WORD DOCUMENT

Service Catalogue – Cybersecurity Practice

Document Version/Details: 1.0/ 15-Mar-2024

Record of Release

Version No.	Modified By	Reviewed By	Authorized By	Release Date	Modifications Done
1.0	Shriram Tyagrajan	Ritika Kumar	Sanjay Bhutada	15-Mar-2024	First version. Created a document with services provided specific from Cyber security practice

Table of Contents

1.0 Purpose

This Service Catalogue has been prepared by the Cybersecurity Practice Business Unit (Cybersecurity BU) of LTIMindtree to provide the following information:

- List of all services that are provided by Cybersecurity BU to its clients
- List of Key Performance Indicators and measurement metrics associated with each service provided
- List of pricing options available for procuring any of the services listed out

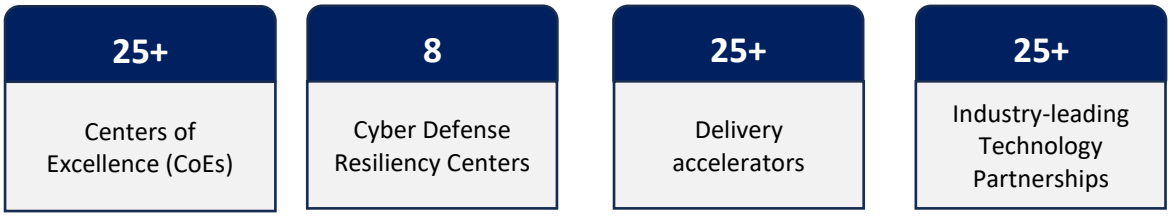
2.0 Service Definition

Digital transformations bring along tremendous benefits, but not without threats to the privacy and security of crucial enterprise data. In present times, cyberattacks are rampant, and new-age cyber threats require dexterous strategies. Therefore, enterprises need to develop cyber defense resilience to counter such incidents.

At LTIMindtree, we follow a customer-centric approach to create cybersecurity solutions that help our clients build resilient enterprises. We offer platform-based enterprise cybersecurity solutions, which are proactive, prescriptive, and cognitively autonomous.

As a security transformation partner, we have helped over 220 clients in more than 30 countries build personalized security roadmaps aligned to their digital transformation goals. We create digital cyber defense capabilities to solve some of the most complex challenges and secure digital transformations at scale.

Our state-of-the-art enterprise cybersecurity solutions are powered by:



Based on our association with our diverse clientele, we understand that customers today want to be "Digital enterprises" and they are at different points in their journey. They want to win consistently, and to Digital completely from competition, with a far-sighted vision to be distinctive, and an overarching ambition to stay ahead of the competition. Some companies have what it takes to be the winner, which can disrupt and embrace disruption at the same time. An enterprise that enables new business models, generates new revenue models, is operationally superior, and enriches experiences. An enterprise that does not just survive but thrives in the new and changing environment.

At LTIMindtree, it is our endeavour to help our customers be the Digital enterprise by managing their Cyber Defense or its journey to pro-actively Monitor, Detect and Secure Digital Assets. To help them excel and lead by powering their ability to transform experiences, use operations as a lever to transform, become data-driven organizations, and digitize their core.

At LTIMindtree, we follow a customer-centric approach to create cybersecurity solutions that help our clients build resilient enterprises. We offer platform-based enterprise cybersecurity solutions, that are proactive, prescriptive, and cognitively autonomous.

As a security transformation partner, we have helped over 220 clients in more than 30 countries build personalized security roadmaps aligned with their digital transformation goals. We create advanced cyber defense capabilities to solve some of the most complex challenges and secure digital transformations at a scale. Our current portfolio of services covers an end-to-end spectrum across consulting, implementation, transformation, and managed services. Our services focus on helping organizations stay ahead of the attackers and weave resiliency across the enterprise ecosystem. We focus on not just protecting the present but scaling it for the future.

Our security transformation approach builds a personalized roadmap for Cybersecurity maturity aligned with our customer's digital transformation ambitions.

Our value proposition include -

- Trusted Partner for large-scale transformation
- Experience of delivering business transformation for Enterprises across their value stream for multinational global enterprises across all verticals
- Deep, best-in-class capabilities across major industry verticals and digital-first customer journey
- Partner / Client-friendly solution (no vendor lock-in) – Open standard, Always ON, Flexible, Agile, and Ease of sustenance
- Best Practices & LTIMindtree's custom framework adoption during the build phase
- Flexible "Everything as a Service model" with top-notch accelerators, platforms, and strategic partnerships
- Library of Use cases and playbooks from day 1 of Operations
- Experienced, Certified, and Skilled Top Talent across Best of Breed products across 60+ different subdomains
- Platform-driven approach to security, fortified by a modern engineering mindset

Digital Enterprises – the Four Strategies

- Operate, To Transform: Though traditionally considered a back-office function and a cost center, we have started seeing Operations through a new lens and believe it to be the engine for creating a lot more value than just keeping the lights on. Application of the digital levers of Analytics, AI, Automation, and Experience enables us to look at Operations as a treasure trove of insight.

- Data-Driven Organization: Across industries, we have evolved our Cyber Threat Data to unlock real benefits for leaders who are cognizant of the importance of Cyber Defense, and for organizations that are becoming increasingly aware of the direct business benefits of Cybersecurity.

- Experience Transformation: With superior customer experience now critical for every industry, business transformation is increasingly guided by the need for better customer interfaces, faster and more robust Cybersecurity, more connected processes, and improved data insights around Cybersecurity Threats, Detection and Response.

- Digitizing the Core: Digitizing the Core Data-driven modernization, a key component in enabling Cybersecurity making based on data-driven insights rather than instincts or

tedious processes, is the top priority and a challenge today for all leading organizations.

Operate, To Transform (Do Less, Do Fast, Do More, Do Better)

We see Operations through a new lens and believe it to be the engine for creating a lot more value than just keeping the lights on.

