Assessment - Power Platform and Dynamics 365 - Security Review

Assessment Program

Duration: 3 Days [Remote | Onsite]
Difficulty Level: 300 - Advanced

Description

A Power Platform and Dynamics 365 Security Assessment is a comprehensive evaluation and training designed to ensure that your Power Platform and Dynamics 365 environment is secure and compliant with industry standards.
This service involved a thorough analysis of your Power Platform tenant, focusing on identifying potential security risks in the configuration and setup of your tenant. During this assessment, a Microsoft Engineer will help to review your tenant's settings and the configuration of one Dynamics or Power Platform environment and App to ensure that they align with recommended best practices. We will focus on identifying potential security risks, data protection vulnerabilities, and compliance issues. The assessment covers aspects such as data access controls, secure data storage practices, and the proper configuration of environment settings. By leveraging best practices and the latest security recommendations, the review aims to fortify your Power Platform solutions against unauthorized access and data breaches, ensuring that your business data remains safe and your operations comply with your organization's security requirements.

Objectives

- Review security requirements
- Identify potential misconfiguration
- Explain configuration options
- Implement best practices
- Advise on Security enhancement strategies
- Deliver final security assessment report and results

Outcomes

- Security gaps identified
- Best practices shared
- Compliance strategies outlined
- Access controls optimized
- Data loss prevention enhanced
- Assessment report presented and explained

Methodology

Assessment
Perform an in-depth evaluation with a Microsoft architect and generate your first set of results.

Review and analysis
Analyze your results and examine the issues identified and how to remediate them.

Develop a plan
Develop a plan to help you remediate issues and improve your environment.

Scope

This document outlines the scope for a comprehensive review of security measures and practices within the Power Platform and Dynamics 365 environment.

- AAD Configuration
- Authentication
- Data Security
- Auditing and Monitoring
- Security Settings
- Integration Security
- Incident Response Plan
- Compliance

Agenda

The agenda for the Power Platform and Dynamics 365 Security Assessment spans three days, focusing on key aspects of security within the Power Platform environment.

- Day 1: Understanding Security Requirements and Access Control
- Day 2: Data Security and Platform Environment Review
- Day 3: Presentation and Closeout

Participants

- Security Architect
- Compliance Officer
- Power Platform Project or Program Owner
- IT Administrator
- Power Platform or Dynamics 365 Developer

Skill Requirements

- Security team should have expertise, understanding and access to Entra ID (AAD)
- Power Platform product or project owner should have a Power Platform or Dynamics 365 Administrator Office 365 security role.

Time Commitment

- 4 hours on Day 1 and Day 2
- 3 hours on Day 3

Microsoft

Delivery Outline

Service	Assessment - Power Platform and Dynamics 365 - Security Review
Participants	• Security Architect • Compliance Officer • Power Platform Project or Program Owner • IT Administrator • Power Platform or Dynamics 365 Developer
Role Requirements	• Security team with expertise, understanding and access to Entra ID (AAD) • Power Platform product or project owner with Power Platform or Dynamics 365 Administrator Office 365 security role.
Time commitment	• 4 hours on Day 1 and Day 2. • 3 hours on Day 3.
Delivery requirement	• Supported version of Windows. • Supported version of Office. • Modern browser, such as Microsoft Edge (or equivalent). • Internet access.
Day One - Understanding Security Requirements and Access Control	• Review Security Requirements • Review of Entra (AAD) Configuration • Authentication and User Access Review
Day Two - Data Security and Platform Environment Review	• Data Security assessment • Power Platform Environment Setting evaluation • Integration Security evaluation • Data collection and analysis
Day Three - Presentation and Closeout	• Close out call and assessment report presentation • Next steps discussion

If you are interested in this engagement for your organization, contact your Microsoft Account Representative.