LTIMindtree

Building Cyber Resilient Enterprises

LTIMindtree Cyber Security Practice Overview

A Larsen & Toubro Group Company

Meet LTIMindtree Cybersecurity Practice

3,500+
Headcount

Our tribe of passionate solvers

220+
Clients

25 Fortune 500 Clients

8
Cyber Defense Resiliency Centers

Enabling Global Footprint

30+
IPs & Accelerators

Driving innovation and automation

25
Strategic Alliances

Joint solution, GTM

- Modernization Focused
- Platform Powered
- Experience in large security transformations
- End to end coverage across 8 security domains
- Best-of-the-breed partnerships
- CoE-driven services – playbooks, templates, frameworks, accelerators

Offering services across dimensions

Cyber Defense Resiliency Service

Adv Threat & VM

- VA/PT Testing
- Application Security testing
- Wireless and IOT Device Security testing
- Red Teaming
- Risk Based Threat and Vulnerability Management
- Cyber Risk Management
- Breach Attack Simulation

Threat Prevention

- UEBA
- Network Security & NBA
- End Point Security & ETDR
- Gateway Security
- Platform Security
- Data Security
- Email Security
- Application Security (WAF, API Security)

Threat Detection

- Next Gen Security Monitoring
- MSOC - Managed Detection and Response Alert Analysis
- Co-ordinated Incident Response & Recovery
- Managed Threat Detection & Response
- Advanced Malware and Sandbox Protection

Threat Hunting

- Security Big Data Lake
- Security Insights & Intel
- Brand Protection
- Threat Modeling
- Threat Intelligence
- Digital Forensics
- Security Orchestration and Automation

Digital Trust

Identity Management

- SSO, MFA
- Identity Governance & Administration
- User Access Mgmt
- Privileged Access Management
- SOD / Entitlement
- Consumer Identity

Data Security

- Data Discovery
- Data Classification
- Data Leak Prevention
- Digital Rights Management
- Data Encryption
- Database Activity Monitoring
- Privacy Governance & Automation

Risk & Compliance

GRC

- Audit and Assessment
- Governance and Risk Management
- Third Party Risk Management
- GRC Platform Implementation and Orchestration
- Unified Compliance Reporting

Digital Defense

IoT / OT Security

- Security & risk/hazard assessment
- Maturity testing, penetration testing
- Security architecture & design
- Control implementation
- 24x7 security monitoring for OT/IOT/IIOT ecosystems
- Threat detection, Threat containment, eradication & recovery

Cloud Threat Defense

Cloud Security

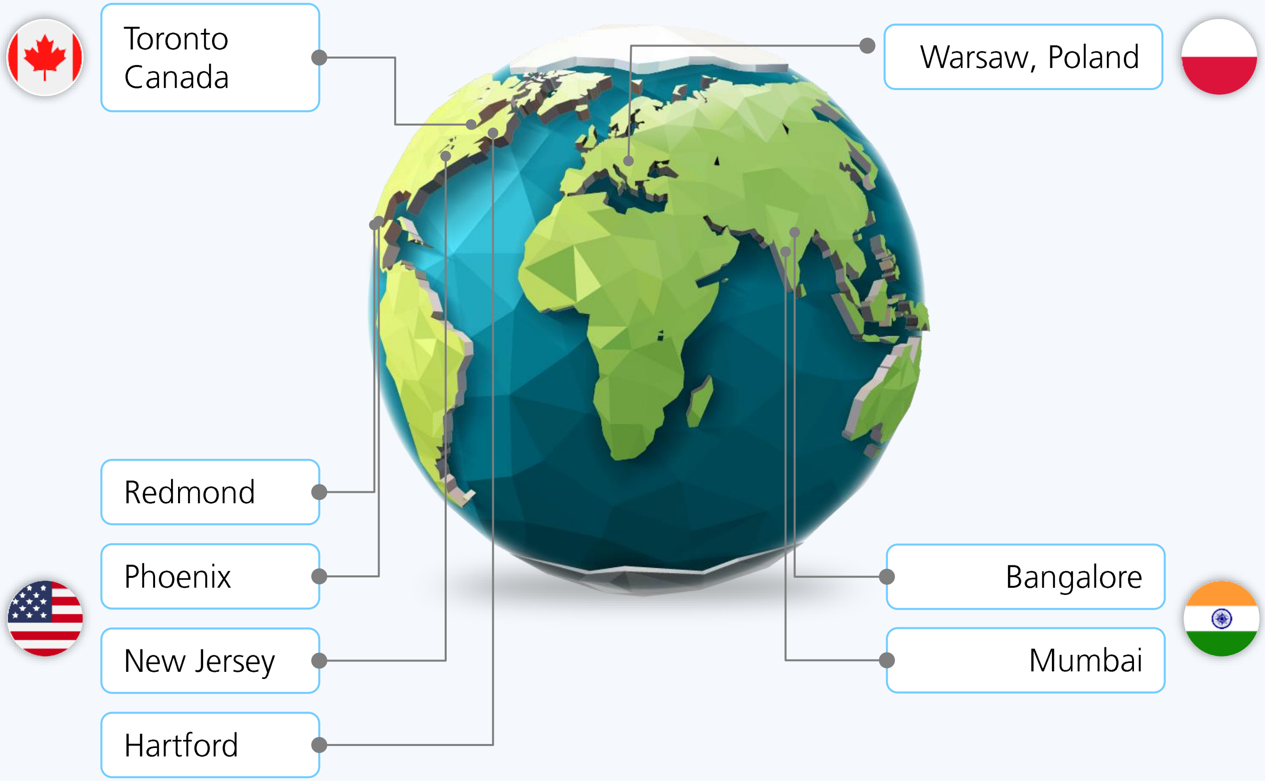
- Cloud Security Posture Mgmt
- Continuous Cloud Workload Protection & Threat Defense
- Cloud Identity & Access Security
- Data Security and Protection
- DevSecOps

🟦 Emerging Areas 🟨 Trending Areas ■ Established Areas

LTIMindtree

Serving Globally. Delivering Locally

Our Cyber Defense Resiliency Centres



Toronto Canada

Redmond

Phoenix

New Jersey

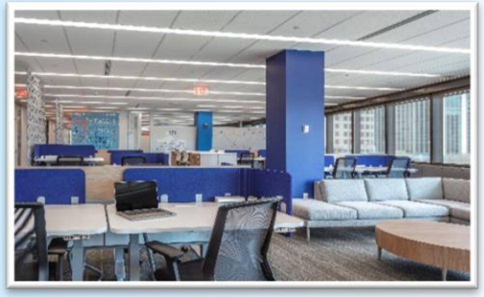
Hartford

Warsaw, Poland

Bangalore

Mumbai

Additionally, we leverage our 50+ Global delivery Centers



ISO 27001, SOC2 certified

24x7x365 operations and remote management services

Co-innovation with customers

Multiple controls at all levels to ensure privacy and confidentiality of Customer data - logical access controls, physical access controls, data segregation and encryption, independent and segregated facilities for service delivery

Trusted Security Partner for clients across verticals

Manufacturing

- HONDA The Power of Dreams
- Carrier
- solar
- Honeywell
- DeLaval
- Accudyne Industries
- SCANIA
- EATON
- SANDVIK
- CLARIOS
- BAKELITE SYNTHETICS
- Club Car
- wsp
- Bekaert
- Axel Johnson International
- CHAMBERLAIN GROUP
- LARSEN & TOUBRO
- Continental
- NORDEX We've got the power.

