



# Let's get to the future, faster. **Together.**

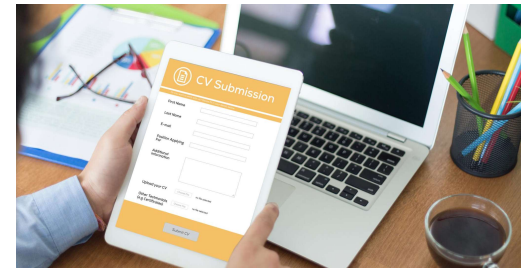
**Prepared for:** EDR-XDR Assessment  
as a Service



# Assessment as a Service

## Introduction

Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) Assessment as a Service is a comprehensive package designed to help LTIMindtree customer organizations efficiently evaluate and optimize their endpoint security posture. This service enables enterprises and other small and medium business to assess the effectiveness of their already deployed EDR/XDR solutions, identify gaps, and improve detection, investigation, and response capabilities. It helps understanding the return on investment.



## What is it?

### Conduct Assessments

Assessment as a Service is a solution that enables organizations to perform assessments with ease. This feature offers flexibility and convenience to both assessors and participants, allowing assessments to be taken from any location at any time.

### Flexible and Efficient Way to Conduct Assessments

Assessment as a Service provides a flexible and efficient method for organizations to conduct assessments. This service simplifies the scheduling process for organizations and facilitates a seamless experience for participants, resulting in a streamlined and effective assessment process.



# Benefits of Assessment as a Service

## ● Increased Efficiency

Assessment as a Service enables remote assessments, saving time and money associated with scheduling and administering them. It also provides instant feedback and results, reducing the time required for grading and evaluation.

---

## ● Flexibility

Assessment as a Service offers organizations the flexibility to conduct assessments anytime and anywhere. This makes it easier for organizations to schedule assessments and for participants to take them.

---

## ● Scalability

Assessment as a Service allows organizations to scale assessments up or down based on their needs, facilitating efficient management of assessment resources.

---

## ● Improved User Experience




This service allows participants to take assessments from anywhere, making it more convenient and accessible.

This results in a better user experience and higher engagement. Additionally, it provides instant results and feedback, helping participants understand their strengths and weaknesses and offering opportunities for improvement.