We, at LTIMindtree, have shifted gears from treating Operations as a 'big spend' in running any business or function (it traditionally constitutes 40-70% of the ongoing spend) to seeing it as a platform to transform enterprises in their Digital journeys. With our deep understanding of the evolving and emerging needs of the Digital enterprise, we see a distinct opportunity to repivot Operations from a 'keep the business running function' to 'keep the business transforming function'. Our Pinnacle Cybersecurity platform is aims to deliver to this new opportunity, thus augmenting the LTIMindtree strategic core designed to steer the transformation of Digital organizations. Powered by our 4D model (Do Fast, Do Less, Do More, Do Better), the O2T (Operate to Transform) delivers operations and business transformation across the four key dimensions of Operations, Landscape, Business Process KPIs and End-User Personas for our customers.

Data-Driven Organization (Data as an enterprise asset, AI led automation, Monetization of data, Right data, right time, right people)

At LTIMindtree, we understand that data is the new oxygen for a Digital enterprise. However, maintaining a robust, data-driven framework, along with analytical capabilities, is a daunting task. Our Pinnacle platform, along with its components, enhances our client's Cybersecurity advantage. LTIMindtree's Pinnacle is a converged platform, offering Advanced Threat & Vulnerability Management, Cyber Defense Resiliency Centers (CDRCs), Identity Management, Data Security, GRC, Cloud Security, OT Security and improved solution experience to its users. Pinnacle enables organizations to undertake quantum leaps in business transformation and brings an insights-driven approach to Cybersecurity making. It helps deliver solutions at the intersection of physical and digital worlds.

Experience Transformation (Empathy led, Persona and journey driven, Immersive to the core, Human centric)

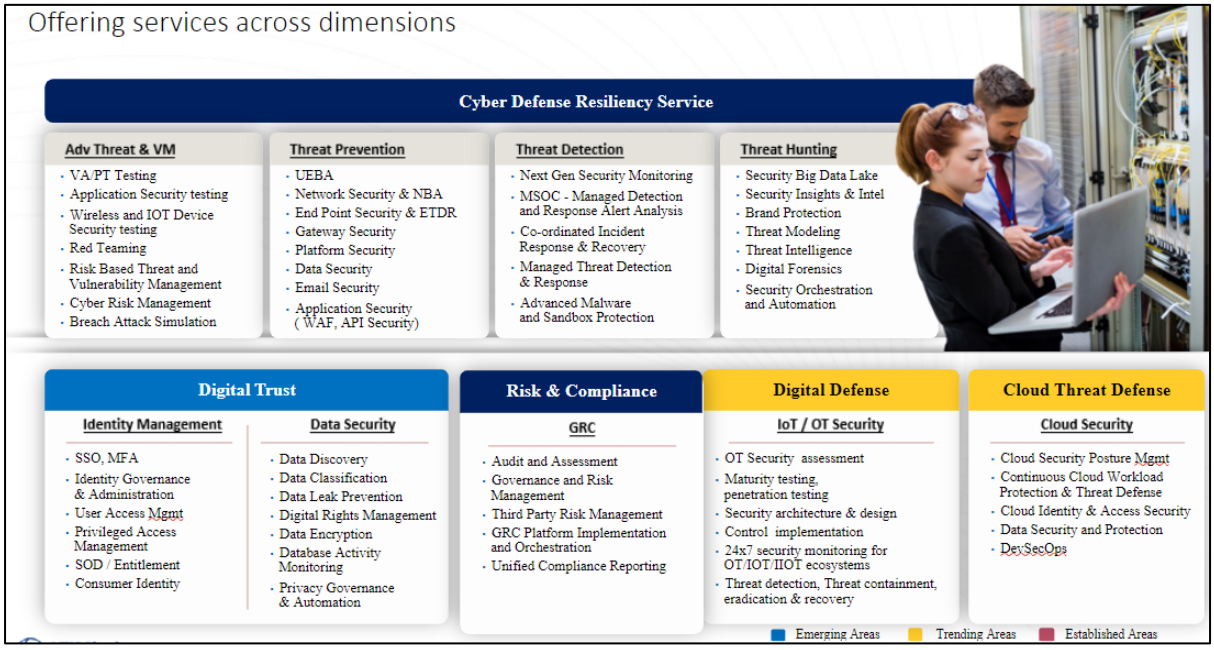
Experience is the only common denominator in managing customer perception and retaining customers over the long term. As the role of immersive customer engagement increases in this changing business environment, companies adopt data more comprehensively to understand user behaviours, journey and life cycle, and, most significantly, how they want their assets to be secured using Cybersecurity solutions. This enables them to implement a pro-active, analyzed, detected, well-defined response to cyber threats thereby securing the organization much faster. Using the power of the digital to read between the lines, LTIMindtree has been consistently delivering 'experience transformation' for its customers. We are helping them harness the power of transformed experiences with human-centric design.

Digitizing the Core (Define the core, Messy legacy to digital core, integrate everything with digital core, Embed automation & intelligence)

It is critical for a successful corporation to understand the multi-dimensional nature of Cyber Defense and integrate various layers at the core of its business infrastructure, platforms and applications. It needs to be understood that without this strong digital core, it cannot scale or sustain digital business transformation. A Digital enterprise recognizes this and takes well-defined steps to establish a digital ecosystem embedded with principles of Cybersecurity at various levels. Powered by cyber threat data, SIEM, SOAR, Data Analysis, secure network infrastructure, BYOD devices, mobile applications, and streamlined business processes, the modern enterprise integrates, incorporates and enhances varied Cyber Defense capabilities, to support the core of data architectures. LTIMindtree is helping its clients move from legacy security practices to a digital core, enabling their business to evolve to a transformed stage of functioning.

LTIMindtree leverages its deep understanding of client's business processes to provide a unique service to help them accelerate their journey to a mature Cybersecurity Framework and of course manage their Digital Infrastructure. To help our consultants achieve this better understanding of clients' business, we have aligned our Cybersecurity sales and delivery organizations to service specific industry verticals. Cybersecurity Services consist of the design, implementation, and management of client's Cybersecurity landscape.

To support the same, our services are organized to secure our customers' end-to-end Cybersecurity Landscape.



Below sections describe services under each of these along with our "Service Lifecycle Framework". Our Service Lifecycle Framework is based on the 3R's spread across Recent (New services to differentiate), Retention (updates to existing offering to align with market) and Retirement (exit the services from selling).