Healthcare and Life Sciences

- Mölnlycke
- COPE HEALTH SOLUTIONS
- AAMC
- thryve DIGITAL
- Banfield PET HOSPITAL
- Abbott
- Mylan
- ResMed
- NEKTAR
- parexel

Communications, Media, and Entertainment

- AICTE
- Paramount
- MINISTRY OF CORPORATE AFFAIRS GOVERNMENT OF INDIA
- DENTONS
- SONY PICTURES NETWORKS
- bread financial
- BLOCKGRAPH
- CRITEO
- WARNER BROS. DISCOVERY
- UNICC
- SITA
- FIU
- UNHCR The UN Refugee Agency
- randstad
- informa

Retail and CPG

- Farmer Brothers
- Kellogg's
- INFINITE ELECTRONICS, INC.
- L'ORÉAL
- P&G
- maurices
- IEEE
- WHITE CAP
- adidas
- dyson
- Dixons
- PHILIPS
- Unilever
- SSP
- TITAN COMPANY
- ELKJOP

Travel, Transport, and Hospitality

- DHL
- allegiant
- Lufthansa
- MARRIOTT
- Sabre
- DELTA
- AMERICAN EXPRESS TRAVEL
- REALOGY

Trusted Security Partner for clients across verticals

Banking, and Financial Services

ABSA

CAPS

Capricorn

Bank of India

citi

GENERAL ATLANTIC

EQUIFAX

HSBC

INTERNATIONAL MONETARY FUND

MSCI

FitchRatings

svb Silicon Valley Bank A Division of First Citizens Bank

WORLD BANK GROUP

TEACHERS federal credit union

WA

Nordea

Principal

standard chartered

NOMURA

nets

ICICI Bank

HDFC BANK

HoistFinance

Insurance

Aspen

GREAT AMERICAN INSURANCE GROUP

LINCOLN INTERNATIONAL

Munich RE

NASSAU RE

ORCHID

TRAVELERS

WS WOODRUFF SAWYER

Bell&Clements A Munich Re company

NFU Mutual

Hi-Tech

GUNNEBO

resonate

GRANICUS

Microsoft

Securitas

ZONES First Choice for IT

syncordis

CISCO

onsemi

hp

Wolters Kluwer

Energy and Utilities

bpx energy

ExxonMobil

أرامكو السعودية saudi aramco

CALPINE

ISS

PGE

Chevron

Chevron Phillips Chemical Company LP

OKQ8

NewFortress energy

EVERSOURCE

ساتورب satorp

VEOLIA

Our key pillars enabling us secure everything…

PINNACLE Cyber Defense Resiliency Platform

25+ Cyber Defense Resiliency delivery accelerators

In-built automation for incident response & remediation

Single Platform to manage multiple security layers across infra, cloud, endpoint, identity

Platform bundles available in a purpose-built or shared model, delivered through managed services approach

Rapid incident response by continuous playbook engineering

PINNACLE Cloud Threat Detection & Response Platform

Multi-Hybrid Cloud 360-degree Security for Full lifecycle code to cloud

A single user experience to secure cloud infrastructure, apps, identities, networks, and data

Integrated with SecOps tools to address issues and alerts

PINNACLE Threat & VM Platform

Well-Architected platform with best of the breed technology product stacks

InfraSec as a Service , AppSec as a Service

Orchestration framework and reusable artefacts

Compliance mapping with industry mandates, external and regional regulations

PINNACLE Identity Platform

Integrated and converged digital identity operations

Digital identity, compliance and assurance library

Pre-built standardized processes, policies and workflows

IGAaaS – Identity Governance Administration as a Service

AGCaaS – Access Governance and Control as a Service

PINNACLE Data Security Platform

Single Platform to manage Data Lifecyle Security

Inhouse IP for Automated Data Discovery, Classification and Labelling

Immutable, Access control automated backups across physical, virtual, and cloud environments

End to end Data Protection with advance detecting and blocking

Differentiators that drive our success stories

Scale and Size

Delivered Security transformation and modernization for Enterprises across their value stream

- 25+ Fortune 500 clients
- Greenfield SOC setup for Fortune 500 enterprises

Practitioner delivered

Library of Use cases and playbooks from day 1 of Operations

Best Practices & LTIMindtree's custom framework adoption during build phase

Flexible

Flexible "Everything as a Service model" with top-notch accelerators, platforms and strategic partnerships

Client-friendly solution (no vendor lock-in) – Open standard,, Agile and ease of sustenance

Platform-driven

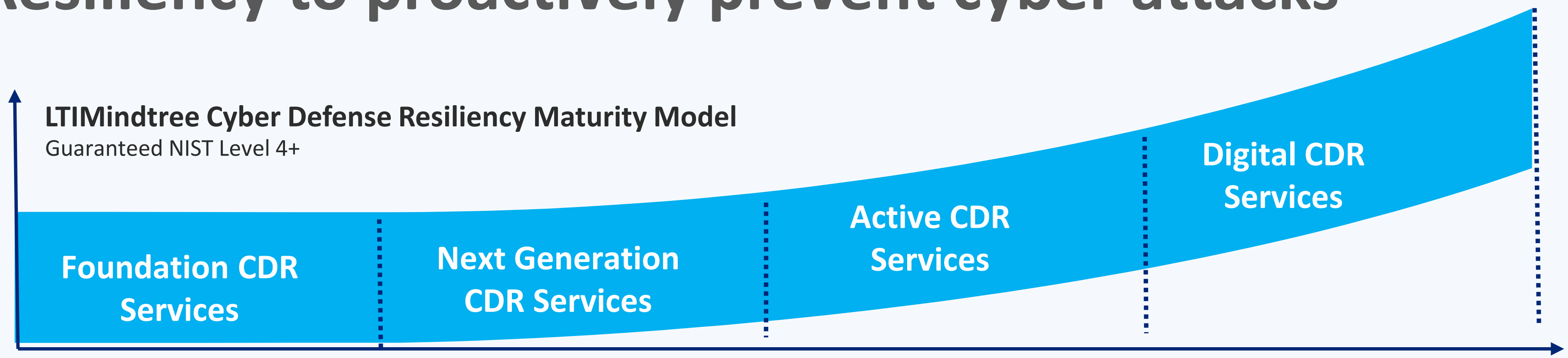
Packaged, bundled services curated for industry and enterprise type

- Pinnacle MxDR
- Pinnacle Cloud Threat Defense
- Pinnacle Threat & VM
- Pinnacle Identity
- Pinnacle Data Security

Cost Effective

- Automate and eliminate L1 efforts
- Converged IT OT Sec Ops and eliminate desperate operations.
- Reduction in false positives AI-ML led threat hunting and SOC operation for head count optimization

Journey that our customers have undertaken in their road to Resiliency to proactively prevent cyber attacks



LTIMindtree Cyber Defense Resiliency Maturity Model

Guaranteed NIST Level 4+

	Threat Prevention and Detection	Advanced Threat Detection and Defense	Adversary Emulation and Recovery	Cyber-Digital Convergence and Assurance
Security Capabilities	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 and 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

Our Key Accelerators… 1/2

Breach Attack Simulations

Automatic simulations of cyber attacks , Provides prioritized actionable remediation insights

- **100%** awareness of all possible attack paths
- Continuously identifies **attack vectors** to target assets 24×7
- Finds **gaps** that expose enterprise critical assets
- **Prioritizes** remediation tasks around risk and exposure
- Provides a **breach impact risk score** to insurance, legal, board members, etc.
- Evaluates **resilience** of existing security investment

Cyber Risk Management

Continuous risk-based visibility into enterprise assets and applications, as well as the associated attack surface area.

- **Quantified** Cyber Security posture
- Realtime **visibility** of risk score at all levels
- Intel led **Ransomware susceptibility**
- **Prioritized** vulnerability remediation
- AI-driven threat analytics by correlating internal security intelligence and external threat data feeds

VOAR

Vulnerability Orchestration Automation Remediation Service for Infra Vulnerability Management

- Vulnerability Contextualization and Management
- **Vulnerability Automation and Response**
- Track all vulnerabilities from a **single dashboard**
- Enhanced security control with single pane of glass visibility

Privacy SmartHub

Flexible and scalable domain-led digital offering, which offers advanced solutions to address data privacy regulations across the globe.