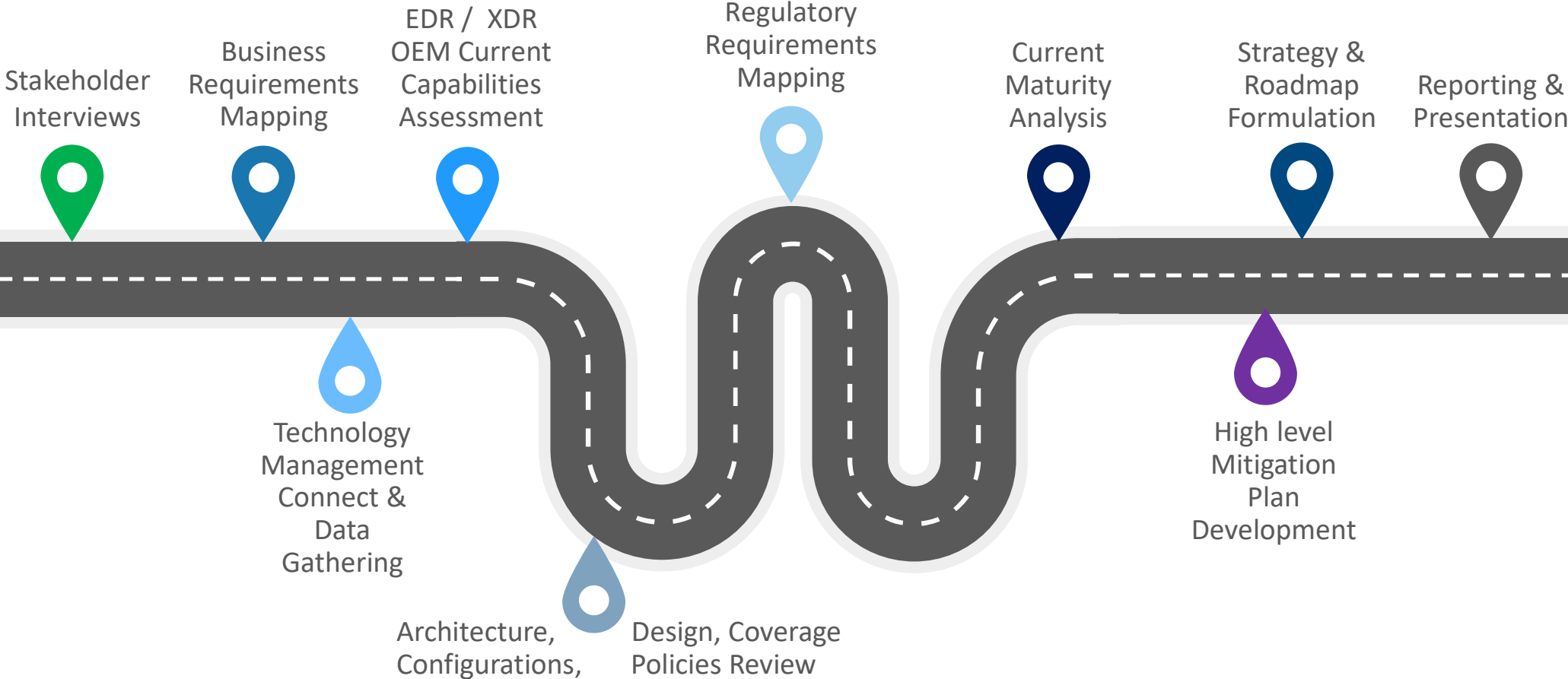


# Objectives & Scope

- Evaluate the customer's current EDR and XDR solutions for endpoint, network, cloud, and hybrid environments
- Identify potential threat detection gaps, response inefficiencies, and integration challenges within the security ecosystem
- Provide recommendations for optimization, automation, and best practices to enhance security posture.

Assessment of Existing EDR & XDR Capabilities	Alignment with Business & Security Objectives	Future Readiness & Security Roadmap
		
<ul style="list-style-type: none"> <li>• <b>Detection and Visibility</b> <ul style="list-style-type: none"> <li>✓ Coverage across the enterprise</li> <li>✓ Technical capabilities across threats</li> </ul> </li> <li>• <b>Response &amp; Automation</b> <ul style="list-style-type: none"> <li>✓ Investigation, automation, response</li> <li>✓ Threat hunting capabilities</li> <li>✓ Remediation effectiveness</li> </ul> </li> <li>• <b>Integration &amp; Operational Maturity</b> <ul style="list-style-type: none"> <li>✓ Platform coverage</li> <li>✓ Ecosystem integration</li> <li>✓ Compliance and reporting</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Risk coverage &amp; threat landscape alignment</b> <ul style="list-style-type: none"> <li>✓ Critical assets and crown jewels protection</li> <li>✓ Industry specific threat mitigation planning</li> </ul> </li> <li>• <b>Regulatory compliance</b> <ul style="list-style-type: none"> <li>✓ Alignment with regulatory frameworks</li> <li>✓ Data residency and privacy obligations</li> </ul> </li> <li>• <b>Costs assessment</b> <ul style="list-style-type: none"> <li>✓ License cost + operational cost vs indirect savings through risk mitigation</li> <li>✓ Over vs under utilization of the EDR/XDR solution</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Scalability &amp; Cloud Readiness</b> <ul style="list-style-type: none"> <li>✓ Scalability readiness across hybrid and multi cloud</li> <li>✓ Support for future cloud workloads</li> </ul> </li> <li>• <b>AI Driven functionality</b> <ul style="list-style-type: none"> <li>✓ Availability and usage of AI driven features</li> </ul> </li> <li>• <b>OEM roadmap and ecosystem strategy</b> <ul style="list-style-type: none"> <li>✓ OEM roadmap vs customer organization IT landscape strategy comparison</li> </ul> </li> </ul>

