Technofocus

Implement multi-cloud security with Microsoft Defender for Cloud and integrated solutions

Course Overview

Duration - 9 Hours | Level - Advanced

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities. Learn how to implement a development security operations (DevSecOps) solution that unifies security management at the code level across multicloud and multiple-pipeline environments. Learn how to enable a cloud security posture management (CSPM) solution that surfaces actions that you can take to prevent breaches and a cloud workload protection platform (CWPP) with specific protections for servers, containers, storage, databases, and other workloads.

Course Modules

Day 1: Improving your security posture with Microsoft Defender for Cloud

Module 1 - Cloud Security Posture Management

Introduction to Zero Trust

Introduction to Microsoft Defender for Cloud

CNAPP strategy

Microsoft Defender Cloud Security Posture Management

Module 2 - Cloud Workload Protection

Cloud security challenges

Microsoft Defender Cloud Workload Protection

Defender for Servers

Defender for Containers

Protect Cloud Databases

Defender for Storage

Microsoft Defender for APIs

Application Infrastructure Protection

Module 3 - Data Security Posture Management

Automatic discovery

DSPM in Defender CSPM

Attack Path Analysis and Scenarios

Cloud Security Explorer

Data sensitivity settings

Interactive Simulated Lab Experience

Enabling Microsoft Defender for Cloud

Enabling Microsoft Defender for SQL

Enabling Microsoft Defender for open-source relational databases

Enabling Microsoft Defender for Storage accounts

Managing VM access and enabling JIT access

Day 2: Protecting cloud workloads with Microsoft Defender for Cloud

Module 4 - Pricing Defender for Cloud (BCB)

Pricing for Cloud Security Posture Management

Module 5 - Policy Management of MDC

Security policies and recommendations

Identifying and analyzing risks across your environment

Overview of Security alerts and incidents

Module 6 - AI Security Posture Management

Landscape and MDC overview

AI security posture

Threat protection for AI

Interactive Simulated Lab Experience

Improving your regulatory compliance

Investigating the health of your resources

Managing security policies

Applying Azure security baselines to machines

Building a query with the cloud security explorer

Assessing, investigating and responding to security alerts

Day 3: Enhancing security with integrated solutions

Module 7 - Integration with Microsoft Sentinel and Data lake

Security alerts and Incidents

Microsoft Sentinel

Integration with Microsoft Sentinel

Module 8 - Defender for DevOps

Managing your DevOps environments

Connecting DevOps environments

Module 9 - External Attack Surface Management

Defender EASM

Discovery

Inventory

Module 10 - Security Copilot in Defender for Cloud

Cloud security challenges

How Security Copilot works

Security Copilot in Defender for Cloud

Module 11 - Defender for Threat Intelligence

Defender TI Capabilities

How Defender TI works

Interactive Simulated Lab Experience

Connecting your Azure DevOps repositories

Creating a Microsoft Defender EASM Azure resource

Discovering your attack surface

Gathering vulnerability intelligence

Using Security Copilot standalone portal to get threat intelligence

Connecting to Microsoft Sentinel to Analyze Security Alerts