- **Privacy by design**
- Consent and **consumer rights** mgmt.
- Data encryption and anonymization
- Data access & user permissions
- Policy management
- **90%** automated processes
- **30+** countries covered

Our Key Accelerators…2/2

CISO Advisory Dashboard

Intuitive & interactive CISO Dashboard

- Drill down dashboard with detailed remediation advisory
- **Custom dashboards, metrics and tracking mechanism**
- **Risk Posture, Incident/ Reporting , SLA , KPI IDAM , VM ,PIM/PAM, Malware**
- Threat Advisory/Bulletins
- Threat susceptivity and actionable insights

CTdX Libs

Ready to deploy Use Case library mapped to MITRE ATT&CK

- Contextual **Threat Intelligence** driven analysis and operations
- Leverages **user and entity behavior analytics** for Insider threats
- MITRE ATT&CK framework-based **threat hunting libraries** to improve threat detection efficiencies

Security Maturity Management

Continuous GRC maturity management

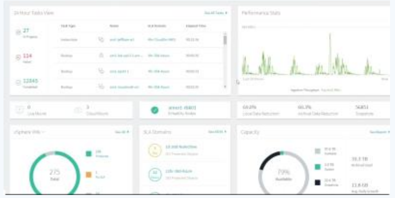
- SaaS Based **Continuous Cybersecurity Maturity and GRC Performance management**
- Initial phishing simulation exercise to understand the current cyber maturity among people
- Unified View of Cyber Maturity across the enterprise
- Establish Integrated Platform with Cross Mapping of controls against multiple standards
- CISO Dashboard

External Threat Landscape Intelligence as a Service

Contextualized Intelligence infusion in SOC Operations

- Deep-dive Threat Intel-led Operations
- **Dark Net Focused**
- Contextual Intelligence **on Trending Vulnerabilities, Threats to customer tech stack , trending hacktivist operations**
- Inputs to prioritize and defend against actionable threats relevant to Customers

Digital Vault as a Service



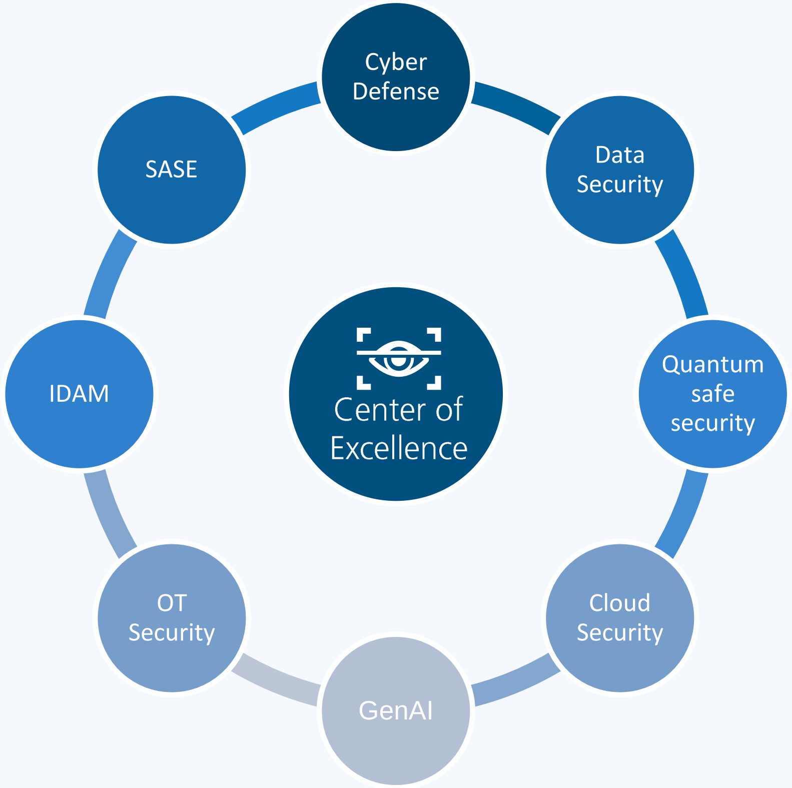
Unified Cyber recovery Platform

- **Immutable architecture** to protect against anomalies and ransomware/cyber attacks
- Expert investigation, incident containment and **sensitive data discovery**
- Intelligent Machine Learning based feature offers rapid anomaly detection and one-click easy recovery
- Reduced costs through modernization of Data Protection, improved recovery times

Our CoE

CoE Commitment

- 80% certified resources
- Best Practices, Frameworks, Playbooks
- Academia Collaborations
- Best-of-the-Breed Partnerships
- Cyber Defense Academy
- Co-Innovation/Joint PoC with clients
- MITRE ATT&CK aligned playbooks
- 10,000+ cybersecurity training modules with LTIM shoshin academy



Center of Excellence

- Cyber Defense
- Data Security
- Quantum safe security
- Cloud Security
- GenAI
- OT Security
- IDAM
- SASE

LTIMindtree

Learn. Create. Innovate.

LTIMindtree's Cyber Defense Academy

Purpose-build Cyber Defense Resiliency For A Rapidly Changing Threat Landscape

LTIMindtree

Quantum threats will soon become real.

Are you ready to face them head-on?

LTIMindtree

Secure As You Scale

With LTIMindtree's Enterprise Cloud Security Services

Business Impact

- Open architecture to easily integrate into existing security landscape
- 80% faster threat detection across engagements
- >60% + TCO optimization with Automation, AI & GenAI
- Board Level Security Risk Advisory
- 80% human efforts reduction in Threat Detection for all MSS clients
- 50% improvement in reusability and skill fungibility
- AI-driven User Entity Behavior Anomaly Detection
- CISO Dashboards

Key Partnerships

Cyber Defense

- Microsoft
- IBM QRadar
- SECURONIX
- CROWDSTRIKE
- paloalto NETWORKS
- CISCO
- Trellix
- SOC PRIME
- CYFIRMA DECODING THREATS
- Recorded Future

Cloud Security

- Microsoft
- Google Cloud Platform
- amazon web services
- Check Point SOFTWARE TECHNOLOGIES LTD
- sysdig
- Lacework

GRC

- TrustMAPP
- SAFE SECURITY
- KnowBe4 Human error. Conquered.
- servicenow
- Prevalent

Identity

- SAP
- Microsoft
- PingIdentity
- okta
- BeyondTrust
- Delinea
- CYBERARK
- SAVIYNT
- ilantus The Identity Management People

Vulnerability

- Qualys
- tenable
- FireCompass
- KALI
- ivanti Neurons Powered by RiskSense
- Fortify
- BURPSUITE

Data Security

- appviewx
- BigID
- Microsoft
- Symantec
- rubrik
- Trellix
- THALES

OT Security

- NOZOMI NETWORKS
- Heimdal
- CLAROTY
- xage SECURITY
- FORTINET
- CYBERARK

Industry Validations

ISG

LTIMindtree has innovative technology and modularized solutions to help solve security challenges across enterprises of all sizes. ”

HFS

LTIMindtree brings a comprehensive approach for transforming cybersecurity—“Reactive Incident Response to Proactive Threat Defense. ”

AVASANT

LTIMindtree continues to transform to mature SOCs and add more intelligence, behaviors analysis and proactive and prescriptive hunting capabilities. It is also adding speed to response through automation and orchestration to minimize any business disruptions from cyber threats . ”

ISG

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

Product Challenger in ISG provider Lens Cybersecurity Services and Solutions 2023– **USA Large market**

Everest Group®

Major Contender” in Everest Group **Managed Detection & Response (MDR)** Services Peak Matrix ® assessment 2023

Major Contender” in Everest Group IT **Security Services** Peak Matrix ® assessment, North America & Europe 2022

Major Contender” in Everest Group **Identity & Access Management (IAM)** Services Peak Matrix ® assessment 2023

AVASANT

Innovator in **Avasant** Cybersecurity services 2023 RadarView

Securing Global Enterprise

Carrier

Modern Greenfield SOC

Next Generation Cyber Ops, Threat Intelligence as a Service, Threat Hunting as a Service, Vulnerability Management, Identity &Application on-boarding & User Life Cycle Management Access management

75% improved TDE

Banfield PET HOSPITAL

Data Security

Endpoint DLP implementation for 22,500 workstations

Proactive monitoring and identification of potential insider threat Prevention of data leakage from endpoints, emails & web

Identification of sensitive data & quarantine to secure location

Significant improvement in data security

CLARIOS

OT Security Assessment

Maturity Assessment of the OT Security landscape - plants across 4 countries in 3 continents.

