




NXT

CyberResilience

▶ Secure ▶ Connected ▶ Contextual



Cyberattacks continue to grow in scale and are becoming more advanced. The run-of-the-mill security services are no longer adequate to fight the battle against these new-age cyber threats.

At LTIMindtree, Our focus is on enabling our clients to go beyond “Security for Compliance” to “Security for Cyber Defense Resiliency.” We follow a Managed Cyber Defense Resiliency Services(MCDR) approach. Our well-defined cyber security maturity model is powered by technology-enabled progression towards Intelligent and Autonomous Cyber Defense. This is augmented with real-time attack adversary emulation and proactive remediation to bring together truly Digital Cyber Defense capabilities to tackle the challenges of an advanced threat landscape.



Leaders in ISG provider
Lens Cybersecurity Services
and Solutions 2022 –
USA mid market



Major Contender in Everest
Group's Managed Detection And
Response Services PEAK Matrix®
Assessment 2023



Proactive and
Predictive-First
Cyber Defense
Framework



Cloud and
Analytics /
AI-First
Experience



Active Cyber
Defense Resiliency
across IT, OT / IoT,
People & Process

220+

Active clients
including
25 Fortune
500 org

15

Cyber
Defense CoEs

25

Delivery
Accelerators

3500+

Cybersecurity
specialists

Global Network of Cyber Defense Resiliency Centers (CDRC)

Global Centers. Local Strategies

Our services are delivered through a global network of CDRCs, which operate around the clock, 365 days a year, to provide purpose-built, customizable, and shared services solutions across the end-to-end Cybersecurity value chain.

Toronto,

Canada



New Jersey, Hartford,
Redmond, Phoenix,

US



Warsaw,

Poland

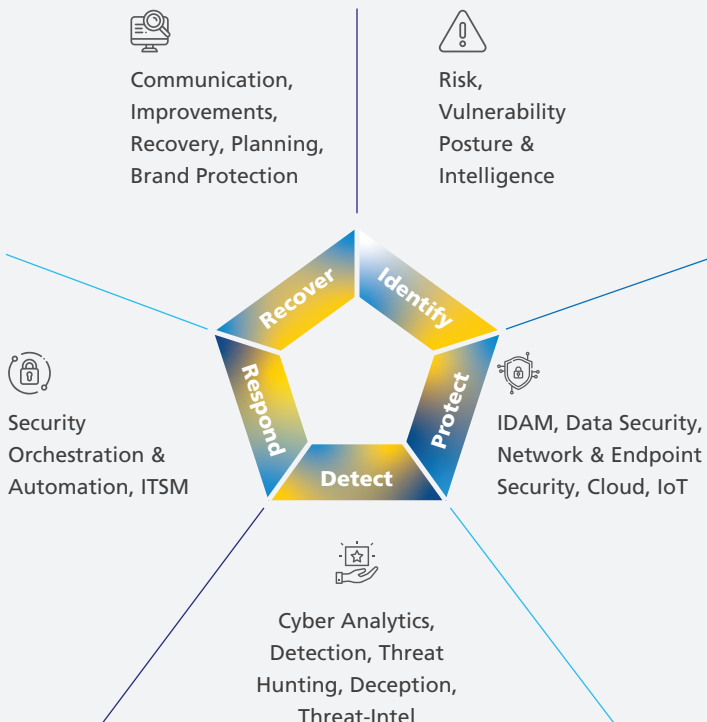


Bangalore,
Mumbai,

India



COE-Driven Approach





Over 25 Alliances across Cyber security

Units for Awareness, Training & Education

Collaboration with Educational Institutions/ Universities

Process & Product Line Training



Cyber Defense Resiliency Services

Active Cyber Defense Resiliency approach to identify, detect, protect, investigates, hunt, respond and remediate Cyber threats



