Microsoft Certified: Security Operations Analyst Associate (SC-200)

This SC-200 Microsoft Security Operations Analyst certification training covers how to contribute to an enterprise network's overall network safety by mastering Microsoft-specific tools. This Microsoft Security Operations Analyst training prepares you for the SC-200 certifying exam by diving deep into Microsoft's three enterprise security programs: Defender, Defender for Cloud, and Sentinel.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Getting to Know MS 365 Defender — 162 min.

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
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

WEEK 2

164 min.

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
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

WEEK 3

152 min.

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

Getting To Know Microsoft Sentinel

Overview	1
SIEMs and SOARs	11
Microsoft Sentinel Workspaces	11

WEEK 4

153 min.

Setting Up Microsoft Sentinel	6
Microsoft Sentinel Roles	7
Microsoft Sentinel Data Storage	15

Microsoft Sentinel Data Connectors

Overview	1
Data Sources and Prerequisites	15
Configuring Data Connectors Via Policies	5
Syslog and CEF Event Collectors	18
Threat Intelligence Connectors	9
Ingesting Custom Logs	12

Microsoft Sentinel Analytics Rules

Overview	1
Intro to Sentinel Analytics Rules	1
Design and Configure Analytics Rules	9
Activate Microsoft Security Analytics Rules	4
Custom Analytics Rules	5
Connector Provided Queries and Workflow	4
Incident Creation Logic with KQL	14
KQL Exercise	7
Manage and Use Watchlists	18

WEEK 5

Microsoft Sentinel Entities and ASIM

160 min.

Overview	1
Microsoft Sentinel Entities	11
Classify and Analyze Data by Using Entities	12
Advanced SIEM Information Model (ASIM)	11
Query Sentinel Data Using ASIM Parsers	11
Developing Custom ASIM Parsers	5
Managing ASIM Parsers	5

SOAR and Incident Response

Overview	1
Creating Playbooks	8
Automation Rules	6
Defender Playbooks	5
Incidents Within Sentinel	15
Multi-Workspace Incidents	6
User and Entity Behavior Analytics (UEBA)	6

Sentinel Workbooks, Notebooks and Hunting

Overview	1
Sentinel Workbooks	10
Custom Workbooks	10
Security Operations Efficiency Workbook	5
Threat Hunting Queries	6
Hunting With Livestreams	4
Sentinel Bookmarks	5
Hunting With Notebooks	13

WEEK 6

18 min.

Configure and Use MSTICPy in Notebooks	17

Last updated 12.3.2024