LTIMindtree Threat Detection Service

LTIMindtree

With constantly changing Threat landscape due to changing business needs and adapting to cloud and mobile based platforms, organizations need to protect themselves against some of the advanced and sophisticated threats in the cyber security area. The adoption of new platform also increases the exposed attack surface and many of the solutions are point solutions working in silos within the environment.

A comprehensive and integrated threat detection solution enables identification, detection and response to various threats originating from multiple point solutions, and from different sources through a single pane of glass.

LTIMindtree's Threat Detection Service

LTIMindtree's Threat Detection Service enables identification and detection of threats that may intentionally or accidentally exploit a vulnerability causing a potential financial, data or reputation loss to the organization. This service enables threat identification through real-time and historical collection of data from different data sources integrating multiple point solutions and assets within the organization.

Service Features

LTIMindtree's Threat Detection service provides 24x7x365 continuous monitoring against threats enabling faster detection and response to threats. The service constitutes 200+ predefined use cases yielding early benefits to customers and the underlying platform is equipped to integrate and collect logs from more than 300 different type of data sources making it an integral security monitoring solution. Threat Intelligence feeds enriches the monitoring solution to identify the latest threats within the cyber security area. This service provides comprehensive reporting dashboard for MIS reports and supports audit and compliance requirements.
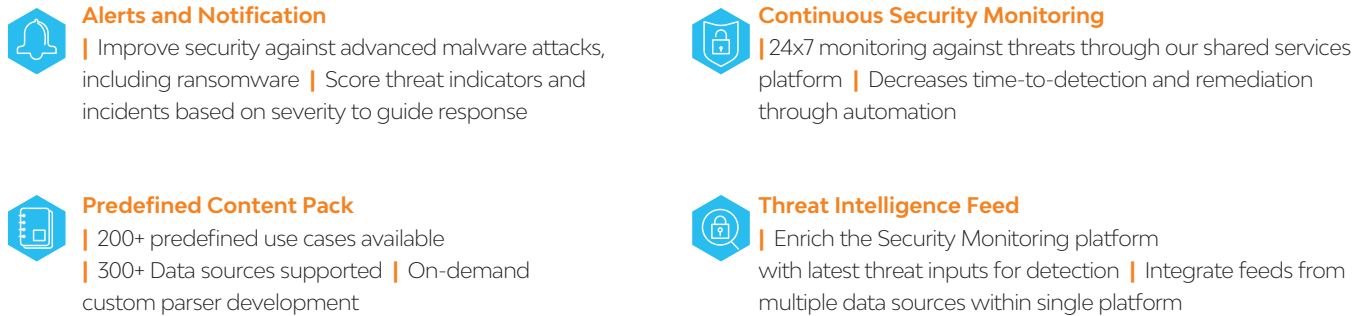
Reporting
| Security Incident report containing details, risk and remediation status
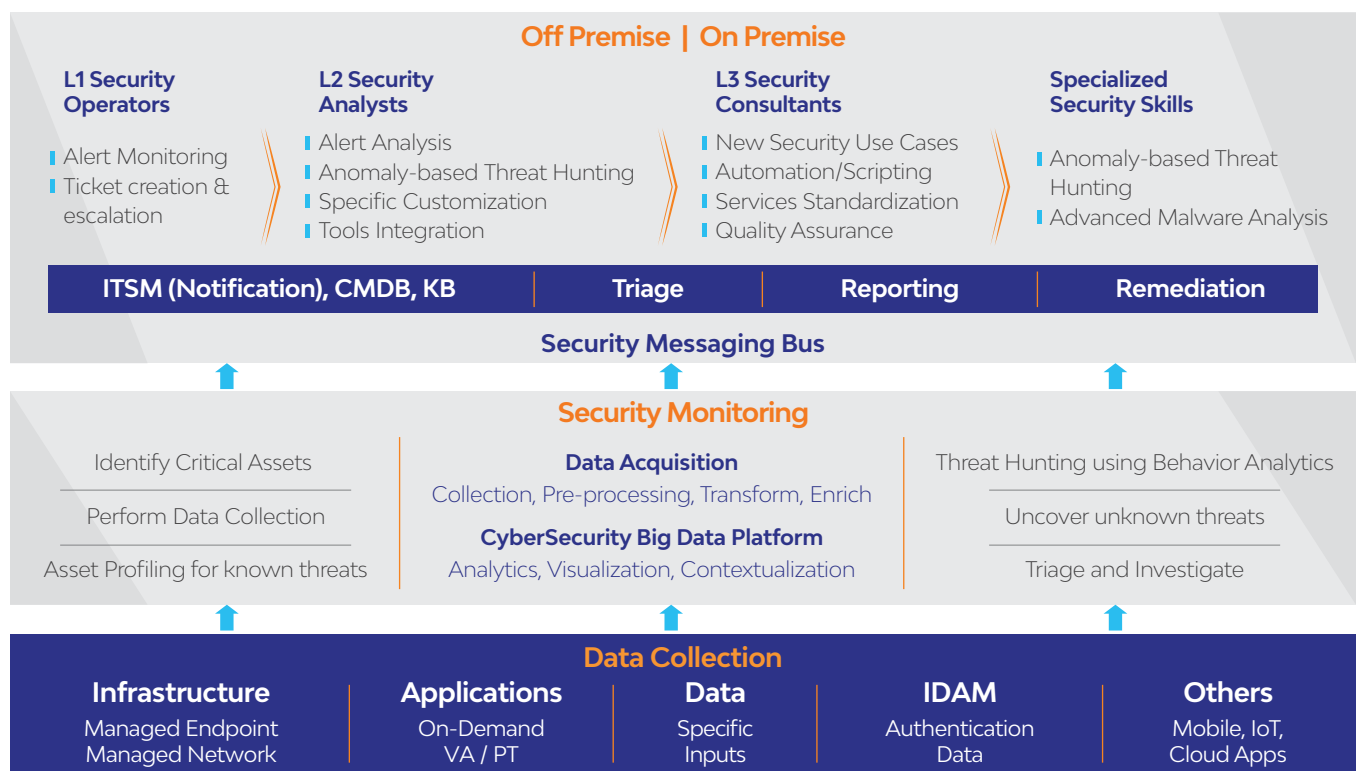| Risk and Compliance report | MIS Reports

