LTIMindtree

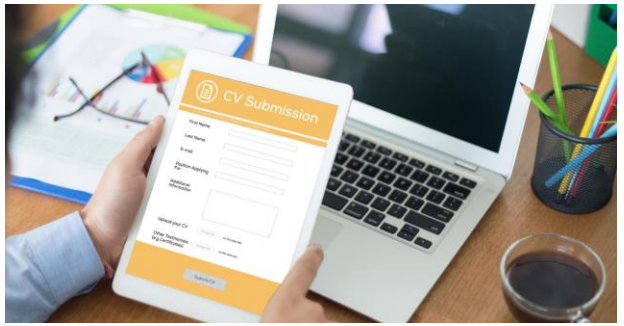
Let’s get to the future, faster. **Together.**

Prepared for: MS Defender for IoT (D4IoT) Assessment as a Service

OT/IoT Security Assessment as a Service

Introduction

Assessment as a Service by LTIMindtree is a comprehensive package aimed at helping organizations conduct risk assessment with efficiently and flexibly. This service allows organizations to evaluate the security posture of their OT environment, identify risks, threats and vulnerabilities, and accordingly plan their OT security transformation roadmap.



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

- Pro-active vulnerability identification
- Enhanced System Resiliency – appropriate controls based on findings
- Help to improve Incident Response
- Regulatory compliance – Helps to meet regulatory requirements & industry standards
- Risk Mitigation – Actionable insights
- Cost Savings – help to prevent potential incidents
- Informed Decision – provides valuable metrics and data, to make decisions on cybersecurity investments & strategies
- Supply chain security – help to enforce stringent cybersecurity practices

Scope of Work

Objective

The objective of an OT Plant Cybersecurity Risk Assessment is to identify and mitigate potential cybersecurity threats and vulnerabilities within operational technology environments.

In Scope

These activities will be carried out **at one site**, having **assets up to 500** nos. (Small Site).

Activities List:

- Understand current security challenges in OT environment
- Review previous risk assessment reports and status
- Study the OT Network Landscape and security measures currently adopted
- Deploy Network Intrusion Detection System (NIDS) to identify threat and vulnerabilities, and communication paths
- Review existing processes and security controls
- Preparation of Assessment report
- Security Awareness sessions to various stakeholders (2 online session of 30 minutes)

Assessment Approach

OT Security assessment is an iterative process while performing certain tasks, with each having a defined goal/milestone. Based on the complexity involved timelines of each activity may vary. The OT Security consultants will work closely with stakeholders and executive activities in 5 phases as per below.

Assessment Kick-off

- Assessment kickoff meeting
- Scope validation
- Stakeholder identification
- Assessment Plan finalization
- Pre-requisites approvals
- Discussion on potential risks

Information gathering

- Document collection & reviews
- Sharing self-assessment questionnaire

Site Visit/ Remote Workshop

- Implementation of NIDS solution
- Validation of network architecture, asset inventory, review of existing controls
- Understand stakeholders' awareness on Cyber Security

Security Analysis

- Identification of gaps in network architecture
- Recording threats & vulnerabilities
- Record current and target security levels
- Document high-level roadmap along with suggested timelines
- Workshop with stakeholders

Submission of report

- Draft report Presentation
- Feedback implementation
- Final submission & Signoff