Optimized working design for OT network monitoring and secure remote access

Improved process machine network connectivity by 60%

PHILIPS

Application Security

Process Definition
Static Application Security Testing
Dynamic Application Security Testing
Application Penetration Testing
Mobile Application Security Testing
Security Testing
Web Services Security Testing
Infrastructure VAPT
DevSecOps Implementation

Reduced the overall efforts for the program by 45%

HONDA
The Power of Dreams

Managed Identity Operations

IAM process automation

Privilege Access management solution across North America

IGA implementation

20% Reduction in identity snooping attacks

INTERNATIONAL MONETARY FUND

Infrastructure Vulnerability Management

Process Definition

Tools Installation & Configuration Compliance Mapping

End-to-end VM activity Automation

Improve Scan coverage & Asset Discovery Standardization of VM Program Framework

50% Reduction in mean time to patch

Securing Global Enterprise

DELTA

Identity & Access Management

End- to-End support of user identity management, access management, Privileged Account Management and directory services 1600+ applications in production and lower environments, 80K users, 25k privileged accounts

30% cost savings, 45% reduction in time for user Onboarding

OKQ8

Managed Cyber Ops

Threat Intelligence Led Operations

Managed Cyber Security Ops

Managed Privilege Access Management

Cloud Security Monitoring

Digital Identity & Access Management

20% reduction in MTTR & MTTD

CLARIOS

Application Security Maturity Program

NIST & OWASP compliance for critical applications.

Security Testing, Risk profiling, Left-shift scan process , Penetration testing, SAST/ DAST tools

Source code analysis

70% increase in NIST & OWASP compliance for critical applications.

EVERSOURCE

Intel Led Cyber Defense

Managed Intel Led Cyber Defense Security Ops with automation

Managed Threat Prevention Services Vulnerability Governance, SIEM/SOAR, endpoint security, network security , OT security, Content, playbook development

Reduction in false positive ratio from 95% to 57%

P&G

Threat & Vulnerability mgmt.

Process Definition

Tools Installation & Configuration

Static Application Security Testing

Dynamic Application Security Testing

Application Penetration Testing

Web Services Security Testing

320+ vulnerabilities identified & mitigated

Chevron Phillips CHEMICAL

Governance, Risk & Compliance

Comprehensive Security Controls Discovery

Established Strong Governance Framework Experienced GRC Staff across geographies

Strong Security Industry Integration

Risk assessment of Cloud & on-premise landscape

60% enhancement in Security Posture in 18 months

Annexure 1

Service Offerings

Cyber Defense - Advanced Threat and Vulnerability Management Services

New-age design, testing, implementation & monitoring services & solutions for managing Cybersecurity Risk

Domain Experience to support risk & compliance efforts with cost effectiveness	Proven approach, listed Accreditations – CREST Penetration Testing Empaneled 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.	Technology Partnerships / COEs – Tool Agnostic.

Security Risks, Vulnerabilities and Risk Mitigation

- Quantifiable risk score for every asset & application
- Risk base Vulnerability prioritization
- AI/ ML Based Triaging and managing remediation
- Proactive risk reduction & mitigation advisory

Insider Threat Management Program

- Correlate activity and data movement, identify user risk, Insider Threat Detection, misconfiguration etc
- Accelerated security incident response.

Vulnerability Management

- Asset Management, Tool Configurations, Scheduled Scanning, FP removals,
- Threat Intel Driven Analysis, AI/ ML Based Triaging
- Vulnerability Scanning, Remediation & Advisories
- Tracking Vulnerability tickets to closure

Penetration Testing

- Blackbox, Grey box – Infra & Apps level
- Enumeration/ Recon, Assessment/ Scanning, Exploitation, Post exploitation, Reporting
- External & Internal

Application Security

- Static Application Security Testing (SAST)
- Software Composition Analysis (SCA)
- Dynamic Application Security Testing (DAST)
- Threat Modeling, Penetration Testing, API Security Testing Processes, Secure SDLC Framework
- Compliance Mapping (OWASP, NIST etc.) .
- DevSecOps, Managed AppSec, Maturity Assessment

Global leader in energy storage solutions	A global multi-line insurer	Global FMCG Gaint	Dutch Conglomerate
Risk Based Application Security Framework, Testing, Remediation Prioritization, Advisory, Compliance Maturity, Dashboard	SAST and DAST services covering over 200+ applications progressing into Managed DevSecOps roll out	Implemented security tools & technologies across SDLC and conducted in-depth security assessment of apps by covering SAST, DAST and Pentesting	Implemented In-Sprint CI/CD based dynamic security testing execution using Azure DevOps

Cyber Defense - Threat Prevention Services

Secure the perimeter and protect the users wherever they work

Purpose-built approach to gradually improve from the current state to next-Gen network security aligned to Zero Trust Principles	Everything-as-a-Service	Best of Breed product partnerships	CoE to continuously enhance engineering and managed security services	Delivery accelerators from day 1 of operations

Value driven consultancy
- Network Security Architecture Design
- Gap Assessment and recommendation
- Tools identification assistance

Engineering
- Design HLD and LLD
- Implementation of Network and Endpoint Security Solutions including Next Generation Firewall,EDR,Email-Security,Cloud WAF,Anti-DDoS,Anti-APT,etc
- Hardening of Network and endpoint Security Controls
- Integration with Threat Intel,SIEM,SOAR
- Continuous rule engineering

Network Access Control as-a Services
- Endpoint classification and profiling
- Endpoint Authorization based on least privilege
- Compliance and Posturing
- Remote isolation
- Guest/BYOD access management
- Enforcing Zero Trust by Connecting trusted users and endpoints with trusted resources
- Dynamic endpoint posture updation

SASE
- Zero trust network access | Secure Web Gateway
- SD-WAN Security | CASB
- FWaaS with Advanced threat protection

Managed Services for Network and Endpoint Security solutions which includes NGFW,Email Security,EDR,Cloud WAF,etc
- Configuration Management
- Troubleshooting BAU Connectivity and access issues
- Service Improvements
- Incident/Change/Problem Management
- SLA/KPI driven service
- Advisory on Malicious IP/URLs/Hash,etc
- 24x7, 24x5, 16x7, 16x5, 8x7, 8x5 Management
- SWAT to handle Major Incidents
- OEM Coordination

American Film Production Company	Major Swedish manufacturer	Energy Major in the US	American Reinsurance Company
Managed Services involving implementation and operation support of network and endpoint security	Implementation of SD-WAN Managed Services for Firewalls,LB,RAVPN,Email Security	Automated endpoint detection & response solution implementation, Extended visibility over infrastructure by seamless integration of all endpoints with Crowdstrike EDR to the MDR platform	Implement and Manage NG Firewalls,NAC,Email Security,SD-WAN security

Cyber Defense - Threat Detection Services

Monitor, Report, Respond, and Govern through a single pane of glass leveraging integrated threat intelligence feeds

Domain experience across custom integration, orchestration, hands-on development, configuration and automation	Framework to support transition and transformation to threat Intelligence driven cyber operations	Predefined Content Pack for faster onboarding Data enrichment through multiple threat intelligence feeds	MSOC Platform offering with Sentinel	Established use case framework to fine-tune and enrich use cases.

Monitoring

- 24x7x365 continuous monitoring against threats enabling faster detection and response to threats
- Decreases time-to-detection and remediation through automation

Alerts and Notifications

- Improve security against advanced malware attacks, including ransomware

Reporting

- Security Incident report containing details, risk and remediation status

Threat Intelligence Feed

- Enrich the Security Monitoring platform with latest threat inputs for detection
- Integrate feeds from multiple data sources within single platform

Technologyy Integration

- Correlates network and endpoint insights for enterprise-grade threat visibility

MSOC – Nextgen Security Operations

- Cloud based SIEM (Microsoft Azure Sentinel)
- Managed Offerings
- Data Protection and ransomware recovery
- Threat Intelligence

US Insurer	UK based Investment Management Company	Global Investment Management Firm	F500 Energy company
Alert Analysis and Incident Response	Complete Threat Management solution implementation including network , email , web , end point , gateway with Threat Detection.	Strategic partner for Enterprise Cybersecurity function to secure modernization and transformation	Single pane of glass view to detect and monitor advance cybersecurity threats and incidents

Cyber Defense - Threat Hunting Services

Proactively Identify and accurately remediate threats with network-based behavior analysis and advanced reporting engine

Combination of integrated system and human-led hunting for advance intelligence	Automated threat management platform built with artificial intelligence-based on machine learning and behavioral analytics to detect attacker behaviors and user anomalies	Industry experience with successful client engagements across multiple verticals	Ready-to-use checklists & templates Library of Playbooks Threat modelling to prioritize risks	Technology Hunting and Research CoE

Security Big Data Lake

- Security Analysis and threat hunting at scale

Brand Protection

- Prioritized, actionable threat intelligence, detect attacks in time and act on emerging threats before they turn into a breach

Security Insights & Intelligence

- Predict and analyze threats based on contextual analysis leveraging analytics and AI

Threat Deception

- Deception technologies integrated with security controls and services to enhance layered defense

Digital Forensics

- Cyber Investigation, Forensics & Response and recovery

Security Orchestration & Automation

- Rapid threat response by automating manual and repetitive processes to drive Context-Driven Investigation.

