Technofocus

Proactive security

Course Overview

Duration - 8 Hours | Level - Intermediate

This course is focused on strengthening security across Azure environments. Designed for technical audiences, it covers Zero Trust principles, Azure security best practices, firewall and network protection, and the security pillar of the Well-Architected Framework. Participants will gain hands-on experience with Microsoft Defender for Cloud, Microsoft Sentinel, and modern security operations strategies to enhance resilience and mitigate risks.

Course Modules

Day 1

Introduction to Proactive Security

Overview of Proactive Security and its importance

Key objectives and expected outcomes of the workshop

Zero Trust Principles

Introduction to Zero Trust security model

Implementing Zero Trust principles in your organization

Azure Landing Zone

Understanding the foundation and architecture design

Security in ALZ

Azure Security

Overview of Azure security features and capabilities

Best practices for securing Azure environments

Firewall and Network Security

Implementing firewall and network security measures

Best practices for protecting network infrastructure

Cloud Adoption Security Assessment

Security Assessment

Regulatory Compliance

Interactive Simulated Lab Experience

Lab 1 - Deploy and configure Azure Firewall using the Azure portal

Lab 2 - Create an application gateway with a Web Application Firewall using the Azure portal

Lab 3 - Enabling Microsoft Defender for Cloud

Lab 4 - Configure network access to a VM by using a network security group

Lab 5 - Managing Network Security Groups

Lab 6 - Filter network traffic with a network security group using the Azure portal

Lab 7 - Log network traffic to and from a virtual machine using the Azure portal

Day 2

Security Pillar in the Well-Architected Framework

Understanding the security pillar and its principles

Implementing best practices for secure architecture

Implementing Microsoft Defender for Cloud

Securing migrations with Defender for Cloud

Implementing Microsoft Sentinel

Setting up and configuring Microsoft Sentinel for security monitoring

Integrating Sentinel with other security tools

Microsoft Security Exposure Management Overview

Understanding security exposure management

Tools and techniques for managing security risks

Business Continuity and Disaster Recovery

Interactive Simulated Lab Experience

Lab 8: Cloud Workload Protection with Microsoft Defender for Cloud

Lab 9: Managing Defender for Cloud security policies

Lab 10: Investigating incidents with Microsoft Sentinel

Lab 11: advanced Threat Protection and response with Microsoft Sentinel

Lab 12 : Security Copilot (Optional)