# Assessment Methodology



# Key Technical Assessment Work Packages

## Endpoint & Workload Threat Detection Capability Assessment

### Scope:

- Evaluate EDR/XDR visibility across endpoints, workloads, and cloud
- Assess technical detection capabilities for malware, exploits, and insider threats
- Measure behavioral analytics, anomaly detection, and threat hunting
- Review remediation effectiveness (containment, rollback, automation)

### Activities:

- ✓ Detection gap analysis across assets
- ✓ False positive/negative tuning recommendations
- ✓ Threat hunting & response maturity assessment
- ✓ Compliance & operational effectiveness review

## XDR Coverage & Data Correlation Effectiveness Assessment

### Scope:

- Assess XDR telemetry ingestion & correlation across security layers
- Identify gaps in threat intelligence enrichment & prioritization
- Review risk-based detection alignment with crown jewels & critical assets
- Evaluate ROI and platform utilization efficiency

### Activities:

- ✓ Telemetry & coverage gap assessment
- ✓ Threat intelligence & correlation effectiveness review
- ✓ Detection alignment with business risk priorities
- ✓ Over/under-utilization analysis of EDR/XDR

## EDR/XDR Platform Integration & Operational Maturity

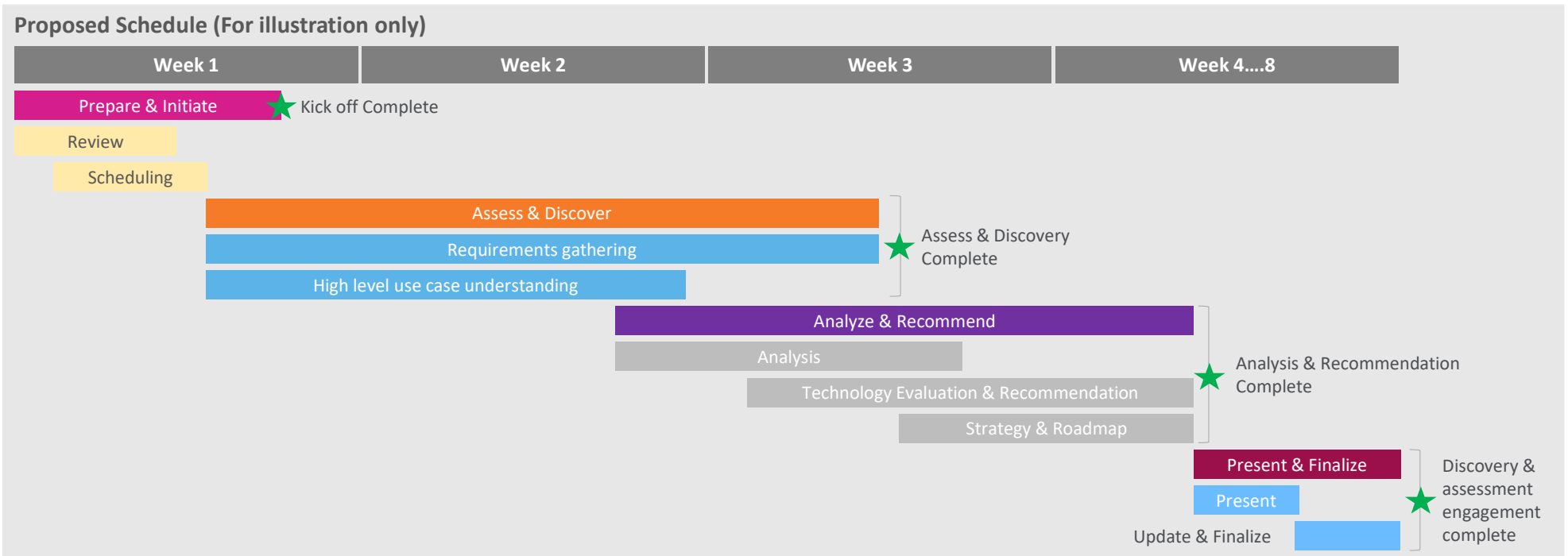
### Scope:

