Brochure

Breach Attack Simulation as a Service

Beat the ‘bad guys’ at their game.
Prepare your network to sustain a cyber attack.

Cyber attacks have evolved dramatically in the past couple of decades regarding their capabilities, scope, fallout, number of targets, etc. Hackers capitalize on human errors like misconfigurations, shadow IT and a lack of awareness to breach an organization's network. They employ legitimate tools and leverage user behavior to infiltrate networks and compromise assets, making any enterprise vulnerable to attacks even with modern security controls and processes in place.

LTIMindtree helps organizations test their security posture from multiple aspects including infrastructure configuration, network vulnerabilities, employee security awareness and security control assessments.

LTIMindtree's Breach Attack Simulation (BAS) Platform can Simulate, Validate and Remediate every hacker's path to your critical assets. Our APT attack simulation platform continuously exposes all attack vectors from breach point to an organization's critical assets, thus acting as a fully automated purple team. The platform addresses real user behavior, poor IT hygiene and security exploits to expose the most critical blind spots.

Key Features

- ✓ Generates automatic simulations of cyber attacks
- ✓ Provides prioritized actionable remediation insights
- ✓ Analyzes cost-effectiveness of potential remediation efforts
- ✓ Increases awareness and know-how of security personnel
- ✓ Continuously updates itself to reflect emerging threats
- ✓ Calculates overall risk score and changes over time
- ✓ Presents a detailed visual display of the attackers' critical paths

Breach & Attack

Identify gaps caused by misconfigurations and human error

See your network like a hacker

Red Teaming

Build or expand your red team

Full APT simulation

Comprehensive up-to-date attack methods

Auto Pen Test

Run continuously

Simulate full attack cycles

Support red and blue team priorities

LTIMindtree's Breach Attack Simulation Platform

The attack vectors found by our advanced decision-making engine may contain several steps, with each vector originating from a different hacking method. The platform assumes that the network's perimeter has been breached, and the peripheral security mechanisms have been compromised. It then tests an attacker's ability to compromise the network towards its strategic assets by mimicking real-life hacker behavior. Once an attack mission has been configured, the system performs all possible attacks by hackers, based on LTIMindtree's deep research of hacking behavior, to compromise the selected targets. The continuous loop of automated red teaming is completed by ongoing and prioritized actionable remediation of security gaps.

LTIMindtree's BAS Platforms allows IT security managers to configure periodic attack missions based on parameters like:

