Mitigating Threats with Microsoft Defender

This Microsoft Defender training helps security analysts protect networks and endpoints against malware and credential theft. Learn threat detection, remediation, and securing IT systems using Microsoft Defender tools. Some Microsoft skills included are Defender for Office 365, Cloud, automation, and investigating endpoint threats, essential for improving organizational security practices.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Describe Threat Protection With Microsoft Defender — 59 min.

Microsoft Defender For Cloud Apps	15
Microsoft Defender for Endpoint	8
Implementing Microsoft Defender for Identity	4
Integrating Microsoft Defender With Endpoint Manager	5
Configuring Endpoint Security	9
Disk Encryption and Firewall Policies	5
Attack Surface Reduction	8

Getting to Know MS 365 Defender

Overview	1
What is Microsoft 365 Defender	8
Microsoft 365 Defender Portal: Introduction	14
Microsoft 365 Defender Portal: Endpoints	9
Microsoft 365 Defender Portal: Email & Collaboration	7
Microsoft 365 Defender Portal: Wrap-Up	10

MS 365 Defender Policies and Rules

Overview	1
MS 365 Defender Policies & Rules: Built-In Rules	10
MS 365 Defender Policies & Rules: Anti-Phishing	11
MS 365 Defender Policies & Rules: Anti-SPAM	9
MS 365 Defender Policies & Rules: Anti-Malware, Safe Attachments & Safe Links	10
MS 365 Defender Policies & Rules: Allow/Block Lists	4
MS 365 Defender Policies & Rules: Additional Rules	9

WEEK 2

154 min.

MS 365 Defender Policies & Rules: Alert and Activity Policies	4

MS Defender for Office 365

Overview	1
Protecting Office 365	6
Teams, Sharepoint and OneDrive Policies	11
Detect, Investigate, Respond and Remediate Threats	18
User Email Submissions	6
DLP Policies and Alerts	12
Sensitivity Labels	9
Insider Risk Policies	6

MS Defender for Endpoint

Overview	1
Into to MS Defender for Endpoint	5
Automated Investigation and Response (AIR)	6
Data Settings and Alert Notifications	6
Attack Surface Reduction Rules	5
Recommend Security Baselines for Devices	15
Custom Detection Alerts	5
Responding to Incidents	11
Recommended Endpoint Configurations	5
Threat Analytics	3

MS Defender for Identity

Overview	1
MS Defender for Endpoint	5
Azure Identity Policies	10

WEEK 3

165 min.

Conditional Access Policies	8
Investigating Azure Identity Events	6
Using Secure Score	5
Tagging Sensitive Accounts	4
Investigating Defender for Identity Events	7

MCACS and MS 365 Defender Portal

Overview	1
Microsoft Defender for Cloud Apps	6
Discovering Cloud Apps	15
Investigating Cloud App Activity	16
Cloud App Policies	6
Cross-Domain Investigations	7
Attack Simulation Training	10

Configuring Defender for Cloud

Overview	1
Microsoft Defender for Cloud	12
Data Retention and Recommendations	10
Data Connectors	7
Connect AWS Cloud Resources	6
Connect GCP Cloud Resources	5
Cloud Alert Rules	10

Managing Defender for Cloud

Overview	1
Intro: Managing Defender for Cloud	1
Automated Responses	18

WEEK 4

33 min.

Types of Alerts	3
Managing Alerts	17
Threat Intelligence	3
Key Vault Alerts	6
Data Privacy	3

Last updated 12.3.2024