3.0 Service Lifecycle Framework

Recent – Introduction of new services to differentiate from the competition

1. Ideation
   Service offering concept creation and mapping with current tech stack, vision and strategy of the BU
   - Source of the idea
   - SWOT analysis of the service proposed
   - Brief summary of the service proposed for development
   - What are the industry challenges that the service can solve, market need?

2. Market assessment
   Positive forecast from Analyst assessment, Market trends, Competition research
   - Market feasibility of the service
     - Is the market genuine and legitimate (backed by trusted studies)
     - Potential customers in the market
     - Is the market fast growing
   - Identification of competitors in the market
     - What are their offerings in the same segment and what could be LTIMindtree differentiators?
     - Study their pricing, operations and marketing activities structure
   - Analyst assessment
     - What should be the target industries
     - Demographics and needs of the market
     - Purchasing behavior and spending power of the market towards tech services

3. Business Case Development
   Develop a robust framework for evidence-based and transparent Cybersecurity
   - Service Definition
     - Specifying the service offering in depth
     - Key Benefits and value proposition for LTIMindtree and clients
   - Financial propositions
     - Present the market data and prepare costing
     - Investment - technological, cross-skilling and upskilling costs, manpower acquisitions
     - Returns of investment – tangible monetary returns, intangible business impacts
   - Offering development plan
     - Enlist key milestones, prepare costing, plan resource management
     - Identification of risks and propose mitigation measures

4. Develop offering
   Identification of an effective process to create offerings and make them market-ready
   - Deliverables, Delivery model(s), Delivery life-cycle, Tools and Accelerators
   - Key components of services – Connectivity, Security, Processes
   - Establish performance metrics and governance mechanism
   - Create working proof of concept and conduct internal pilot runs
   - Confirm delivery readiness

5. Sales and Distribution planning
   Achieve sales readiness and control where we want to take our service and how
   - Creation of service catalogue and capability deck
   - Design, create and distribute sales collaterals such as brochures, battlecards, flyers
   - Prepare internal document such as elevator pitch, sales guide, FAQs, use case repository
   - Conduct training sessions for LTIMindtree representatives on the requisite knowledge of the service

6. Service announcement
   Commercialization and communication
   - Create an enthralling Press Release
   - Launch Social Media Marketing campaigns on LinkedIn & Twitter
   - Update relevant sections on our website update and maximize Search Engine Optimization
   - Leverage field marketeers, onsite sales offices, and other corporate communication channels for maximum outreach

7. Post-launch activities
   Business relationship engagements and continuous evolvement
   - Conduct trainings and information webinars
   - Participate in Analyst briefings

In the idea economy, in order to succeed, organizations need best ideas which address the client needs. Idea generation should not be restricted to only a set of people as great ideas could come from various corners of the organization.

With participation open across the BU, we invite new idea proposals and solutions throughout the year, which post-evaluation by our expert committee, are realized and incorporated to our current array of customer offerings. Offerings are then built by Cybersecurity Practice based on the feasibility and readiness of the ideas selected by the expert committee.

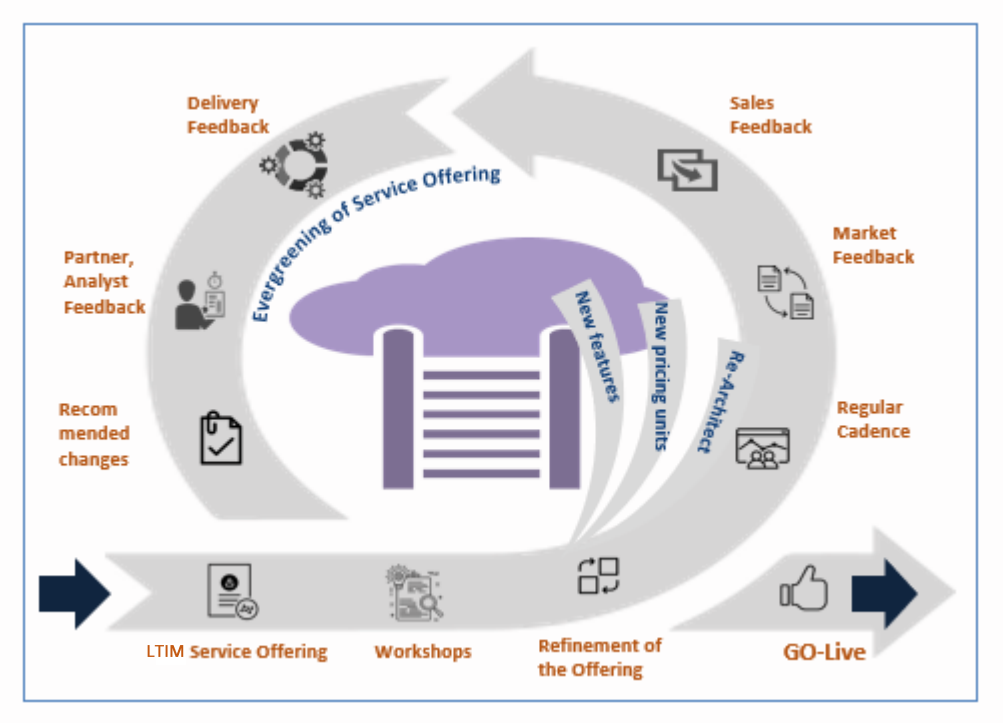
Cybersecurity Practice has helped nurture a high-order thinking environment in the BU and has helped achieve some out-of-the-box solutions. This has improved our quality of offerings and allowed us to position ourselves better in the charts of the leading global analysts.

To learn more about the Cybersecurity Practice, please visit our website at:
LTIMindtree Cybersecurity Portal

Retention – Updates to the existing offerings to align with market

Service retention or enhancement is a continuous improvement continuous development process where we input constant feedback from the various stakeholders associated with the service offering and incorporate the same in order to attain an evergreening of our services.

The below flow chart depicts the various steps in our retention framework.



Retirement – Exit the services from selling

1. We wish to exit the market – that is, we don't want to be in the market anymore. This could be due technological, legal or geographical reasons.