Purpose-built approach to gradually improve from the current to a Digital state



Everything-as-a-Service




25 best of the breed product partnerships



Multi-tenanted Cyber Defense with Platform-based approach



25+ Cyber Defense Resiliency delivery accelerators



Security Orchestration and
Automation Incident
Management, Monitoring
& Support

Cyber Defense Response &
Recovery Digital forensics
and cyber
event-driven Recovery

Threat Prevention and Detection

- Identification and implementation of controls across the landscape
- Monitoring, triage, alert handling, use case engineering, intelligence-led cyber operations, and incident response

Active Threat Intelligence

- Contextual threat Intelligence Analysis

Cyber Analytics

- Threat Hunting, Predictive and Prescriptive Analytics

Threat Hunting & Investigation

- Behavior Analytics
- Anti-Phishing / Anti-Malware Analytics
- MITRE ATT&CK based co-relation

Breach Attack Remediation

- Breach Attack Remediation, Threat Deception
- Compromise Assessment and Remediation

Advance Threat & Vulnerability Management

- Infrastructure /Apps /Cloud Vulnerability Management

Identity and Access Management

Enabling Trusted Digital Enterprises with Digital Identity Assurance & Compliance



Integrated and Converged
Digital Identity Operations



Pre-built standardized processes,
policies and workflows



Accelerators/playbooks and
frameworks for a Zero Trust Roadmap



Domain know-how from
75+ IDAM engagements



Well architected platform with best
of the breed technology product stacks



Assessment & Strategy

IAM Roadmap to
industry
standards

Attestation and Certification

Automated JLM
Access Certification
Data Access
Governance
Cloud Governance

Managed Services

IAM Monitoring,
Support, Operations
and Governance

Privileged Management

Privileged
Administration
& Compliance

Zero Trust

IAM Deployment based
on Zero-trust
Access Risk Management

Value based Integration

Access
Analytic Identity
Intelligence

Applications Security

New-age design, testing, implementation and configuration solutions for fending off application security breaches



Domain Experience to support risk & compliance efforts with cost-effectiveness



Proven approach, listed Accreditations – CREST Penetration Testing Organization



Industry experience with successful client engagements across multiple verticals



Ready-to-use checklists & templates across domains for implementing best practices such as OWASP, NIST, ISO, PCI, SANS, Privacy Laws, etc.



DevSecOps as a Service, AppSec as a Service approach



Technology Evaluation

- Risk based identification / categorization
- Roadmap definition, maturity assessment
- Secure Architecture Review & Threat Modelling

Best Practices and Training

- Secure SDLC Framework
- DevSecOps

Unified Reporting

- Single Pane of glass view for integrated test findings
- Application Security Orchestration and Correlation (ASOC)

Cyber Risk Management

- Quantifiable risk score for every application
- Risk prioritization
- AI/ ML Based Triaging

Security and Compliance Testing

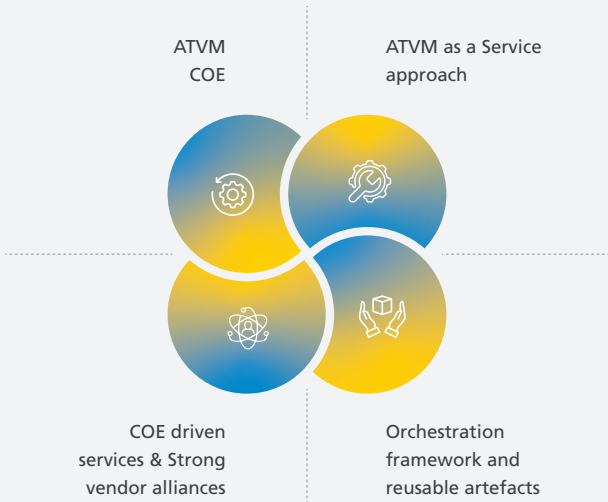
- Static Application Security Testing (SAST)
- Software Composition Analysis (SCA)
- Dynamic Application Security Testing (DAST)
- Threat Modeling, Penetration Testing, API Security, Testing Processes
- Compliance Mapping (OWASP, NIST, etc.)
- Penetration Testing