Energy Major in the US	F500 Manufacturing org	American Film Production Company	Global leader in optimized resource management
ETDR & Threat Hunting - Actionable information on high risk events for early attack detection	Threat Hunting as a Service - Operationalization of 9k+ use cases for Intelligence and Purple team driven threat hunting	Cyber Analytics tool enabled Threat Hunting Services	Use case engineering, intelligence driven hunting, custom hunt

Identity & Access Management

Enabling Trusted Digital Enterprises with Digital Identity Assurance & Compliance

Dedicated IDaaS CoEs

Reusable Playbooks & Accelerators

Zero-Trust Approach

Domain know-how from several IDAM engagements

Identity Centric, Microservices based extendable & scalable Product Architecture

Assessment based on Industry Framework

- Evaluate Control Point based on NIST, ISO frameworks
- Discovery of the current state and provide IDAM Road map
- Solutionn migration
- Product Fitment

Privileged Management and Compliance

- Azure Privileged Management
- Privileged Access and Security Policies
- Zero Trust for Privileged Activities
- Privileged Access Audit, Compliance, Reporting
- Password Vaulting and Session Management for Windows, Linux, Mainframes
- Disaster Recovery and High Availability
- Web Application Session Management

- Network Devices Access Control Password Mgmt.
- Database access monitoring password Management.

Identity and Access Attestation and Certification

- Role/Privilege/Policy Design & Management
- Intelligent Access Request / Review
- Data Access Governance
- Cloud Access Governance
- Application SOD Management
- Privilege Account Governance / Monitoring
- Usage, Peer and Behavior Analysis

Zero Trust Journey with IAM

- Risk Based Authentication
- Adaptive Authentication
- Access validation and Certification
- Access Analytics

Managed Services

- IAM Platform Management
- Manual UAM Operations and Governance
- Identity Governance Campaign and Operations
- PAM operations
- CIAM – B2B, B2C, G2E, G2C operations
- IAM Process validation and Improvements
- 24x7, 24x5, 16x7, 16x5, 8x7, 8x5 Monitoring and Support Services

Value based Integration

- Common Ticketing platform integration with ITSM tools like
  - Service Now with IGA and PAM solutions
- Identity Intelligence with Integration with SIEM platform
- Common Dashboarding across Identity, Access and Privileged Management and other Security tools

F500 Manufacturing org

Design and Implementation of IAM stack with SSO, Web Access and IGA

Global Auto Giant

Managed service involving architecture, design, implementation and rollout of Privilege Access Management solution across North America

Major American Airline

Global Security support majorly North America region for 80k+ users with 600+ Applications

Producer of dairy and farming machinery

200+ Applications tested for SHA2 compliance

100K+ Certificates migrated from On- premise to cloud

Governance, Risk & Compliance

Manage risks, stay compliant with evolving regulatory mandates

Business aligned security architectures and infrastructure design. Vendor agnostic, interoperable and secure by design

Integrated risk and compliance management (GRC/ IRM)

Industry-standard security architecture and risk assessment frameworks

COE driven GRC strategy and technology services.
Strong vendor alliances

Effective integration of security architecture with agile development and delivery

Governance

- Board and cyber executive advisory
- Cyber defense program development and assessment
- Developing Security baselines / Policies & Procedures
- Governance reviews and framework evaluation setting
- Maturity assessments, benchmarking

3rd Party Risk Management

- Third Party Onboarding & categorization
- Assessments & Audits, Risk Scores,
- Monitor Risk & Issue Mitigation, Industry Compliance
- Continuous Risk Monitoring along with unified Cyber, business and financial intelligence.

Risk Management

- Enterprise IT risk management (IRM)
- Security risk management
- End-to-end risk management lifecycle of third parties (Third Party Vendor Risk Management)
- Periodic and surprise IT Security Health Check
- Risk management framework

Compliance Management

- Policy and compliance management lifecycle
- Compliance Posture Assessment mapped against NIST/CMMI
- Controls compliance monitoring and management
- Regulatory compliance services
- Internal audit Services
- Unified controls compliance
- Control testing & remediation services

Security Architecture

- Enterprise Security architecture based on TOGAF & SABSA
- Mapping of security requirements to solution and business objectives
- Reusable Security Architect, patterns and artefacts
- HLD & LLD Security design and capabilities
- Security Controls definition and design
- Security policies, standards and publications
- Security & technical design governance & risk

Finnish multinational Telcom Company

Security assessment against NIST 800-53, CIS benchmark for over 100+ technologies stack, processes. Assessment of over 50+ vendors for compliance

A global leader in aviation

Maturity assessment & advisory, curated security governance structure, established detailed compliance processes

Major Petrochemical company

Risk assessment of cloud & on-premise landscape, security control implementation, resulting in 60% security posture improvement in over 12 months

Dutch Information Services Company

Management of SOX Compliance , SOC 2 Attestation & ISO 27001

Internal Audit and Third-Party Risk Management also implemented

Data Security

Prevention of data leakage and cryptographic Security

Assets and Platforms	Productized & containerized solutions for reduced implementation time	LTIMindtree privacy smartHub – a domain-led digital offering, to address data privacy regulations	Best-of-the-breed partnerships

Data Discovery
- Scanning various data sources and systems
- Identification of Sensitive data
- Asset inventory
- Structured and Unstructured data
- On-premise and in the cloud

Data Classification
- Classification framework
- Classification and tagging of data
- Manual and Auto classification
- Analytics and Reporting
- On-premise and in the cloud
- Emails and Documents

Data Protection
- Data Loss Prevention
- Data Masking and Tokenization
- Data Encryption
- PKI (Certificate Management)
- Information Rights Management (IRM)
- Database Activity Monitoring (DAM)
- Cloud Access Security Broker (CASB)

Operations
- 24x7 support for all data security services
- Breach monitoring, alert handling
- Incident management
- Agent Troubleshooting
- End-user support

Data Privacy Impact Assessment
- Data inventory, privacy risk status

Technology evaluation
- Data protection technology evaluation & recommendation
- Implementation roadmap
- Tool fitment and vendor selection
- Integration with third-party applications
- Analytics and Automation

Engineering
- Data Security Assessment
- HLD and LLD solution design
- End-to-End solution implementation
- Enhancement of LTIMindtree Platforms as per specific needs of customers

Global E-commerce Giant

Implemented Data Deletion, Anonymization, Retention Policy for 28 EU countries which resulted in 65% reduction in processing time

Swedish Finance Major

Design and Implemented 2 tier MSPKI and HSM for storing CA private Key

Global Health Services Company

Mapped the data discovery reports with ROPA template for GDPR compliance by achieving 70% time-savings from automation

Finnish Financial Services Company

Automated solution to extract/subset, mask and generated synthetic test data & achieved 100% accuracy in data creation

Cloud Threat Defense

Hybrid-Multi Cloud Threat Defense Solutions inbuilt with Analytics, AI /ML, TI/TH, & Automated Threat Defense

Exhaustive Security controls, framework, blueprint, technology stack combination

Strong strategic partnerships with major cloud platform providers

SOC Framework to integrate and monitor across multiple cloud services providers and managed security services providers.