2. Cost is exceeding our revenue – Current performance of the product will give us the relation between cash inflows (whatever we are getting from the customer) and cash outflows (resource cost + employees cost) and will give us an idea where we are leaking the money. Ensuring no further optimization is possible, we will take a call on retiring the service.

3. If the market has matured (according to Gartner and Forrester reports) no further impact can be made.

   Based on the above factors, we will decide to either change or discontinue the service. For discontinuing the service, a roadmap for retiring and taking it off our portfolio will be used.

4. Roadmap: Vision strategy, wins (freeing of HR + IT resources) and losses (risk of losing customers), getting approval on the roadmap, formal communication to all the stakeholders, separate communication to the customer (prepare them for it) phased manner, reallocate or redeploy the freed resources in a more profitable setup

4.0 Engagement Options

All services provided by Cybersecurity Practice are listed out in Section 4.0 of the document. It is however not necessary for a client to procure all these services at once and a client has a choice to procure a sliver of service using one of the following engagement options.

- Out-tasking / Co-sourcing

  In this engagement model, the client employs LTIMindtree to carry out a limited set of tasks within one or more service towers. This engagement model is best suited for clients that are seeking to augment their IT support for key services.

- Limited Outsourcing

  In this engagement model, the client employs LTIMindtree to provide support for a complete service tower (e.g. SIEM/SOAR) with all support tasks required for providing service included in scope. This model is best suited for clients, with a strong focus on outsourcing their non-core activities but still desiring to retain some level of control over delivery of services.

- Total Outsourcing

  In this engagement model, the client employs LTIMindtree to support its entire IT Infrastructure landscape. In this model LTIMindtree takes complete responsibility of designing, implementing and supporting IT Infrastructure complements required for supporting the in-scope landscape. This model is best suited for clients who are seeking to outsource their entire IT Infrastructure and are ready to transfer the associated risk and control to LTIMindtree.

5.0 List of Cybersecurity Services

5.1 Service: Cloud Security

Element	Description
Service	Cloud Security
Status	LIVE
Description	At LTIMindtree, we understand the security roadblocks in an organization's cloud-first journey. Our enterprise cloud security services and solutions are based on strategic partnerships with industry-leading cloud providers. We follow a collaborative platform-based approach that enables enterprises to manage hybrid

	and multi-cloud environments and navigate their cloud transformation journey in a secure and accelerated manner. Key Service Offerings: • Cloud Security Posture Management (CSPM) • Cloud Workload Protection Management (CWPM) • Cloud Threat Detection and Response (CTDR)
Service Category	This service falls under the Cloud Security services category.
Service Owner	BU Head & respective Technology Office Lead
Service Criticality	The criticality of the service will be determined by understanding the Business criticality of the functions supported and will be documented in the SDP.

Standard Service Features	CSPM - Cloud Security Posture Management • Visibility and Insights in Cloud • Strengthen security and compliance posture. • Protect against threats and Automated response. • Help to Secure faster. CWPM - Cloud Workload Protection • Protection of Workloads, Endpoint, Serverless, Application, API/Interface • Continuous Vulnerability scanning of workloads and remediation. • Hardening of Workloads and Network • Detection of threats on workloads and response Cloud Defense SIEM • Seamless Integration • Data lake for logging & analytics • Real-time security incident detection, monitoring, and response. • Enrichment of security incidents and continuous Threat hunting • Automation and Playbooks to handle security incidents. Data Security • Encryption of Data • Data discovery, classification, and labeling. • Data Loss Prevention prevents unauthorized data sharing intentionally/unintentionally. • Data Masking & Tokenization protects sensitive data with masking and tokens. • Data Anonymization removes PII datasets, sanitizes data, and remains anonymous. CASB - Cloud Access Security Broker • Discovery and Visibility of Shadow/Non-shadow IT • Application compliance assurance • Protecting Data/Information from data loss/unauthorized access • Detection of Threats and automated response CIEM - Cloud Infrastructure & Entitlement Management • Discovery and Visibility of human/non-human identities and entitlement • Monitor, enforce, and remediate the risk (excessive/unauthorized/inactive access) • Identity Anomaly behavior detection based on AI/ML and response. • Ensure the Principle of least privileges (JIT, JEA) Container Security • Detecting misconfiguration and automated response • Vulnerability scanning of container Image and hardening. • Run-time security to the container • Detect security threats at the cluster and node level.
Transformational services	• Strategy, Architecture & Planning • Cloud Security Assessment, Management, and Operations
Exceptions to the services	The service does not take into account, BUrchase/renewal of OS and application software licenses, hardware components, platform subscriptions, unless explicitly included in the contract.

Delivery Scope	All offerings that are mentioned in the Standard Service Features
Delivery Channels	• Remote support from our global delivery Centers • Desk-side support and multilingual support leveraging partner eco-system
Service Hours	The service window for this service is 24x7 or dependent on Client requirements
User Requirements	As requested by the user (subject to necessary Approvals)
Service Initiation	The services of Consulting, Transformation and managed services are triggered/ initiated via RFP/RFI process and proactive assessments done in existing accounts The user support service initiation for managed services is user driven and is initiated via the front end such as User Portal, Bots, Phone Email, Chat, etc. The Service Desk function acts as the single point of contact for the services.
Service Support	An engagement manager will be assigned, for issue escalation and resolution. A steering committee will also be set up for any extraordinary issues and their resolution. Day to day operations is effectively managed with reports and review mechanisms
Standard Costs	• Fixed Cost based pricing depending on size of client's landscape, support coverage requirements and service level expectations • RU Based pricing model depending on landscape (User, Device, Applications, etc.) • Time & Material based pricing based on number of resources working on the engagement
Optional Costs	Depends on the type of engagement and scope of services.
Service Targets	Please refer to Section 6 of the CYBERSECURITY Service Catalogue - Service Delivery Metrics and Measurements

5.2 Service: Cyber Defense Resiliency Service (CDRS)

Element	Description
Service	MxDR
Status	LIVE
Description	At LTIMindtree, Our Managed Security Services portfolio is designed to set up a comprehensive cyber security framework for organizations with 24X7X365 support. We are a trusted security partner to 220+ global enterprises, including some of the largest Fortune 500 companies. We at LTIMindtree specialize in championing large scale security transformations and solving security challenges from simple to some of the most complex ones.
Service Category	This service falls under the Managed Security Services category.
Service Owner	BU Head & respective Practice Head

