Secure Azure Services and Workloads with Microsoft Defender for Cloud Regulatory Compliance Controls (SC-5002)

Duration: 1 day
Audience: Professionnel TI

Who is this training for?

Mid-level professionals, administrators, and security engineers.

Training objectives

Gain the skills to secure Azure services and workloads with Microsoft Defender for Cloud in real-world scenarios.

Summary

Applied Skills training courses are designed to validate specific skills by being oriented towards real-world scenarios. They offer a targeted alternative to traditional role-based certifications, with a focus on applying technical skills in real-world business situations.

This learning lab walks you through securing Azure services and workloads using Microsoft Cloud Security Benchmark controls in Microsoft Defender for Cloud through the Azure portal.

Course outline

- Filter network traffic with a network security group using the Azure portal.
- Create a Log Analytics workspace for Microsoft Defender for Cloud.
- Set up Microsoft Defender for Cloud.
- Configure and integrate a Log Analytics agent and workspace into Defender for Cloud.
- Configure Azure Key Vault network settings.
- Connect an Azure SQL server using an Azure private endpoint using the Azure portal.

Approach and methodology

Practical and structured approach combining focused theory and guided workshops.

Participants progressively secure Azure services and workloads using Microsoft Defender for Cloud's regulatory compliance controls through real-world exercises inspired by business scenarios, driving immediate application of learnings. They learn how to assess security posture, apply compliance controls, and strengthen the protection of cloud resources.

Led by a Microsoft certified trainer, the training focuses on interactivity and the development of directly transferable technical skills to ensure the security and compliance of Azure environments in a professional context.

Prerequisites

Recommendations

- Basics of cloud security and cybersecurity (threats, access control, compliance)
- Knowledge of Microsoft Azure environments Understanding of regulatory compliance and governance concepts
- Identity security concepts (Microsoft Entra ID) Familiarity with Azure resources (VMs, storage, networks)