysmon data for endpoints, etc.).

Once the threat is identified based on deep threat analysis, an incident is created with the local IT team to remediate the threat along with required and recommended resolutions. The resolution and feedback from local IT team is incorporated within the threat hunting platform. Both explicit feedback and Active Learning algorithms help in reducing false positives, thus increasing the effectiveness of the threat hunting team.

Integrated dashboards available as integral component of the platform help analyze threats based on user and network behavior and machine learnings available within the platform.



Benefits of Threat Hunting Services

LTIMindtree's Threat Hunting service reduces the security gaps by providing real-time visibility & robust threat intelligence that can help proactively prevent attacks in real-time, before a breach.

Key benefits of the services include:

Proactive threat detection and resolution	Identification of unknown threats	Faster detection of threats	Proactive reduction in attack surface area available to hackers

About LTIMindtree

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 — solves the most complex business challenges and delivers transformation at scale. For more information, please visit https://www.ltimindtree.com/.