Service Criticality	The criticality of the service will be determined by understanding the Business criticality of the functions supported and will be documented in the SDP.
Standard Service Features	**Managed Endpoint Security with EPP & EDR** **Consulting and Architecture/Design** • Technology Roadmap and Vendor Selection • Network Security Architecture and Business Continuity planning • Preparation of High-level (HLD) and security capabilities and design • Micro-segmentation • Third Party Integrations **Migration Service** • EDR / EPP Migration Assessment and planning • Pre-migration planning • Migration, Fallback, and testing during the actual migration. • Post-migration validation • Migration to the same vendor or different OEM solution **Managed Services** • 24/7 Anti-Virus Detection Response, Endpoint Detection & Response • Monitoring, alerting, and reporting device parameters and performance. • Containment & Response Automation • Advance Threat Hunting • Service reviews; monthly, quarterly, or annually, performance reporting and dedicated service management **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.

	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. Mobile Device Security • Endpoint Security: Monitoring mobile devices continuously to detect threats and alert security teams to act when necessary. • Virtual Private Networks (VPN): Deploying VPNs to ensure that the data transmitted through mobile devices is securely encrypted. • Secure Web Gateways: Integrating security with the cloud to identify an attack on one location and immediately prevent it at other branches. • Email Security Solutions: Ensuring end-to-end encryption of the data transmitted through emails. • Cloud Access Security Broker: We leverage CASB tools to ensure a secure gateway between on-prem infra and cloud apps. • Deployment of strict security policies
Optional Service Features	Assessment & On-boarding existing clients into delivery platform
Transformational services	• Security Orchestration & Automation • Software Composition Analysis (SCA) • Security Misconfiguration • Mobile Device Security Policy Management • Threat Detection and Response Management of Mobile Devices
Exceptions to the services	The service does not consider, purchase/renewal of application software/tools licenses, unless explicitly included in the contract.
Delivery Scope	All infrastructure areas that are in scope of the contract awarded by the Client to LTIMindtree.
Delivery Channels	• Onsite Support • Offshore Support
Service Hours	The service window for this service is 9x5 or dependent on Client requirements
User Requirements	NA
Service Initiation	Service will be initiated in two ways • On request from the client • At the start of a remote management engagement where implementation of tools will be initiated by LTIMindtree
Service Support	An engagement manager will be assigned, for issue escalation and resolution. A steering committee will also be set up for any extraordinary issues and their resolution.

Standard Costs	• Time & Material based pricing based on number of resources working on the engagement • Fixed Cost based pricing depending on an agreed upon scope of implementation provided by the client
Optional Costs	Depends on type of engagement and scope of services.
Service Targets	Service targets for activities will be finalized based on the scope of the engagement.

5.3 Service: Governance, Risk and Compliance (GRC)

Element	Description
Service	Governance, Risk and Compliance (GRC)
Status	LIVE
Description	LTIMindtree's GRC services are designed and customized for enterprises to sustainably manage and govern their information and cyber security program. A well-rounded GRC framework facilitates the formulation and sustained management of information security risks. Such a framework helps identify risks proactively & systematically, and enables the security governance function to achieve adequate and mature security with the desired levels of internal & external compliance.
Service Category	This service falls under the GRC Services category.
Service Owner	BU Head & respective Practice Head
Service Criticality	The criticality of the service will be determined by understanding the Business criticality of the functions supported and will be documented in the SDP.
Standard Service Features	Management Services • Based on Managed GRC Services platform LTIM Pinnacle • V-CISO as-a-service • Cybersecurity Advisory Services for Board/CISO organization • Managed GRC Office • IT Governance • Technology Risk Management • Industry & Regional Regulatory Compliance Cybersecurity Maturity as-a-service (powered by OEM platform) • Platform-enabled cybersecurity maturity/performance assessment and management services • Remediation roadmap • Remediation advisory

	Managed GRC Automation as-a-Service (powered by OEM platform) • Technology enablement for (Cyber) Risk, Policy and Compliance and Audit Management – Platform Implementation & Support services • Discovery, assessment, baselining and other consulting services Cyber Risk Quantification Service (powered by OEM platform) • Platform implementation and configuration services Compliance-as-a-service • Continuous controls compliance monitoring against standards/frameworks • Remediation roadmap • Remediation advisory Attestation/Certification* readiness assistance • Consulting services Cybersecurity Audit/Assessment Services • Governance Audits • Compliance Audits • Information Security Audits • 3rd Party/Supply Chain Audits Managed Third-Party Risk Management as-a-service (powered by OEM platform) • Platform Implementation & Support Managed Security Awareness & Training as-a-service (powered by OEM platform) • Platform-enabled security education and training delivery • Automated phishing simulation exercises for awareness CISO Dashboard as-a-service (powered by OEM platform) • Platform-enabled security metrics reporting • Executive, customized dashboarding *For certain standards
Transformational services	CISO Dashboard as-a-service Cybersecurity Maturity as-a-service Risk Quantification as-a-Service Managed Third-Party Risk Management as-a-service
Exceptions to the services	The service does not consider, BUrchase/renewal of ServiceNow software/tools licenses, unless explicitly included in the contract.
Delivery Scope	All infrastructure areas that are in scope of the contract awarded by the Client to LTIMindtree.
Delivery Channels	• Onsite Support • Offshore Support

Service Hours	The service window for this service is 8x5 or dependent on Client requirements
User Requirements	NA
Service Initiation	Service will be initiated in two ways • On request from the client • At the start of a remote management engagement where implementation of the tools will be initiated by LTIMindtree
Service Support	An engagement manager will be assigned, for issue escalation and resolution. A steering committee will also be set up for any extraordinary issues and their resolution.
Standard Costs	• Time & Material based pricing based on number of resources working on the engagement • Fixed Cost based pricing depending on an agreed upon scope of implementation provided by the client
Optional Costs	Depends on type of engagement and scope of services.
Service Targets	Service targets for activities will be finalized based on scope of the engagement.

