LTIMindtree

Brochure

Modernize Your SOC with **LTIMindtree's Active Cyber Defense Resiliency**

Overview

In our hyper-connected world of ‘Internet’, ‘things’, and ‘us’, we are becoming increasingly reliant on intelligent software solutions infused with autonomous algorithms, drones combining IoT, Mobility, and Robotics in every walk of our business and life. We are now a component in many of these ”Internet + Everything” scenarios.

With the exponential rise of Internet of Everything, Cloud-native Digital transformation, and the DevOps movement, the number of unknown advanced persistent cyberattacks and incidents have increased multi-fold. Also, there is a continuous decline in the time at hand to respond to these incidents and breaches. Thus, organizations are struggling to maintain their cyber defense posture to ensure threats are kept at bay.

Organizations need a paradigm shift in their cybersecurity strategy, to be one step ahead of threat actors including state-sponsored adversaries in this digital era. LTIMindtree envisions an Active Cyber Defense Resiliency approach, where the system identifies, detects, protects, investigates, hunts, responds, and remediates ”the Internet + Things + us” in real-time and secures “Internet + Everything.”

LTIMindtree's Cyber Security for the Digital World

An Evolving and Emerging Standard of Active Cyber Defense Resiliency

The New Way: 4 Pillars that augment Active Cyber Defense Resiliency

Cyber Defense

Active and Cognitive Threat Defense

Automated and AI/ML-driven pre-configured threat defense with identification, protection, detection, investigation, learn and recover, and automated response/recovery.

Cloud Threat Defense

Multi-cloud Threat Defense and Resiliency

Real-time cloud security governance, control, visibility, and management.

Digital Trust

Digital Identity, Things and Data Protection

With right user and right things, along with right access for right data and right reason.

Digital Defense

Real-time Cyber Defense for Things

Convergent cyber defense, secure access, automated discovery, and risk mitigation for Internet of Everything.

Powered by

X-CDR (Cyber Defense Resiliency) XaaS Benefits –

- Adopting a service-led approach will help organizations achieve economies as service providers broad-base their offerings and make them more fungible.
- Everything-as-a-Service enables businesses to focus on their core competence and reduce costs.
- Service standardization helps deliver more predictability and bring about efficiency

LTIMindtree Cyber Defense Service Offerings

Security Orchestration and Automation	✓ Integrated & Agile incident management services ✓ Synchronized Security Policy Management ✓ 24x7 monitoring and support services ✓ Governance for threat response and recovery with CCMP
Cyber Defense Response and Recovery	✓ AI/ML-driven digital forensics ✓ Cyber event-driven recovery with network, application, and data instance visibility analysis
Threat Prevention and Detection	✓ Identification and implementation of controls in perimeter, network, endpoint, application, data, cloud, and mobile ✓ MITRE ATT&CK® based co-relation ✓ 24x7 security monitoring, triage, alert handling, use-case engineering, intelligence-led cyber operations, and coordinated Incident Response
Active Threat Intelligence	✓ Contextual threat intelligence integration & analysis ✓ Brand protection and takedown ✓ Cyber defense attack and protect surface profiling
Cyber Analytics	✓ Security big data lake ✓ AI/ML-driven threat hunting ✓ Predictive and prescriptive cyber analytics

Threat Hunting and Investigation

- User and entity behavior analytics
- Packet capture-based behavior analytics
- Network behavior analytics
- Anti-phishing/Anti-malware analytics

Breach Attack Remediation

- Threat deception
- Cyber risk posture
- Compromise assessment and remediation
- Zero trust and micro-segmentation

Advance Threat and Vulnerability Management

- Infrastructure vulnerability management
- Application vulnerability management
- Cloud vulnerability management
- Vulnerability orchestration and automation
- Specialized testing for IoT/OT
- SecDevOps-as-a-Service with ASOC

LTIMindtree Digital Trust Service Offerings

Strategic Design

- Maturity assessment
- Roadmap definition
- Technology evaluation
- Application assessment
- Business case evaluation

Implementation -Integration

- ✓ Technology implementation
- ✓ Application integration
- ✓ Custom development
- ✓ Technology migration
- ✓ RPA-based automation implementation
- ✓ SOD design and implementation

