LTIMindtree

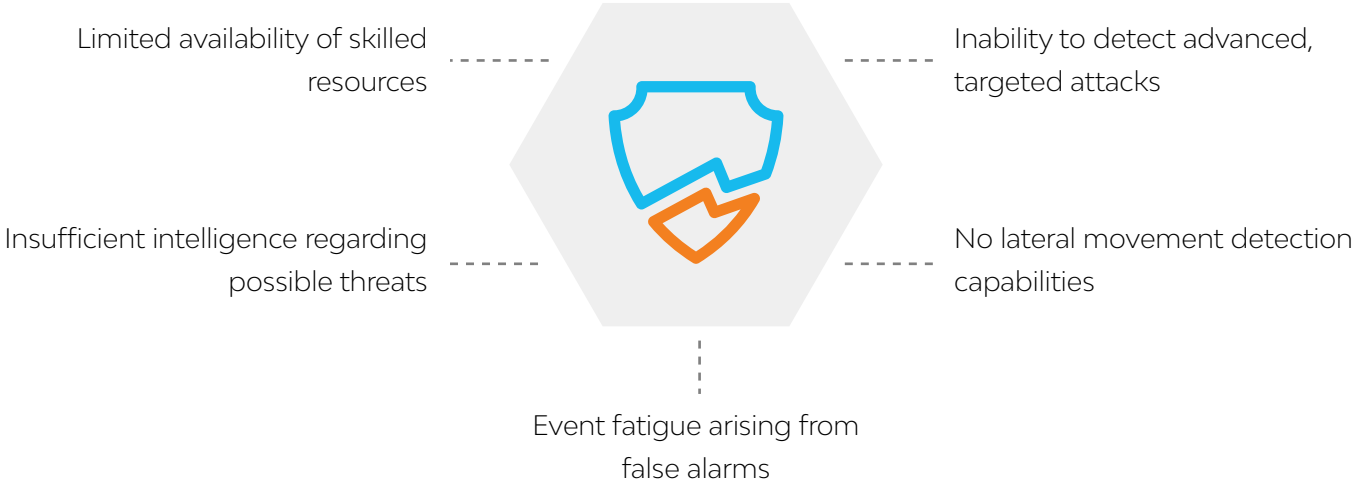
LTIMindtree Threat Deception Services

A Larsen & Toubro Group Company

As hackers and attackers gather more intelligence by the day, they are focusing on mounting targeted attacks against traditional enterprise security solutions. Consequently, organizations with static defense strategies are increasingly becoming vulnerable to cyber attacks. Here are four key reasons why it is easy for hackers to breach defenses:

- Over 360,000 new types of malware are identified on a daily basis
- More than 85% of weekly security alerts received are false alarms
- Current defenses are not equipped to prevent penetration by attackers
- It's extremely difficult to detect intruders in time

Intelligent attacks are difficult to manage if enterprises stick to convention and restrict their defenses to strengthening existing security solutions. In the current scenario, organizations face multiple challenges including:



To overcome these challenges, organizations need an 'Active Defense' that will help them gain control and proactively avert attackes.

LTIMindtree Threat Deception Services

LTIMindtree's Threat Deception services create virtual 'pots of gold' as decoys across your network, drawing the stealthiest hackers away from real assets and enticing them into revealing themselves. Integrated with threat monitoring and hunting systems, these decoys are strategically placed to map out your internet facing infrastructure as low hanging fruits for hackers. This enables accurate discovery of attackers within the first phase of the kill-chain itself.

Our Threat Monitoring and Hunting team at Cyber Defense Resiliency Center (CDRC) leverages deception based alerts to initiate immediate investigation. Deception service helps us to reducethe overall number of alerts, in turn enabling a continuous response mechanism that does not affect the performance of production systems. Moreover, the technology is not 'in-line' with legitimate systems, so it does not affect performance or cause downtime.

LTIMindtree's Threat Deception service suite is available through flexible deployment models, including hardware and virtual appliances, as well as public and private clouds.

Types of Decoys

Threat Intel Decoys: External facing and capable of detecting pre-attack reconnaissance. They generate alerts only on targeted attacks, not random Internet scans.

Threat Magnet Decoys: Dummy credentials inserted into end points sans agents. Lure hackers that are escalating privileges, direct them toward decoy systems, and trigger alerts when used.

Network Decoys: Mock work stations and servers running real services which mimic real database servers, Web applications, file shares and more.

Persona Decoys: Fake personas of high-value employees that are likely to be phished. Detect spear-phishing attacks, and forensically save email evidence.

File Decoys: Microsoft Office documents embedded with a tracker that can be placed on high-value target systems, and capable of raising a silent alarm when opened.

LTIMindtree Threat Deception Approach

Benefits

Business Case	Business Benefits
Improved threat detection	Faster detection directly reduces incident costs.
Higher quality alerts	Reduced cost of triaging alerts, improved security team productivity.
Blind-spot reduction	Improved visibility into currently unmonitored areas, scales easily.
Faster detection time	Reduced average time to detect and remediate threats.
Low friction deployment	Easy to implement quickly without any production impact.

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/.