5.4 Service: Advanced Threat & Vulnerability Management

Element	Description
Service	Vulnerability Management
Status	LIVE
Description	LTIMindtree's Advanced Threat & Vulnerability Management (ATVM) has a strong and comprehensive vulnerability management practice, that supports the organizations application and Infrastructure across on-premise, cloud infrastructure, digital environment. Our services provide an end to end comprehensive view of the overall security posture of your application and infrastructure landscape.
Service Category	This service falls under the Vulnerability Management Services category.
Service Owner	BU Head & respective Practice Head
Service Criticality	The criticality of the service will be determined by understanding the Business criticality of the functions supported and will be documented in the SDP.
Standard Service Features	Infrastructure Security Vulnerability Management • Vulnerability Assessment • Penetration Testing • Secure Configuration Review • Compliance Assessment • Remediation Advisory

	• AI/ ML Based Triaging and managing remediation and Remediation Assistance Application Security Vulnerability Management • Threat Modelling • Static Application Security Testing • Software Composition Analysis • API Testing • Dynamic Application Security Testing • Penetration Testing • Remediation Advisory Breach Attack Remediation Red Teaming Attack Surface Management
Transformational services	• Risk Based Vulnerability Management • DevSecOps • Automated Threat Modeling • Automated Infrastructure Penetration Testing • Vulnerability Orchestration and Automation Remediation Product
Exceptions to the services	The service does not consider software/tools licenses, unless explicitly included in the contract.
Delivery Scope	All application and infrastructure areas that are in scope of the contract awarded by the Client to LTIMindtree.
Delivery Channels	• Onsite Support • Offshore Support
Service Hours	The service window for this service is 8x5 or dependent on Client requirements
User Requirements	NA
Service Initiation	Service will be initiated in two ways • On request from the client • At the start of a remote management engagement where implementation of the tools will be initiated by LTIMindtree
Service Support	An engagement manager will be assigned, for issue escalation and resolution. A steering committee will also be set up for any extraordinary issues and their resolution.
Standard Costs	• Time & Material based pricing based on number of resources working on the engagement • Fixed Cost based pricing depending on an agreed upon scope of implementation provided by the client
Optional Costs	Depends on type of engagement and scope of services.
Service Targets	Service targets for activities will be finalized based on scope of the engagement.

5.5 Service: OT/IoT Security

Element	Description
Service	OT/IoT Security
Status	LIVE
Description	As a part of the L&T group, LTIMindtree, with the quintessential engineering DNA, has a competitive edge while creating OT/IoT security solutions. Our rich domain experience in heavy industrial engineering and smart cities makes it easier to relate to the challenges of various industries and manage the complexities of OT/IoT security risks. With our network of industry-leading technology partners, in-house IPs, frameworks, and playbooks, we deliver robust and integrated OT/IoT security services for our customers.
Service Category	This service falls under the OT Security Services category.
Service Owner	BU Head & respective Practice Head
Service Criticality	The criticality of the service will be determined by understanding the Business criticality of the functions supported and will be documented in the SDP.
Standard Service Features	Network and Data Security • Network segmentation • Ransomware encryption protection Endpoint Security and Vulnerability management • System Hardening • Vulnerability management • App whitelisting • Penetration Testing Access Management • Role-based Access Controls • Secure Remote access Security Monitoring and Incident Response • 24*7 Security monitoring and threat detection • Incident response • Cyber Crisis management • OT Threat Intel analysis and reporting • Threat Hunting GRC • Defining OT Security Policies and procedures

	• OT System management • Asset management • Security awareness trainings for users • OT Security maturity assessments Supplier risk management • Third party risk management
Transformational services	• Endpoint Security and Vulnerability management • GRC
Exceptions to the services	The service does not consider, Purchase/renewal of ServiceNow software/tools licenses, unless explicitly included in the contract.
Delivery Scope	All OT/IoT infrastructure areas that are in scope of the contract awarded by the Client to LTIMindtree.
Delivery Channels	• Onsite Support • Offshore Support
Service Hours	The service window for this service is 8x5 or dependent on Client requirements
User Requirements	NA
Service Initiation	Service will be initiated in two ways • On request from the client • At the start of a remote management engagement where implementation of the tools will be initiated by LTIMindtree
Service Support	An engagement manager will be assigned, for issue escalation and resolution. A steering committee will also be set up for any extraordinary issues and their resolution.
Standard Costs	• Time & Material based pricing based on number of resources working on the engagement • Fixed Cost based pricing depending on an agreed upon scope of implementation provided by the client
Optional Costs	Depends on type of engagement and scope of services.
Service Targets	Service targets for activities will be finalized based on scope of the engagement.

5.6 Service: Data Security

Element	Description
Service	Data Security
Status	LIVE
Description	LTIMindtree's Data Security services are focused on data as the primary asset encompassing its lifecycle, aimed at offering end-to-end protection to the clients' enterprise data.

	Key Differentiators include: • Expertise on Data Lifecycle Management • In-depth understanding of comprehensive protection mechanisms. • Tightly integrated with GRC to address business and compliance requirements.
Service Category	This service falls under the Data Security Services category.
Service Owner	BU Head & respective Practice Head
Service Criticality	The criticality of the service will be determined by understanding the Business criticality of the functions supported and will be documented in the SDP.
Standard Service Features	Data Security Lifecycle Management • Data Loss Prevention • Database Access Monitoring (DAM) • Information Rights Management (IRM)/DRM • Public Key Infrastructure (PKI) • Data Discovery • Data Classification • Data Masking • Data Tokenization • Data Encryption Next-Gen Data Security Services • AI/ML for true detection • Multi-cloud data security • HSM-As-A-Service • Automated remediation with Playbooks • Unified Management Console • UEBA with CASB • PKI-As-A-Service • Advance Reporting & Analytics
Transformational services	• Next-Gen Data Security Services
Exceptions to the services	The service does not consider, Purchase/renewal of ServiceNow software/tools licenses, unless explicitly included in the contract.
Delivery Scope	All infrastructure areas that are in scope of the contract awarded by the Client to LTIMindtree.
Delivery Channels	• Onsite Support • Offshore Support
Service Hours	The service window for this service is 8x5 or dependent on Client requirements
User Requirements	NA
Service Initiation	Service will be initiated in two ways • On request from the client

	• At the start of a remote management engagement where implementation of the tools will be initiated by LTIMindtree
Service Support	An engagement manager will be assigned, for issue escalation and resolution. A steering committee will also be set up for any extraordinary issues and their resolution.
Standard Costs	• Time & Material based pricing based on number of resources working on the engagement • Fixed Cost based pricing depending on an agreed upon scope of implementation provided by the client
Optional Costs	Depends on type of engagement and scope of services.
Service Targets	Service targets for activities will be finalized based on scope of the engagement.