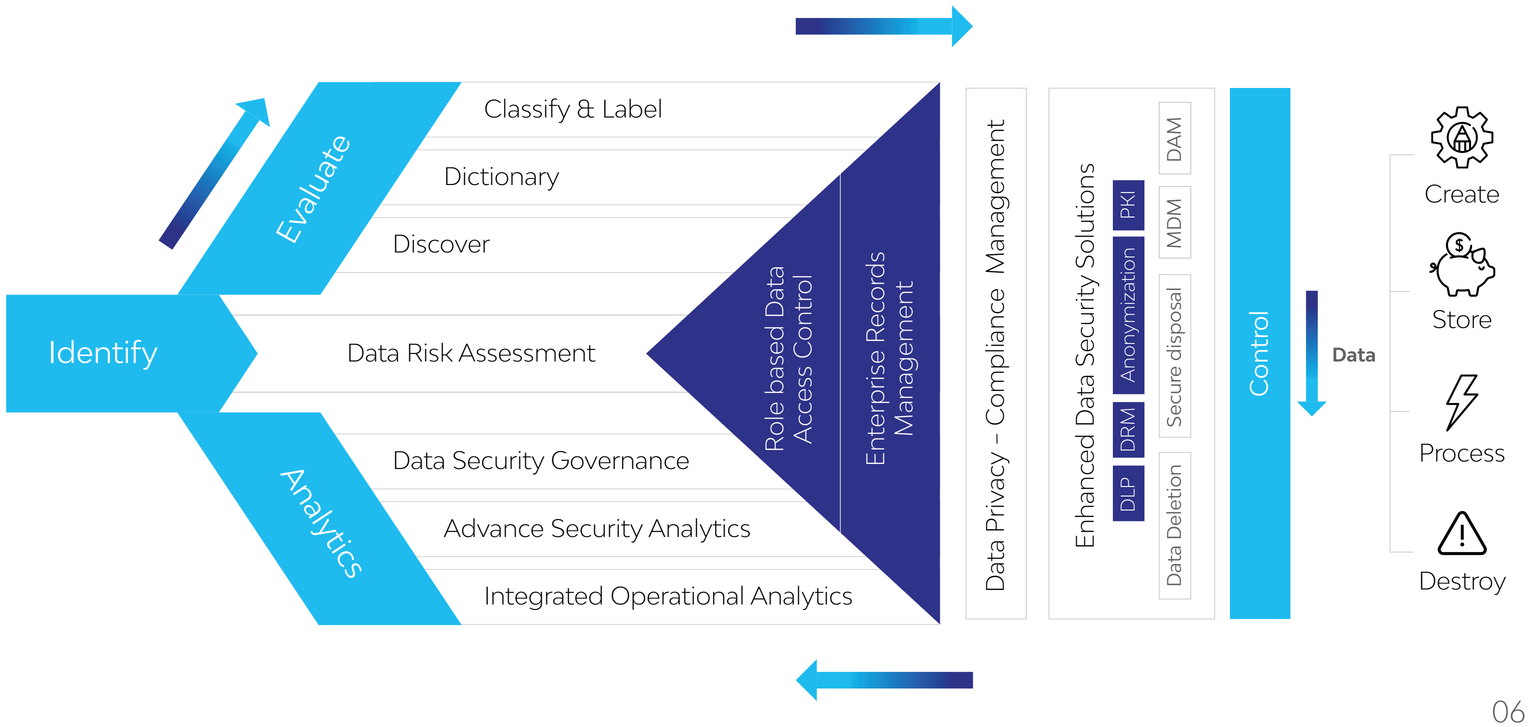
Operations

- ✓ IAM platform management
- ✓ Manual identity operations
- ✓ Automated identity operations
- ✓ Identity governance operations

Digital-as-a-Service

- ✓ Digital SOD-as-a-Service
- ✓ Digital identity governance and administration-as-a-service
- ✓ Digital self-defending key management-as-a-service

Data Assurance Framework – for Information Protection



LTIMindtree Digital Defense Service Offerings

Risk/Hazard Assessment and Risk Strategy Definition

- Vendor review
- Security & risk/hazard assessment of OT/IoT/IIoT ecosystem/application/smart buildings/smart cities
- Security program maturity assessment
- Penetration test
- Red team
- Vulnerability assessment
- Risk management strategy definition

Security Architecture and Design

- Product security architecture
- OT security architecture
- Edge security architecture
- Security architecture design for digital initiatives
- Secure application design

Technology Implementation /Integration (OT/IoT/IIoT)

- Security control evaluation
- Security control implementation
- Micro/Pico segmentation implementation
- Custom integration development and deployment

Managed Security Services

- 24x7 security monitoring for OT/IoT/IIoT
- ecosystems
- Threat detection and remediation
- Recovery services
- Fuzz testing
- Key management services
- Threat hunting
- Threat containment, eradication, and recovery

Digital Forensic Services

- Incident analysis
- Evidence gathering
- Analysis
- Root cause & remediation identification

Attain the right level of Cyber-maturity with LTIMindtree's purpose-built Active Cyber Defense Resiliency approach

Foundation CDR Services Threat Prevention and Detection	Next Generation CDR Services Advanced Threat Detection and Defense	Active CDR Services Adversary Emulation and Recovery	Digital CDR Services Digital SOC for digital Trust
Security Monitoring & Incident Response	**Advanced Threat Detection and Defense**	**Adversary Emulation and Recovery**	**Cyber-Digital Convergence and Assurance**
SIEM Monitoring on 24 x 7 basis with device management Threat Detection and Security Alert Management EDR, Infra, and Network Security E-mail security for monitoring Generic Threat Intel	UEBA with SBDL Contextual Threat Intel with Threat Intel Platform Augmented Incident Response with SOAR Augmented Threat Detection with NBA or NTA and PCAP Proactive Threat Detection and Incident Response with Threat Hunting	Adversary Emulation& Incident Response through Continuous Red & Blue Teaming Breach Attack Response Real Time Attack Surface Visibility Cyber Recovery Cyber Risk Management Threat Deception Cyber Awareness SASE and Micro segmentation	Advanced Threat Detection & Defense Proactive Advisories and Remediation Assistance Rapid Response and Recovery Vulnerability Management, Authentication and Encryption Value Added Service Offering with Specialized Testing for IOT and OT Device Digital Trust & Assurance
Reactive Cyber Operations Capability	**Reduced Dwell Time of attacks Accelerated Mean Time to Respond**	**Real Time Visibility of Risk & Attack Surface Accelerated Recovery and Response**	**Convergence of the Digital assets - Data & Identities with Cyber SOC**