

Implement Agent 365 to observe, govern, and secure AI apps, Copilot & Agents

MS Course ID: 00970

Course Overview

This advanced course is designed to equip security professionals and architects with the knowledge and skills necessary to implement, secure, and govern AI agents using Microsoft Agent 365. The curriculum focuses on the security architecture, governance frameworks, and operational controls required to manage enterprise-scale AI agent deployments securely. Participants will learn how to leverage the Agent 365 control plane to enforce policies, monitor activities, and mitigate risks associated with autonomous and assisted agents.

Course Details

Duration:	12 hours	Readiness Stage:	Project Ready
Level:	Advanced	Labs:	Yes
Role:	Technical	Solution Area:	Security, AI Business Solutions (ABS), Cloud and AI Platform

Course Syllabus

1. Observe & control agents in real time

180 mins | Lecture

Module 1:

Microsoft Agent 365 as the Control Plane

Module 2:

Observe - real-time control for agents

- Discover and inventory agents across your organization
- Track agent performance, behavior and risk signals
- Visualize agent relationships and ecosystem fit

2. Hands-on Labs

60 mins | Lab

- Environment Setup
- Agent discovery and registry management using Agent 365
- Agent Identity configuration and monitoring in MS Entra

3. Govern and secure agents at Scale

180 mins | Lecture

Module 3:

Govern - guardrails for agents and users

- Navigating the Agent 365 overview page
- Agent Lifecycle Management in Agent 365
- Onboard agents with IT oversight and security policy
- Governing agent identities (Preview) and ownerless agents in Agent 365
- Audit, logging and compliance with Microsoft Purview

Module 4:

Secure - comprehensive agent protection

- Extend Conditional Access and identity controls to agents
- Protect agent interactions with Microsoft Purview
- Defend agents against threats, vulnerabilities and attacks

4. Hands-on Labs

60 mins | Lab

- Configuring Conditional Access for Agent Identities
- Applying Sensitivity Labels and DLP for Copilot in MS Purview

Interactive Simulated Lab Experience

- Threat Hunting for AI agents using MS Defender

5. Extend security across the AI lifecycle

180 mins | Lecture

Module 5:

- Agent data access & sharing risks

Module 6:

- Security Dashboard for AI

Module 7:

- Security Copilot & Microsoft Security Store

Module 8:

- Foundry Control Plane - AI lifecycle governance

6. Hands-on Labs

60 mins | Lab

- Oversharing Assessment and Remediation using DSPM in MS Purview
- Audit, Retention, and Security Copilot in MS Purview