5.7 Service: Identity Management

Element	Description
Service	Identity Management
Status	LIVE
Description	LTIMindtree's Digital Identity Assurance Compliance Platform incorporates identification, authentication, and authorization, and coupled with advanced monitoring & analytics engines, offers comprehensive protection from unauthorized access and modifications. This ensures that while the approved users have the necessary access to perform their jobs, unauthorized users are kept away from sensitive resources and information. Through LTIMindtree's Digital Identity Analytics and Orchestration Platform, enterprises can realize tangible business value, including increased operational efficiency, benefits of automation, orchestration, robust security, improved action-oriented visibility, simplified regulatory compliance, and enhanced employee & customer satisfaction.
Service Category	This service falls under the Identity Management Services category.
Service Owner	BU Head & respective Practice Head
Service Criticality	The criticality of the service will be determined by understanding the Business criticality of the functions supported and will be documented in the SDP.
Standard Service Features	Access Management • Password less Authentication • Single Sign-On on Legacy, modern and web applications • Zero Trust based Adaptive Access Deployments • Access Analytics • Migration to another SSO

	Identity Governance Administration • Automated JLM • Access Workflow • Access Certification Campaigns • Role/Policy Based Access • Audit and Compliance Reporting • Framework based Assessments Privilege Identity & Access Management • Enterprise password vault management • Privilege Session Management • Privileged Activity Monitoring • Privilege Threat Analytics • Endpoint Privilege Management • App Control & Credential Theft Protection • Just in Time Access for Privileged Access • Audit and Monitor Privileged Management • Privileged Governance and Compliance Consumer Identity and Access Management • Self-Registration, Social Login, Consent Management • Account Validation • Single Sign-On & self-service portal • Access Analytics • Dashboarding on the key metrics for Access • Protect access with Multi Factor Authentication Directory Services • Design and Architect new Directory Services • Identity consolidation into single Directory Repository • Single Source of Truth • Privilege Threat Analytics • Consolidation of Directory Services into Large Directory • Migration of Directory Services
Transformational services	• Directory Services Program • Identity Governance Administration
Exceptions to the services	The service does not consider, purchase/renewal of ServiceNow software/tools licenses, unless explicitly included in the contract.
Delivery Scope	All infrastructure areas that are in scope of the contract awarded by the Client to LTIMindtree.
Delivery Channels	• Onsite Support • Offshore Support
Service Hours	The service window for this service is 8x5 or dependent on Client requirements

User Requirements	NA
Service Initiation	Service will be initiated in two ways • On request from the client • At the start of a remote management engagement where implementation of the tools will be initiated by LTIMindtree
Service Support	An engagement manager will be assigned, for issue escalation and resolution. A steering committee will also be set up for any extraordinary issues and their resolution.
Standard Costs	• Time & Material based pricing based on number of resources working on the engagement • Fixed Cost based pricing depending on an agreed upon scope of implementation provided by the client
Optional Costs	Depends on type of engagement and scope of services.
Service Targets	Service targets for activities will be finalized based on scope of the engagement.

6.0 Service Delivery Metrics and Measurements

NOTE: All Process Metrics and KPIs defined herein are CYBERSECURITY Internal targets to enable baselining and drive improvements at CYBERSECURITY Level.

While all Projects / Accounts are expected to capture these CYBERSECURITY level Metrics in MAP (Metrics Action Plan),

IT IS MANDATORY to comply with and track Service Level Agreements / KPI and Metrics as per Contractual agreements.

Sr. no.	Metrics						Baselines & Goals
	Definition				Data Collection		
	Metric Parameter	Definition/ BUrpose of the metric	Formula	Unit of metric	Mechanism	Frequency	Goals / Target (CYBERSECURITY Internal)
1	Incident Volume	Volume of Incidents created/ received in the environment [Incident Trends]	No. of incidents (By Priority) created or received in the measurement period	# Count	MAP	Monthly	Tracking and reporting only. Note: Query is by "Created/ Open date". To know what the volume month on month is
2	Incident Reduction	Quarterly incident trends [Trend]	[(Average No. of incidents received in the previous	%	SMR	Quarterly	Tracking and reporting. Must show reducing

			quarter - Average No. of incidents received in the current quarter)/ (Average No. of incidents received in the previous quarter)] * 100				trend of at least 5% YoY (white noise elimination is not counted) *Note: Scope increase / Other exception factors will need to be considered in calculation*
3	MTTR1 (Mean Time to Respond)	Average time taken to respond to incidents in a given period. [MTTR1 reduction]	Total time taken to respond to incidents (of a Particular Priority) / Total No. of Incidents (of that Particular Priority) assigned in the period	Time	MAP	Monthly	Tracking and reporting only. Must show reducing Trend
4	MTTR (Mean Time to Resolve)	Average time taken to resolve incidents in a given period. [MTTR reduction]	Total time taken to resolve incidents (of a Particular Priority) excluding Hold times / Total No. of Incidents (of that Particular Priority) resolved in the period (Note : Priority OR a Set of Priorities)	Time	MAP	Monthly	Tracking and reporting. Improvement Trend > =10% in Y1 > =5% improvement in Y2 & Subsequent years *Note: Auto resolved tickets via Monitoring/ event management system to be excluded from*
5	Overall TTR (Time to Resolve)	Speed with which the overall incident is effectively resolved (Creation to Resolution Stage) [Total Cycle Time]	Total time taken to resolve incidents (of a Particular Priority) / Total No. of Incidents (of that Particular Priority)	Time	MAP	Monthly	Tracking and reporting. Improvement Trend > =10% in Y1 > = 20% improvement in Y2 & Subsequent