Cloud Security Operation & Defense

- MSOC
- Container, Kubernetes Security
- Cloud SIEM & Data Lake
- MITRE ATT&CK detection library
- Threat Hunting & Threat Intelligence
- UEBA, IoC/IoA & SOAR
- Red & Blue Teaming
- Cloud Infrastructure Entitlement, CASB

Cloud Workload Advanced Threat Detection & Response

- Endpoint Security, EDR, Network Micro-Segmentation
- Threat & Vulnerability Management
- Data Security, Labelling, Masking, Data Loss Prevention
- Encryption, Key Management
- Security Threats, Detect and Response, Application whitelisting, File Integrity,
- Advanced Automation & Playbook

Cloud Security Posture Monitor & Response

- Security Configuration Management & Response
- Regulatory Compliance Management
- Network Security Management
- IAM Security Management
- Control Mapping Framework

Major Utility Services Provider

Security roadmap definition to achieve cloud security posture, streamline the tech stack

Major petrochemical company

Cloud security assessment & Microsoft E5 deployment

Major distributor of building products in US

Assessment of comprehensive security landscape including workload, data, users in Cloud and the security posture improvement

European sourcing and services company

Azure Sentinel, DLP, Information protection , Azure SSO, MFA and PIM

IoT/OT Security

Securing the OT environment for uninterrupted operation of the Plant

Deep Domain Knowledge of relevant industry domains from corporate heritage of engineering, infrastructure and construction	Rich experience of managing cyber operations of large and complex projects across airports, power plants, oil rigs etc.	COE driven services	Strong vendor alliances – Xage, Claroty, CyberX, Qualys, Armis	Experience of enabling Digital Transformation of engineering engagements at scale

Assessment & Roadmap

- Vendor review
- Security & risk/hazard assessment of OT/IOT/IIOT ecosystem/application
- Security program maturity assessment
- Vulnerability assessment, risk management strategy definition
- Maturity testing, penetration testing

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

Multi-commodity mining and metals company

IEC 62443 based security solution design & implementation for PCN Infrastructure

Indian Multinational tyre manufacturing company

Design and implementation of OT Security Architecture for the plant inline to Purdue reference architecture

National railway network.

NESA and IEC 62443 based security solution design & implementation for IT/OT Infrastructure of Freight Rail Network

State Governments of India

Device Security Hardening, Security design & implementation to protect the data.

Annexure 2

Cybersecurity Platforms

LTIMindtree Pinnacle MxDR Platform

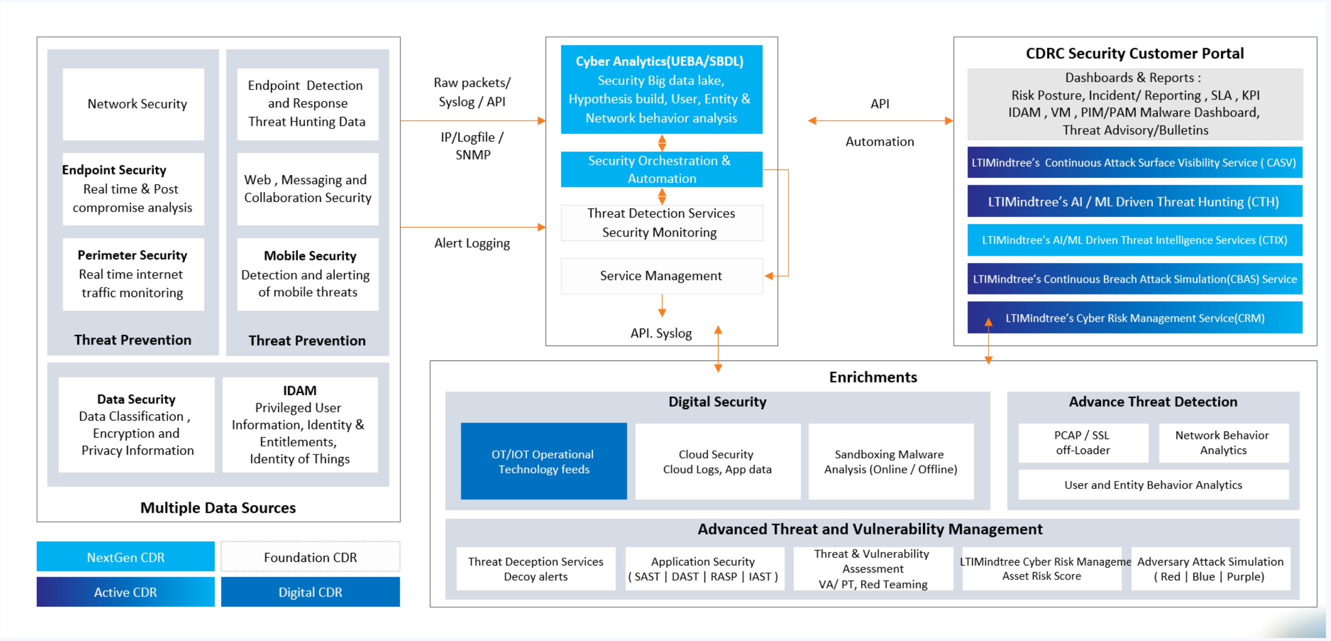
Proactive & Prescriptive, Cognitively Autonomous & Convergent Managed Cyber Operations

Converged and Active Cyber Defense Resiliency across IT , OT / IOT, People & Process

25+ Cyber Defense Resiliency delivery accelerators

22,000+ use case library

Multi-tenant shared Services/Hybrid/Dedicated Platform



Network Security

Endpoint Detection and Response Threat Hunting Data

Endpoint Security Real time & Post compromise analysis

Web , Messaging and Collaboration Security

Perimeter Security Real time internet traffic monitoring

Mobile Security Detection and alerting of mobile threats

Threat Prevention

Threat Prevention

Data Security Data Classification , Encryption and Privacy Information

IDAM Privileged User Information, Identity & Entitlements, Identity of Things

Multiple Data Sources

NextGen CDR

Foundation CDR

Active CDR

Digital CDR

Raw packets/ Syslog / API

IP/Logfile / SNMP

Alert Logging

Cyber Analytics(UEBA/SBDL) Security Big data lake, Hypothesis build, User, Entity & Network behavior analysis

Security Orchestration & Automation

Threat Detection Services Security Monitoring

Service Management

API. Syslog

API

Automation

CDRC Security Customer Portal

Dashboards & Reports : Risk Posture, Incident/ Reporting , SLA , KPI IDAM , VM , PIM/PAM Malware Dashboard, Threat Advisory/Bulletins

LTIMindtree's Continuous Attack Surface Visibility Service (CASV)

LTIMindtree's AI / ML Driven Threat Hunting (CTH)

LTIMindtree's AI/ML Driven Threat Intelligence Services (CTIX)

LTIMindtree's Continuous Breach Attack Simulation(CBAS) Service

LTIMindtree's Cyber Risk Management Service(CRM)

Enrichments

Digital Security

OT/IOT Operational Technology feeds

Cloud Security Cloud Logs, App data

Sandboxing Malware Analysis (Online / Offline)

Advance Threat Detection

PCAP / SSL off-Loader

Network Behavior Analytics

User and Entity Behavior Analytics

Advanced Threat and Vulnerability Management

Threat Deception Services Decoy alerts

Application Security (SAST | DAST | RASP | IAST)

Threat & Vulnerability Assessment VA/ PT, Red Teaming

LTIMindtree Cyber Risk Manageme Asset Risk Score

Adversary Attack Simulation (Red | Blue | Purple)

Service Offerings

Advance Threat & Vulnerability Management

VA/PT Testing | Application Security testing | Red Teaming | Risk Based Threat and Vulnerability Management | Cyber Risk Management | Breach Attack Simulation

Threat Prevention

UEBA | Network Security | End Point Security | Gateway Security | Data Security | Email Security | Application Security (WAF, API)

Threat Detection

Next Gen Security Monitoring | Co-ordinated Incident Response & Recovery | Managed Threat Detection & Response , Advanced Malware and Sandbox Protection

Threat Hunting

Security Big Data Lake | Security Insights & Intel | Brand Protection , Threat Modeling | Threat Intelligence | Digital Forensics Security Orchestration and Automation

Exhaustive Security controls, framework, blueprint, technology stack combination

Domain-led digital Platform and productized offering,

Ready-to-use checklists & templates
Library of Playbooks
Threat modelling
to prioritize risks