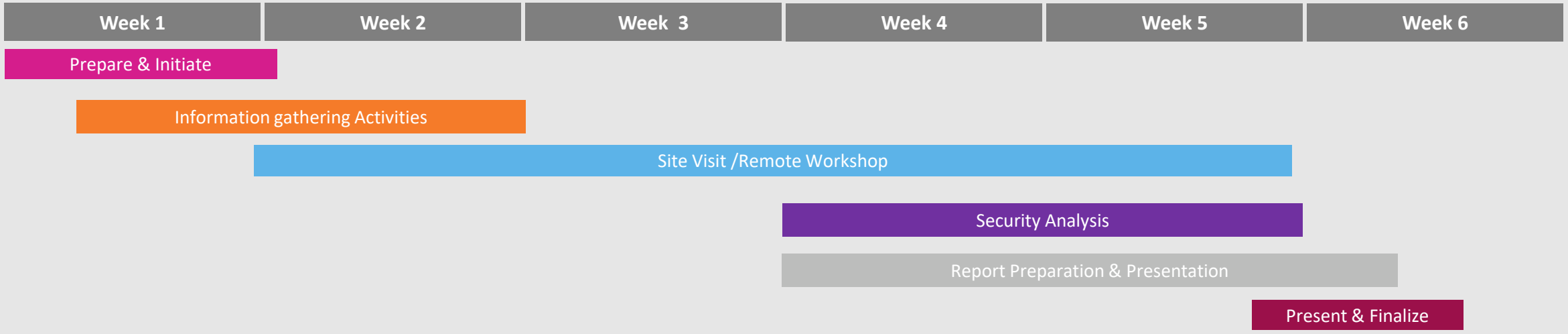
Aassessment Key Activities

Assessment Kickoff	Information Gathering	Site Visit or Remote workshop	Security Analysis	Report Submission

•Assessment kickoff meeting
•Scope validation
•Stakeholder identification
•Assement plan finalization
•Pre-requisites approvals
•Discussion on potential risks
	•OT Policies/Procedures
	•Network Diagram
	•Asset Inventory
	•Process flow details
	•Previous assessment reports
	•Existing control details
	•Documents related to following processes:
	  •Vendor Risk Management
	  •Change and Incident Management
	  •Asset Management
	  •Anti-Virus (AV), Patch Management (PM), Remote Access(RA) Management
	  •Backup & Restoration
		•Self-assessment questionnaire – distribution and gathering their responses. Gathered information will be used to compare actual evidence collected at site.
		• Site Walk through – to understand systems, processes and access controls.
		•OT/ICS Network architecture review
		•Sample configuration audits
		•Meeting with stakeholders & record their pain points and challenges
		•Identification of critical business processes and technologies – to understand how various technologies (AV,PM, RA etc.) & respective risks .
		•Assets information and sample configuration reviews
		•Review of physical and administrative controls
		•Tool based (NIDS) based evidence gathering – create asset inventory, capture network flow, identification of threats & vulnerabilities.
			•Analysis of architectural details i.e. identification of zones & conduits
			•Threats and vulnerabilities
			•Risk Analysis – categorized into High, Medium, and Low
			•Documentation of current maturity level
			•Baselining of current controls
			•Documentation of current state and target state details
			•Documentation of high-level roadmap highlighting indicative timelines for implementing security controls
				•Baselining of current controls
				•Identified threats, vulnerabilities, and risks
				•Need for tools, technologies, and process improvements
				•Prioritized remediation recommendations, and roadmap
				•Present report to client management

Assessment Plan on a Page

Proposed Schedule



Note:

1. Assessment Activities will start once appliance reaches plant/site
2. The customer will assist in hosting the appliance at identified monitoring point
3. It is assumed that the switch identified for network monitoring (SPAN) has visibility to all the assets

Deliverables

Risk Assessment Report:

- Executive Summary
  - Brief on the activities carried out at site
  - Stakeholder involved
  - High level site rating
- OT Asset Inventory – inventory along with classification
- Threat & Vulnerability findings – Risk ratings & asset vulnerabilities report
- Network architecture as identified by automated tool
- Key Observations
- Recommendation & High-level Roadmap
  - Actionable mitigation recommendations
  - Best practices
  - High level roadmap

Pricing Models

Fixed price risk assessment

Fixed price Microsoft defender for IoT solution implantation contract

Microsoft sponsored risk assessment activities

T&M Model for anything that doesn't fit in fixed price model

Contact us for more details.

Let's get to the future, faster, Together

Thank you