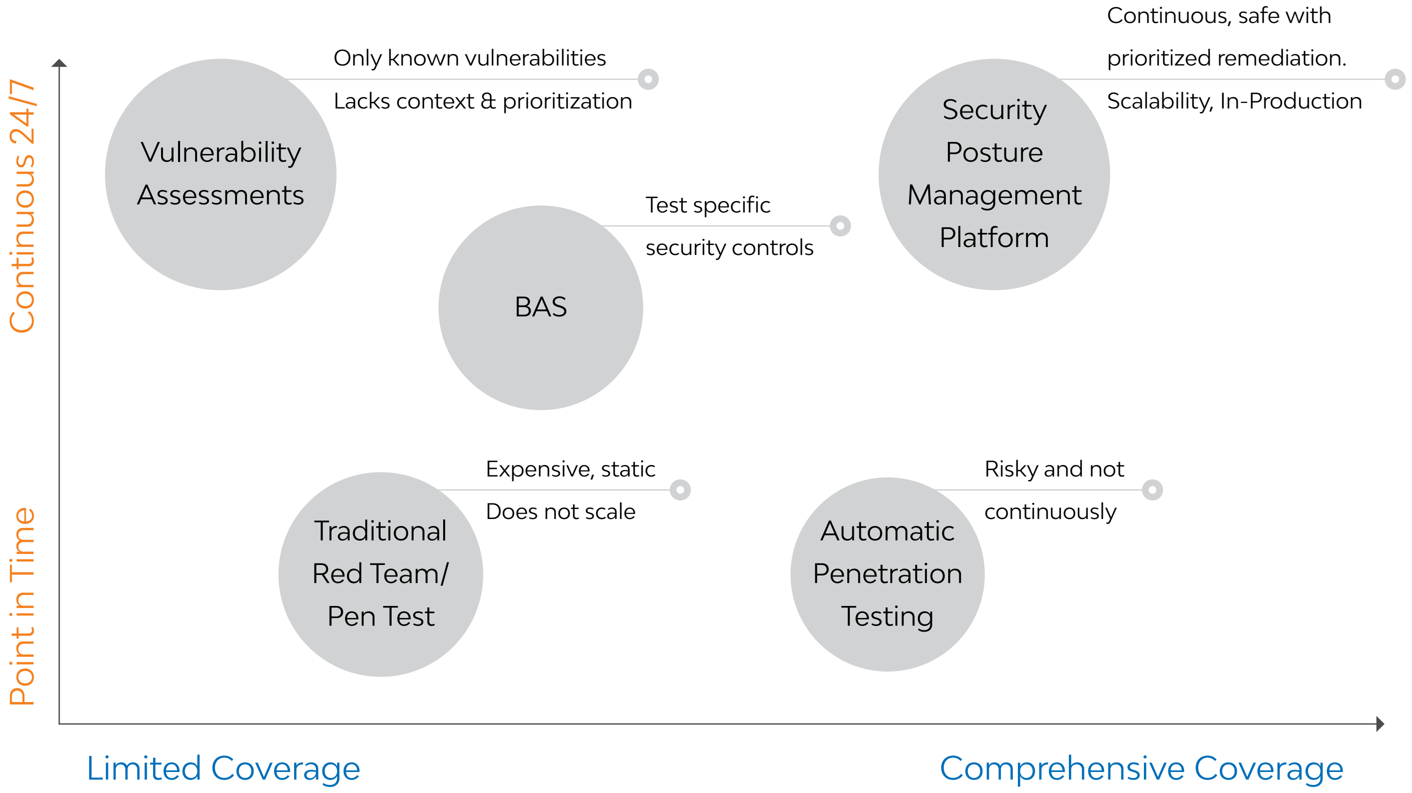
- Attacker's capabilities and toolset
- Potential breach points in the network
- Attack targets
    - Network-related asset
    - Device asset
    - Data asset

Key Benefits

- ✓ 100% awareness of all possible attack paths
  - o Continuously identifies attack vectors to your target assets 24×7
  - o Simulates attacks using latest tools and techniques
- ✓ Finds gaps that expose your critical assets
  - o Spots misconfigurations, unapplied patches, and software vulnerabilities
  - o Tests vulnerabilities, user access issues and other IT-related risks
- ✓ Delivers higher efficiencies
  - o Prioritizes remediation tasks around risk and exposure
  - o Build/ expand internal red and blue teams
- ✓ Manages security risks
  - o Provides a breach impact risk score to insurance, legal, board members, etc.
  - o Evaluates hardiness of existing security investment

Why LTIMindtree

Current marketplace offerings and LTIMindtree's platform


Continuous, safe with
prioritized remediation.
Scalability, In-Production
Only known vulnerabilities
Lacks context & prioritization
Vulnerability Assessments
Security Posture Management Platform
Test specific
security controls
BAS
Continuous 24/7
Expensive, static
Does not scale
Risky and not
continuously
Traditional Red Team/ Pen Test
Automatic Penetration Testing
Point in Time
Limited Coverage
Comprehensive Coverage

- Extensible software-based platform
- Easy to deploy and activate
- Generates automatic simulations of cyber attacks
- Provides prioritized actionable remediation insights
- Analyzes cost-effectiveness of potential remediation efforts
- Increases awareness and know-how of security personnel
- Continuously updated to reflect emerging threats
- Calculates overall risk score and changes over time
- Provides 24×7 support from different locations globally

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/.**