MITRE mappings and enhanced threat intelligence

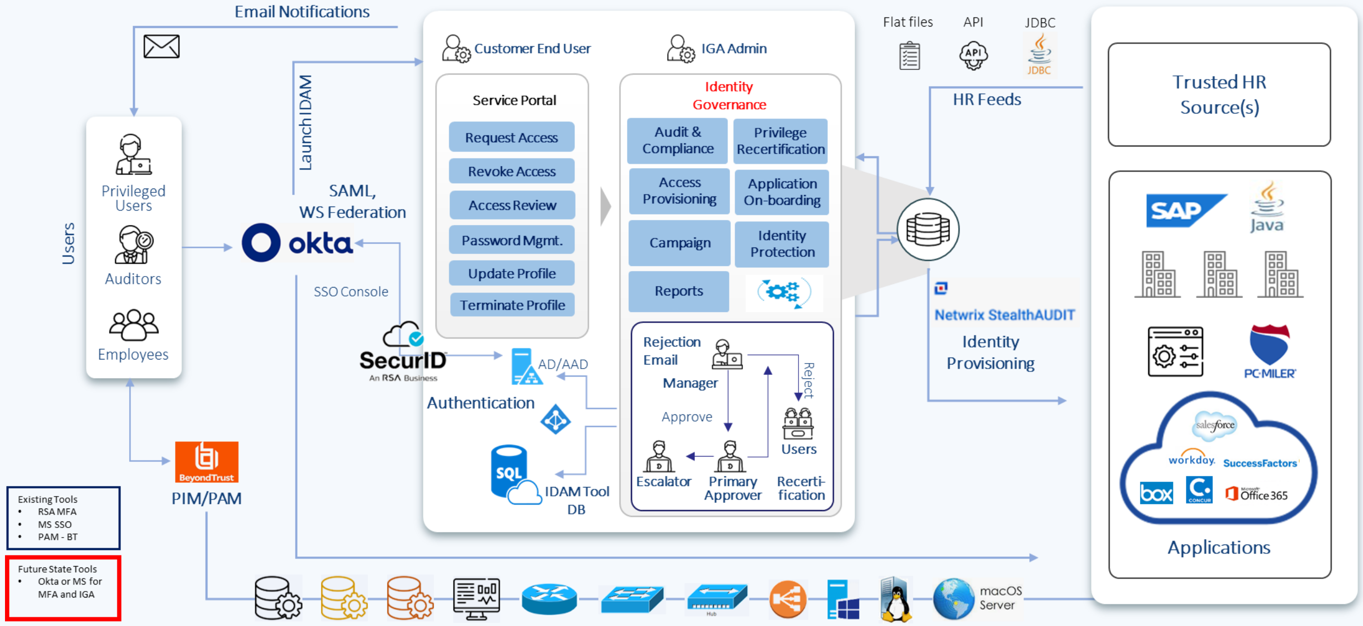
Full detailed attack visibility
Automated incident investigation

Bundled offerings customized for large & mid-market

LTIMindtree Pinnacle Identity Platform

Converged Digital Identity as a Service Platform with cloud-native, risk-aware, all in-one solution that is built on the Zero-trust Framework to provide Identity-first holistic cybersecurity

- Adaptive Access
- Self-service Portal
- Dynamic Orchestrated Authorization
- Identity of Human + Things
- Zero Trust Approach



Service Offerings

- Identity Governance & Administration
- Access Management
- Privilege Identity & Access Management
- Consumer Identity and Access Management

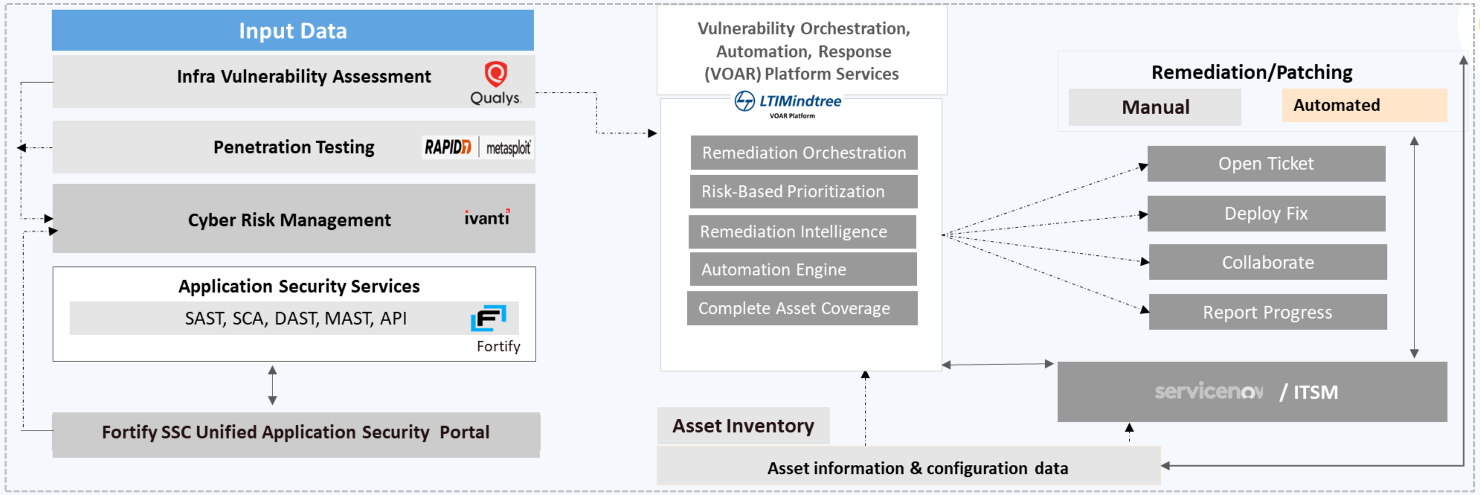
- Digital identity, compliance and Assurance Library
- Pre-built standardized processes, policies and workflows
- Accelerators/playbooks and frameworks for a Zero Trust Roadmap
- Well-Architected platform with best of the breed technology product stacks
- Over 40% faster onboarding timelines with a factory-based deployment model
- AI/ML and Autonomous Digital Identity Operations

LTIMindtree Pinnacle Advance Threat & Vulnerability Management Platform

Integrated Risk-Based end-to-end Vulnerability Management Platform

LTIM Accelerators:

- Application Security Orchestration and Correlation (ASOC)
- Cyber Risk Management
- Vulnerability Orchestration and Remediation (VOAR)



Input Data

Infra Vulnerability Assessment — Qualys

Penetration Testing — RAPID7 | metasploit

Cyber Risk Management — ivanti

Application Security Services

SAST, SCA, DAST, MAST, API — Fortify

Fortify SSC Unified Application Security Portal

Vulnerability Orchestration, Automation, Response (VOAR) Platform Services

LTIMindtree VOAR Platform

- Remediation Orchestration
- Risk-Based Prioritization
- Remediation Intelligence
- Automation Engine
- Complete Asset Coverage

Remediation/Patching

Manual | Automated

- Open Ticket
- Deploy Fix
- Collaborate
- Report Progress

servicenow / ITSM

Asset Inventory

Asset information & configuration data

Service Offerings

Infra VM| App VM | Security Maturity Assessment | Third Party Risk Mgmt | Cyber Risk Mgmt

- >40% Reduction in time spent on vulnerability detection, remediation and reporting
- Well-Architected platform with best of the breed technology product stacks
- Contextual and quantified risk-based scoring
- Quick onboarding timelines with a factory-based deployment model
- Ready-to-use checklists & templates across domains such as OWASP, NIST, ISO, PCI, SANS, Privacy Laws etc.
- Compliance mapping with industry mandates and external and regional regulations