Threat and Vulnerability Management

- Threat Intel Driven Analysis
- AI/ ML Based Triaging
- Vulnerability Remediation & Advisory

Advance Threat & Vulnerability Management

Closing the Vulnerability Gap





Infrastructure Vulnerability

- Vulnerability assessment
 - Penetration testing
 - Secure configuration review
 - Assessment for compliance
 - Remediation advisory
 - Risk tracking and remediation assistance
-

Application Vulnerability

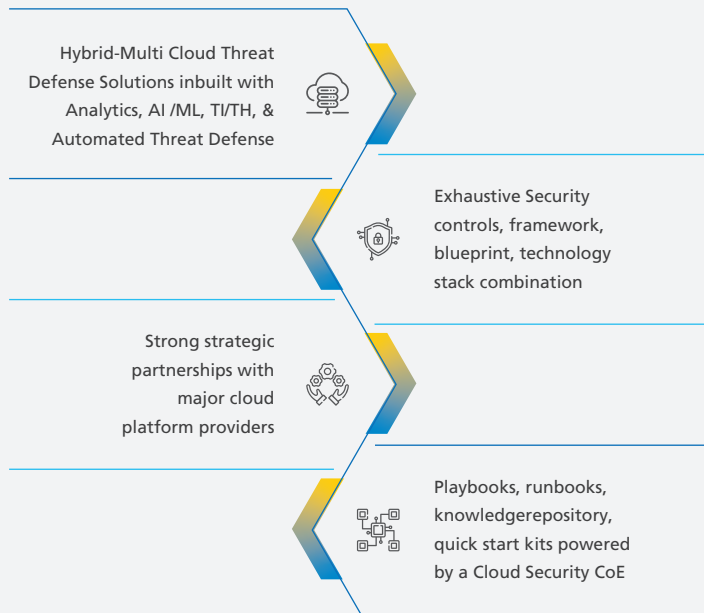
- Static application security testing
 - Dynamic application security testing
 - Penetration testing
 - Open-source security analysis
 - Software composition analysis
 - Threat modeling
 - Remediation advisory
 - Risk tracking and remediation assistance
-

Specialized Vulnerability

- Red Team Tests
- IoT security Testing
- Fuzz testing
- Mobile security testing
- Cloud security testing

Cloud Threat Defense

Secure and govern the hybrid and multi-cloud environment against evolving new-age cyber threats



