



LTIMindtree's Threat Intelligence Platform and Service

Transform your data security by putting real-time intelligence at the core of every decision

Cyber threats to an enterprise are getting more sophisticated and organized, and even with the best of firewalls, IPS, and other security systems, organizations still suffer security breaches. That's because the volume and variety of security threats can overwhelm security teams and the infrastructure.

Threat Intelligence as a service provides real-time intelligence for preemptive protection and enables multi-layered protection against known and unknown vectors. By leveraging a combination of machine and human analysis, LTIMindtree fuses open-source, dark web, technical sources, and original research to dynamically link and update intelligence in real-time.

You Can Control Only What You Can See

In many enterprises today, intelligence and data security are out of sync. Teams and objectives are siloed, the response is slow and reactionary, and analyses lack relevance, resulting in lost time and wasted resources. IT teams usually take a reactive or compliance-driven approach to data security with no blueprint for preventing attacks before they can breach through.

Attack vectors found by the IT security system may contain several steps and each threat can originate from a different hacking method. To drive down risk while achieving meaningful operational outcomes, intelligence must be embedded into the core of every security workflow, function, and decision.

What if there was a security system cognizant of hundreds of different threat scenarios that could lead to a cyber-attack? A system that employed a unified approach for collecting, analyzing, and automating data and insights to proactively stop a cyber-attack.

LTIMindtree's Threat Intelligence Service

This is more than an offering – rather, it's a philosophy for how we empower our clients with the intelligence they need to drive every security initiative and strategic decision across their organizations. Our Threat Intelligence solution is your first line of defense against potential cyber-attacks. It creates outcomes that can be consumed by analysts and integrated with security systems to proactively reduce security risks.

Comprehensive Threat Overview

We believe that to fully benefit from the power of Threat Intelligence, you must source the right threat data, discover and implement the right process and methodologies, implement automation, and improve information sharing both with external and internal stakeholders.

We protect you by monitoring your external risk profile, aggregating and analyzing thousands of threats, and automating risk mitigation. Our data-mining algorithms and machine learning (ML) capabilities continuously scan the cyber world to deliver actionable, contextual reconnaissance about potential threats to your organization and seamlessly integrate with your existing security solutions to eliminate operational vulnerabilities, secure data, and protect resources.

Get answers to questions like:

- ✓ What are your security systems detecting?
- ✓ Who poses a threat to your business?
- ✓ What is your threat landscape?
- ✓ What tools can be used to attack your organization and how?
- ✓ Is your security system robust enough to withstand a cyber-attack?
- ✓ What security measures should be taken to ensure adequate protection?

Key Features

LTIMindtree’s Threat Intelligence solution can be deployed on-premises or in the cloud as per your requirements. Our service includes:

-  Monitoring and gathering of information and intelligence from multiple sources, including geopolitical risks and external threats.
-  Contextualization and classification of gathered information for actionable intel.
-  Prioritization of threat intel based on client’s threat landscape.
-  Detailed malware analysis including safe execution, payload analysis and recommendations for preventive measures.
-  AI/ ML driven analysis of collated intelligence to remove false positives and add relevance
-  Use of security intel to improve visibility and output, automate response, and amplify value across multiple distinct, strategic solution areas

Darknet

Persona based deep access to restricted/ invite-only areas

Reporting

Multi-Review robust publishing process



Attack Surface

Monitor customer attack surface

Automation

Credential leak/ Card leak monitoring

Reporting Methodology



- ✓ Detailed information about threats discovered by LTIMindtree from a variety of sources such as the Darknet, media articles, security blogs, social media, etc.
- ✓ Advisory report for frequent delivery of information on an ongoing cyber-attack which is reported or expected in the future.
- ✓ Bulletin reports with weekly/ fortnightly summary of threats such as summaries of vulnerabilities, threats round-up, attacker IPs observed on Honeypot sensors, etc.
- ✓ Guidance report for advice on cyber-security best practices and preventive measures to defend against advanced threats.

Use Cases



Brand / Asset / Credential Monitoring



Trend Analysis and Threat Research



Adversary Identification and TTP Alerting



IOC Identification and Enrichment



Vulnerability Identification



Proactive Event Alerting

Why LTIMindtree

- ✓ Lead with intelligence across your security teams, processes, and workflows with security intelligence solutions
- ✓ Real-time transaction data analysis combined with actionable threat intelligence
- ✓ Continuous monitoring and proactive response increase security defenses and help protect infrastructure and services
- ✓ Broad contextual analysis by utilizing advanced analytical techniques
- ✓ Predictable operating costs and reduced operational expenditure
- ✓ ML-driven validation of data among multiple intelligence sources, ensuring maximum security and minimum false-positives.

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/>.