- Assess EDR/XDR integration with SIEM, SOAR, firewall, cloud and other technologies
- Review policy tuning complexity & operational efficiency
- Evaluate compliance readiness & security governance
- Compare OEM roadmap with IT strategy for future viability
- Assess EDR/XDR automated response capabilities & AI-driven analytics
- Evaluate EDR/XDR related playbook efficiency, SOAR integration, and remediation speed
- Identify scalability & future AI-driven automation potential

### Activities:

- ✓ Integration maturity & API efficiency analysis
- ✓ Policy and security posture review
- ✓ Compliance, reporting, and governance review
- ✓ OEM vs. organizational IT strategy alignment
- ✓ Response automation, workflow & playbook assessment
- ✓ AI-driven detection & behavioral analytics review
- ✓ Scalability readiness & automation maturity analysis

# Assessment Plan on a Page



## Deliverables

### Assessment Report:

- A detailed document outlining our findings, gaps, and recommendations.

### Roadmap for Implementation with a plan:

- High-level solution design and implementation plan and methodology.
- High-level plan with effort estimation, cost analysis, target operating model with business impact analysis.
- RAID Log to align on the Risks, Assumptions, Issues, and Dependencies with a mitigation plan.
- RACI Matrix to align with the responsibilities and accountabilities of all stakeholders, including other vendors (if any).



# Leveraging LTIMindtree's EDR-XDR Maturity Framework (Based on NIST CSF)

	Maturity Levels				
Security Control Phase	Level 1: Initial	Level 2: Managed	Level 3: Defined	Level 4: Quantitatively Managed	Level 5: Optimized
Identify	No structured threat identification, limited endpoint visibility	Basic threat identification exists but lacks automation	Threat risks identified and managed using structured processes	Threats proactively identified and continuously monitored	Threat monitoring integrated into business decisions
Protect	Security controls are reactive, inconsistent across environments	Security controls enforced but inconsistently applied	Protection aligned with defined security policies	Security controls actively monitored and adapted to risks. Basic automation applied	Security standards enforced via advanced automation, AI and analytics
Detect	Threats remain undetected until after operational impact	Anomaly detection exists but lacks reliability	Normal activity baselines established for anomaly detection	Continuous monitoring program detects threats in real time	Threat detection adapts based on evolving behaviors
Respond	No defined incident response, manual and inconsistent actions	Incident response roles exist, but actions remain reactive	Incident response includes containment, analysis, and remediation	Incident impact minimized through proactive response strategies	Incident response regularly tested and optimized for new age threats and OEM features
Recover	No formal recovery process, prolonged downtime risks	Recovery processes applied but inconsistent across incidents	Recovery process minimized impact and prevents reinfection	Recovery times monitored, ensuring minimal downtime by incorporating all previous learnings	Recovery processes continuously improved and validated for new age threats



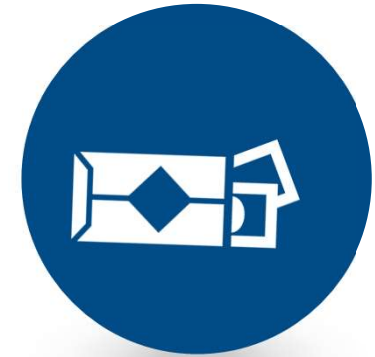
## Pricing Model



Options for fixed-price assessments or hourly consulting rates.



Potential for subscription-based support for ongoing assessments.



Microsoft and LTIM joint collaboration

Contact us for more details.

Let's get to the future, faster, Together

Thank you