Cloud Security Operation & Defense

Container,
Kubernetes
Security

Cloud SIEM
& Data Lake

MITRE ATT&CK
detection library

UEBA, IoC/IoA,
& SOAR

Threat Hunting
& Threat
Intelligence

Cloud
Infrastructure
Entitlement,
CASB

Red & Blue
Teaming

Cloud Workload Advanced Threat Detection & Respond

Endpoint Security,
EDR, Network
Micro-Segmentation

Threat & Vulnerability
Management

Data Security,
Labelling, Masking,
Data Loss Prevention

Encryption,
Key Management

File Integrity,
Advanced Automation
& Playbook

Security Threats
Detect and
Response Application
whitelisting

Cloud Security Posture Monitor & Response

Regulatory
Compliance
Management

Network Security
Management

Automation &
Workbook

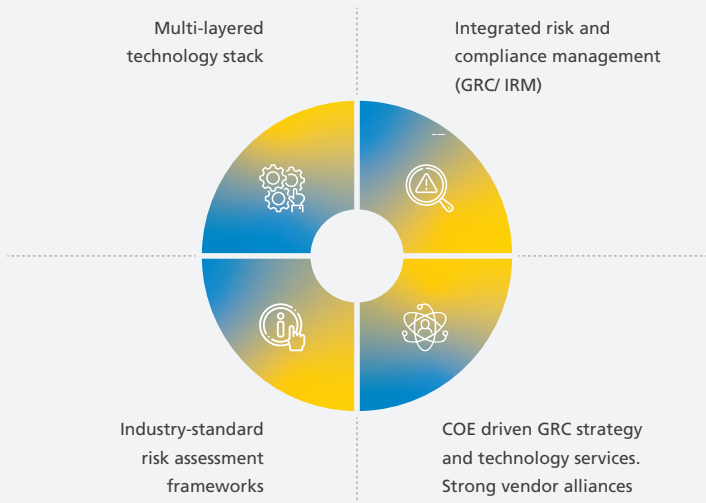
IAM Security
Management

Control
Mapping
Framework

Security
Configuration
Management &
Response

Governance, Risk & Compliance

Manage risks, stay compliant with
evolving regulatory mandates



Governance

Risk Management

Compliance Management

Board and cyber executive advisory

Developing Security baselines/ Policies & Procedures

Cyber defense program development and assessment

Governance reviews and framework evaluation setting

Maturity assessments, benchmarking

Enterprise IT risk management (IRM)

Security risk management

Risk management framework

End-to-end risk management lifecycle of third parties (Third Party Vendor Risk Management)

Periodic and surprise IT

Security Health Check

Regulatory compliance services

Policy and compliance management lifecycle

Controls compliance monitoring and management

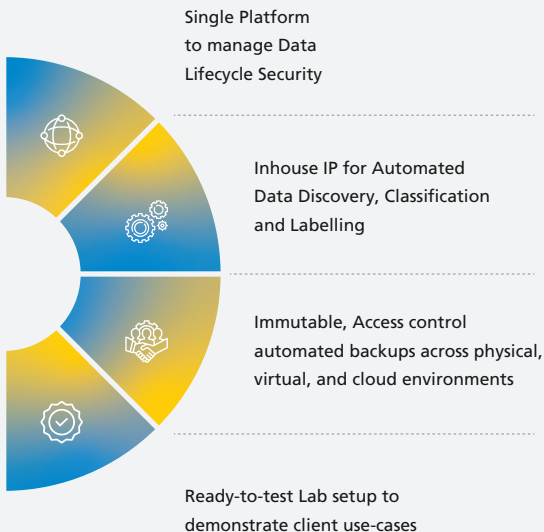
Internal audit Services

Unified controls compliance

Control testing & remediation services

Data Security

Digitize the core, enhance data-driven experience with a focus on data privacy





Integrated Insights

Privacy insights & dashboards
implementation for each
application,
vendor and process

Privacy across data lifecycle

e2e lifecycle in
data collection,
processing,
sharing, archival

Data Protection & Data Breach Management

Role-based anonymization,
pseudonymization,
masking & encryption

Breach
monitoring,
alert handling

Privacy analytics

AI/ML driven PII
data discovery

Data Privacy Impact Assessment

Data inventory,
privacy risk status

Technology evaluation

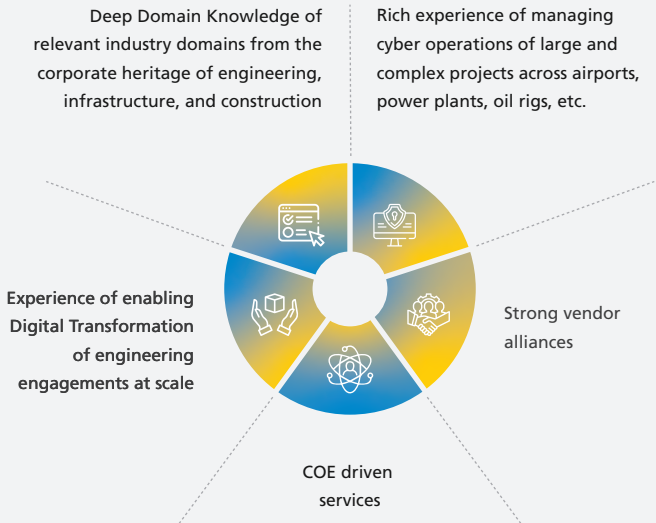
Privacy technology evaluation &
recommendation