			resolved in the period (Note : Priority OR a Set of Priorities)				years
6	Variance between TTR & MTTR	Reducing Gap between Overall Cycle time (TTR) verses Mean time to resolve (MTTR) [Process Maturity]	Overall TTR for a particular priority of incidents in the measurement period (minus) MTTR for that particular priority in the period (Note : Priority OR a Set of Priorities)	Time	MAP	Monthly	Tracking and reporting only. Reducing Quarterly - 15% *Note: Auto resolved tickets to be excluded from Calculation*
7	Incident Backlog	To track all Incidents that are not resolved or closed at the point of measurement. [Incident Backlog]	[No. of Incidents assigned to LTIMindtree assignment groups that are not in 'Resolved' or 'Closed' Status at the point of measurement/ Total No. of Incidents received in the period of measurement] * 100	%	MAP	Monthly	<= 3% of Monthly Incident count *Note: Auto resolved tickets to be excluded from Calculation.*
8	Service Request Backlog	To track all Service Requests that are not completed or closed at the point of measurement. [SR Backlog]	[No. of Service Requests assigned to LTIMindtree assignment groups that are not in 'Resolved/ Completed' or 'Closed' Status at the point of measurement / Total No. of SRs received in the period of measurement] * 100	%	MAP	Monthly	<= 5% of Monthly SR count Note: Auto resolved tickets to be excluded from Calculation.

9	Ticket Reopen Rate	Tracking of tickets that were not satisfactorily resolved and had to be reworked [Rework/ Customer Dissatisfaction]	[No. of incidents or service requests that were reopened by user or customer post resolution in the period / Total No. of resolved tickets in the period of measurement] * 100	%	MAP	Monthly	<=10% in Y1 <5% in Y2 < 3% Y3 Onward
10	Tickets not Updated	Tracking of tickets that have not been updated recently. [Effective Ticket Management]	[Total No. of incidents or Service requests not updated in last 48 hrs. (or 2 days) / Total No. of incidents or Service requests assigned to LTIMindtree Assignment groups] * 100	%	MAP	Monthly	Target <= 5% of Daily Average volume in that month *<u>Note:</u> Incidents and SR to be tracked separately* *Resolved & Closed Tickets to be excluded*
11	Ticket Hops	No. of Ticket assignment transfers before the ticket is addressed for the appropriate resolution [MTTR reduction] [Ticket Re-Assignment]	Sum of Total No. of reassignments across all incidents or Service Requests in the measurement period / Total No. of incidents or Service Requests resolved in the measurement period	%	MAP	Monthly	Tracking and reporting. Must show reducing Trend. 90% overall Tickets <= 3 Hops *<u>Note:</u> Any tickets that were transferred more than 3 times to be analyzed for improvement.*

							Incidents & Service Requests to be tracked
12	RCA Submission Timeline	% Root Cause Analysis (RCA) reports submitted to stakeholders as per agreed timelines. [RCA Rigor]	[No. of RCA submitted within SLA / No. of RCA due for submission in the measurement period]*100	%	MAP	Monthly	As per agreed RCA timelines per Contract. OR *In case there are no contractual Target Set/ agreed* - Internal KPI of >= 95% within 5 Business days *to be followed*
13	Change Volume	Volume of changes in the environment by (Planned) scheduled date [Change Trends]	No. of Change requests (By Type) scheduled in the measurement period	# Count	MAP	Monthly	Tracking and reporting only. Note: Planned Date of implementation. Change types include Normal, Standard, Emergency and Expedited/ Urgent.
14	Change Success Rate	% of changes that met the objective of the planned change (as originally planned) while following all Change Process requirements without causing an incident (or disruption) in the environment. [Change Success Rate]	[No.of Change requests (CR) that were closed as successful / No. of CR completed in the measurement period]* 100	%	MAP	Monthly	>= 95% *<u>Note</u>: Changes closed as Failed, Rolled back or Backed out are considered as unsuccessful changes.*

15	Fast Tracked Changes	% of Fast tracked Change Requests in the environment [Change Type Trend/ Control]	[No. of Emergency or Expedited (Urgent) changes scheduled in the period / Total No. of Change requests scheduled in the period of measurement] * 100	%	MAP	Monthly	<= 5% *Note: Important to keep Change backlog at a minimum to capture true state.*
16	Unauthorized Changes	Tracking of change requests that were implemented without following (or bypassing) the defined Change Management process. [Change Discipline]	No. of changes implemented without requisite approvals or those that were implemented without following defined Change Management process in the environment	# Count	MAP	Monthly	Target = 0 / Nil / None *Note: Changes that were deployed outside the approved Schedule time/ window or those that did not follow original/ approved Change plan are also treated as Unauthorized changes.* Any Change in in the environment without a change record must ideally create a CR and mark/ flag it as unauthorized.
17	VSM - Value Stream Mapping	Reduce "non value" added efforts [Eliminate Waste]	Effort Spent on Non Value added activities before VSM- Effort Spent on Non Value added activities post VSM	Effort	SMR	NA	Target = 1 VSM (@ Minimum) *Note: Duration 1 Month.*

7.0 Service Components

7.1 Service specific dependency list

Name of the service component	Service name/s	Category	Dependency target (For internal groups, it is OLA)
Laptop/Desktops	All Services	Hardware	OLA with IT Infra group
Network Connectivity	All Services	Communication Links	OLA with IT Infra group
Microsoft Office	All Services	Software	OLA with IT Infra group
MSA, SOW, SOPs, Project Documents and Cybersecurity	All Services	Data	Needs to be available in Project CMDB
Microsoft outlook, Messenger	All Services	Software	OLA with IT Infra group
Compass 2.0	All Services	Tool	Needs to be available during working hours. Adequate Role based access
Ticketing tool	All Services	Tool	Needs to be available during working hours. Adequate Access required to all team members
Monitoring tool	All Services	Tool	Needs to be available during working hours. Adequate Access required to all team members
Datacentre	Hosting & Colocation	Infrastructure	24x7 availability
Power Backup	Hosting & Colocation	Infrastructure	24x7 availability

LTIMindtree

Let’s get to the future, faster. Together.