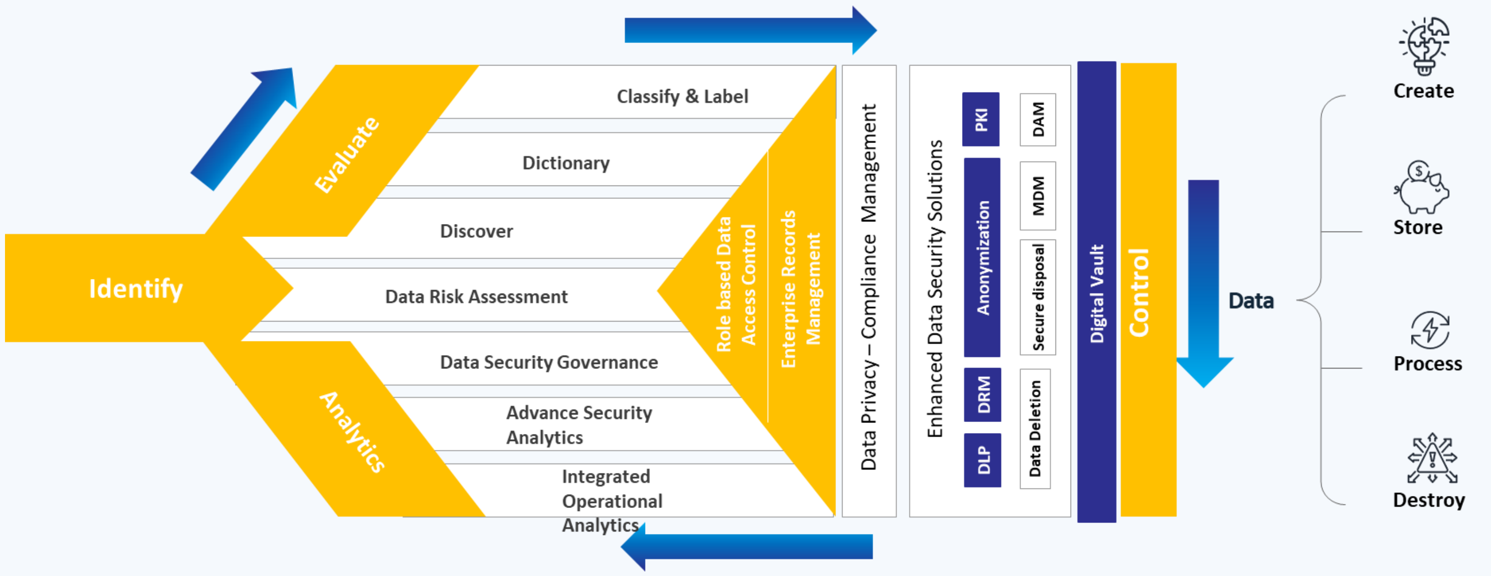
LTIMindtree Pinnacle Data Security Platform

End to end Data Security & Privacy Platform

Zero Trust Data Security Architecture

Immutable, Access control automated backups across physical, virtual, and cloud environments

Integrated Platform for Data Resilience, Data Observability & Remediation



Service Offerings

Data Discovery
Identification of Sensitive data | Asset inventory | Structured and Unstructured data

Data Classification
Classification and tagging of data

Data Protection
Data Loss Prevention Data Backup Data Masking and Tokenization | Data Encryption PKI |IRM | Database Activity Monitoring (DAM)

Operations
24x7 support | Breach monitoring, alert handling | Incident management

Single Platform to manage Data Lifecyle Security

Ready-to-test Lab setup to demonstrate client use-cases

Strong pool of resources with certifications across privacy and information protection

Data Resilience, Data Observability & Remediation

Inhouse IP for Automated Data Discovery, Classification and Labelling

End-to-End protection with cost effectiveness

LTIMindtree Pinnacle Cloud Threat Detection & Response (CTDR)

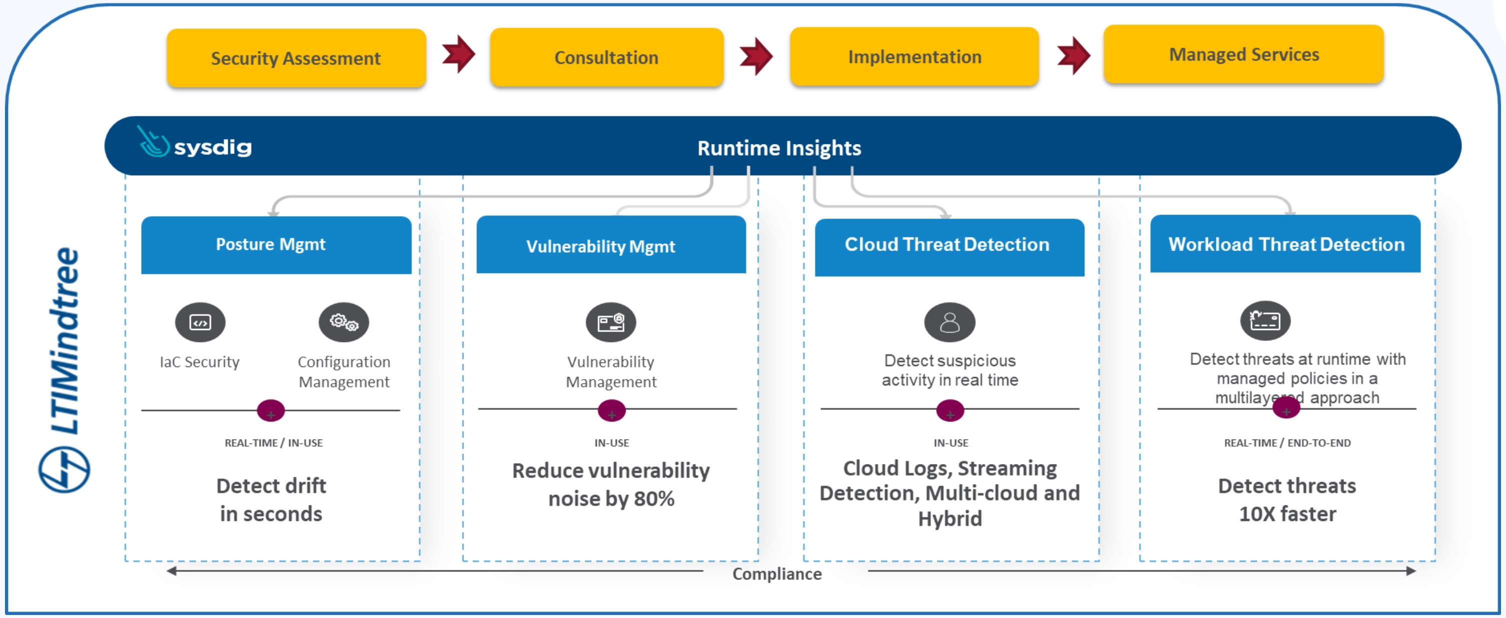
Multi/Hybrid Cloud Threat Defense Platform

Consolidate security across containers, hosts, cloud services, idntity and third-party apps

Enable Prioritization of what is in use with runtime insights

30% Reduction in Alerts w/o Sacrificing Security

Stop attacks in motion with real-time detection



Service Offerings

- Native Cloud Security Controls Management
- Data & Endpoint Security
- Cloud Security Posture Management
- Cloud Workload Protection
- Threat Hunting & Investigation
- Threat Intelligence

Respond with live threat investigation. See the full lineage from user to process.

CoE skilled resource, Industry Expertise

Container Forensics , Fix at source, Automate compliance and governance

Data Resilience, Data Observability & Remediation

Active Threat hunting, Threat intelligence, AI/ML contextualized led automated response

Multi-layered Threat Detection

Let’s get to the future, faster.

Together.

Thank You

LTIMindtree: A Quantum Ready Partner

Strong Complimenting Workforce

We have already built a strong team of 20+ Research Engineers, Quantum Native Developers, ML engineers and Domain experts complimenting each other. We are growing further…

Collaborative Ecosystem Development

We are establishing collaboration ecosystem with Quantum Tech Orgs, statups and academia.

IBM

QUANTUMXCHANGE

amazon

D:Wave The Quantum Computing Company

UNIVERSITY OF OXFORD

QuEra COMPUTING INC.

Learning & Development

Continuous learning and upskilling on latest Quantum Computing Frameworks (e.g. Quera, IBM Qiskit, Dwave Ocean)

Research and Development

We have adopted an ‘Science Led and Enterprise Driven’ Applied research approach towards building Industry focused use cases (e.g. Portfolio Optimization, Fraud detection etc.)

Service Offerings

Quantum-Safeguard Discovery and Assessment (QSDA)

Quantum-Safe communications POC

Quantum-Safe VPN