Implementation
roadmap

Tool
fitment

Digital Defense

Manage the complexities of IoT/OT security risk with the right experience, solutions and frameworks



Assessment & Roadmap

Security & risk/
hazard assessment of
OT/IoT/IIoT ecosystem/
application/smart
buildings/smart cities

Vulnerability
assessment, risk
management
strategy definition

Security
program
maturity
assessment

Security program
maturity assessment

Maturity testing,
penetration testing

Vendor
review

Transformation & Integration

Security
architecture
& design

Security control
evaluation

Security
control
implementation

Managed Services

24x7 security
monitoring for OT/
IoT/IIoT ecosystems

Threat
detection and
remediation

Incidence
response

Threat
hunting

Threat containment,
eradication and recovery

| Success Stories

Managed Security Services

Financial Service Provider in Europe

Managed Cybersecurity Services

- Intelligence-led operations, Managed Threat and Vulnerability, Managed Cyber Security Ops
- Setup of Security operations (SIEM, UEBA, NTA)

Improved cyber risk posture

**Improved device availability
by over 99%**

**Reduced repetitive tasks
by over 70%**

Fortune 500 Manufacturing Organization

Next Generation SOC

Setup and operations of Next Generation SOC with 24x7 threat intelligence driven managed services

Global Delivery model

- USA, Canada, India

**Significantly improved
security posture**

**Proactive and prescriptive
threat detection**

**Automated incident
response Protection against
the zero-day threats**

Success Stories

Managed Security Services

US based Media House

Managed Cybersecurity Services

- Network - Threat & Vulnerability, End Point Security, and Security Incident Response
- 24 x 7 operations across India and UK

Service Towers:

- Network Monitoring
- Vulnerability Management
- Application Vulnerability
- Endpoint protection
- Proxy & Content Filtering
- Antiphishing

Over 35% Reduction in cost

Over 66% reduction in incident response time

42% reduction (YoY) from inherent to residual risk

Multinational Auto Giant

Intelligent Digital Identity Operations & Compliance

- Protect and manage Privilege accounts, 24X7 end-user support
- CyberArk PAM tool Implementations such as - PAM2.75, PAM3.0 etc

Global Delivery model – India, US

Enhanced Security Control

Reactive to Proactive Security Operations

Superior Regulatory Compliances

| Success Stories

Technical Security Services

US based Energy Company

Automated endpoint detection & response solution implementation

- Transformation of existing SIEM solution to more advanced, cutting edge MDR platform with built in security analytics , threat hunting and orchestration capabilities

Overall operational efficiency improvement and reduced cost of operations by 30% through automation

Over 60% reduction in false positives

US based Insurance company

Vulnerability Management Solution

- Comprehensive vulnerability management covering the applications, infrastructure based on client's CIA requirements, on-premise and cloud assets without any blind spots
- Qualys-based Hybrid Solution with cloud agents & scanners

45% reduction in false positives in the first year

Over 95% compliance achievement

Success Stories

Strategic Security Services

US-based Petrochemical company

Security governance & risk management

- Cloud assessments and cyber risk evaluation against leading industry standards (such as NIST 800-53 and CIS18).
- Audits and assessments against crucial regulatory requirements such as GDPR, SOX, CCPA, etc.
- Risk assessments & remediation advisory activities for cloud & on-premise technologies.

60% enhancement in security posture

99% SLA compliance

Europe-based Telecom Major

Cloud security posture assessment

- Defined future To-be roadmap for an ideal enterprise level of cloud security
- Built industrial security controls list, security blueprint, technologies stack, operating model for strengthening enterprise cloud security posture

80%+ improvement in cloud security posture in over 12 months

50+ Vendors assessed for service level and information security compliance improvement



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 83,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit <https://www.ltimindtree.com/>.