Technology Integration
| Correlates network and endpoint insights for enterprise-grade threat visibility | Works alongside existing AV solutions with no impact on endpoint performance

Alerts and Notification
| Improve security against advanced malware attacks, including ransomware | Score threat indicators and incidents based on severity to guide response

Continuous Security Monitoring
| 24x7 monitoring against threats through our shared services platform | Decreases time-to-detection and remediation through automation

Predefined Content Pack
| 200+ predefined use cases available
| 300+ Data sources supported | On-demand custom parser development

Threat Intelligence Feed
| Enrich the Security Monitoring platform with latest threat inputs for detection | Integrate feeds from multiple data sources within single platform

Service Delivery Model

LTIMindtree's Threat Detection service is offered as a Managed Service from our Cyber Defense Resiliency Centres (CDRC) located in India and Canada. A highly skilled team of trained and certified resources monitor the environment on 24x7x365 basis, who helps in identification and detection of threats on real-time basis within the integrated data sources, such as endpoints and network security devices both on-premise and on cloud. Security analysts coordinate with resolver teams to resolve security incidents and incorporate feedback to reduce false-positives to increase efficiency.

Off Premise | On Premise

L1 Security Operators
| Alert Monitoring
| Ticket creation & escalation

L2 Security Analysts
| Alert Analysis
| Anomaly-based Threat Hunting
| Specific Customization
| Tools Integration

L3 Security Consultants
| New Security Use Cases
| Automation/Scripting
| Services Standardization
| Quality Assurance

Specialized Security Skills
| Anomaly-based Threat Hunting
| Advanced Malware Analysis

| ITSM (Notification), CMDB, KB | Triage | Reporting | Remediation |

Security Messaging Bus

Security Monitoring

Identify Critical Assets

Perform Data Collection

Asset Profiling for known threats

Data Acquisition
Collection, Pre-processing, Transform, Enrich

CyberSecurity Big Data Platform
Analytics, Visualization, Contextualization

Threat Hunting using Behavior Analytics

Uncover unknown threats

Triage and Investigate

Data Collection

| **Infrastructure** | **Applications** | **Data** | **IDAM** | **Others** |
| Managed Endpoint Managed Network | On-Demand VA / PT | Specific Inputs | Authentication Data | Mobile, IoT, Cloud Apps |

This service provides customers a comprehensive CDRC portal with which customers can view their security posture, reporting dashboards and provide feedback to our analysts.

LTIMindtree

Benefits of Threat Detection Service

LTIMindtree's Threat Detection service enables threat detection through real-time monitoring for integrated data sources and using threat intelligence feed sources.

Key benefits of the service include:

1 | Faster onboarding through predefined content pack

2 | SLA and KPI-driven metrics

3 | Single pane of glass for security status

4 | Offline and online log storage for audit and compliance

5 | Periodic review and finetuning of correlation rules

6 | Cost-effective leveraging shared delivery model

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/.**