Microsoft

Microsoft Security Operations Analyst

Exam Ref SC-200

Yuri Diogenes
Jake Mowrer
Sarah Young

Microsoft

Exam Ref SC-200 Microsoft Security Operations Analyst

Yuri Diogenes
Jake Mowrer
Sarah Young

Exam Ref SC-200 Microsoft Security Operations Analyst

Table of Contents

Cover

Title Page

Copyright Page

Contents at a glance

Contents

Introduction

- Organization of this book
- Preparing for the exam
- Microsoft certification
- Errata, updates & book support
- Stay in touch

Chapter 1 Mitigate threats using Microsoft 365 Defender

- Skill 1-1: Detect, investigate, respond, and remediate threats to the productivity environment using Microsoft Defender for Office 365
  - Examine a malicious spear phishing email
  - Configuring a Safe Links policy
  - Malicious attachments
  - Anti-phishing policies
  - Attack Simulation Training
  - Data protection, labeling, and insider risk
  - Investigate and remediate an alert raised by Microsoft Defender for Office 365
- Skill 1-2: Detect, investigate, respond, and remediate endpoint threats

Table of Contents

using Microsoft Defender for Endpoint

Configuring Microsoft Defender for Endpoint

Respond to incidents and alerts

Creating custom detections

Managing risk through security recommendations and vulnerability management

Skill 1-3: Detect, investigate, respond, and remediate identity threats

Identifying and responding to Azure Active Directory identity risks

Identifying and responding to Active Directory Domain Services threats using Microsoft Defender for Identity

Using Microsoft Cloud App Security to identify and respond to threats in Software as a Service

Skill 1-4: Manage cross-domain investigations in the Microsoft Defender Security portal

Examine a cross-domain incident

Manage a cross-domain incident using Microsoft 365 Defender

Thought experiment

Securing Contoso Corporation from modern threats

Thought experiment answers

Chapter Summary

Chapter 2 Mitigate threats using Azure Defender

Skill 2-1 Design and configure an Azure Defender implementation

Plan and configure Azure Defender settings, including selecting target subscriptions and workspace

Configure Azure Defender roles

Configure data retention policies

Assess and recommend cloud workload protection

Skill 2-2: Plan and implement the use of data connectors for ingestion of data sources in Azure Defender

Identify data sources to be ingested for Azure Defender

Table of Contents

Configure automated onboarding for Azure resources and data collection

Connect on-premises computers

Connect AWS cloud resources

Connect GCP cloud resources

Skill 2-3: Manage Azure Defender alert rules

Validate alert configuration

Set up email notifications

Create and manage alert suppression rules

Skill 2-4 Configure automation and remediation

Configure automated response in Azure Security Center

Design and configure a playbook in Azure Defender

Remediate incidents by using Azure Defender recommendations

Create an automatic response using an Azure Resource Manager template

Skill 2-5: Investigate Azure Defender alerts and incidents

Describe alert types for Azure workloads

Manage security alerts

Manage security incidents

Analyze Azure Defender threat intelligence

Respond to Azure Defender Key Vault alerts

Manage user data discovered during an investigation

Thought experiment

Monitoring security at Tailwind Traders

Thought experiment answers

Chapter Summary

Chapter 3 Mitigate threats using Azure Sentinel

Skill 3-1 Design and configure an Azure Sentinel workspace

Plan an Azure Sentinel workspace

Configure Azure Sentinel roles

Design Azure Sentinel data storage

Table of Contents

Configure Azure Sentinel service security

Skill 3-2: Plan and implement the use of data connectors for the ingestion of data sources into Azure Sentinel

Identify data sources to be ingested into Azure Sentinel

Identify the prerequisites for a data connector

Configure and use Azure Sentinel data connectors

Design and configure Syslog and CEF event collections

Design and configure Windows Events collections

Configure custom threat intelligence connectors

Create custom logs in Azure Log Analytics to store custom data

Custom log ingestion via the Azure Monitor HTTP Data Collector API

Custom log ingestion via Azure Logic Apps

Skill 3-3: Manage Azure Sentinel analytics rules

Design and configure analytics rules

Create custom analytics rules to detect threats

Activate Microsoft security analytics rules

Configure connector-provided scheduled queries

Configure custom scheduled queries

Define incident creation logic

Kusto Query Language (KQL)

Skill 3-4 Configure Security Orchestration, Automation, and Response (SOAR) in Azure Sentinel

Create Azure Sentinel Playbooks

Use Playbooks to remediate threats

Use Playbooks to manage incidents

Use Playbooks across Microsoft Defender solutions

Skill 3-5: Manage Azure Sentinel incidents

Investigate incidents in Azure Sentinel

Triage incidents in Azure Sentinel

Table of Contents

Respond to incidents in Azure Sentinel
Investigate multi-workspace incidents
Identify advanced threats with user and entity behavior analytics (UEBA)
Skill 3-6: Use Azure Sentinel workbooks to analyze and interpret data
Activate and customize Azure Sentinel workbook templates
Create custom workbooks
Configure advanced visualizations
View and analyze Azure Sentinel data using workbooks
Track incident metrics using the security operations efficiency workbook
Skill 3-7: Hunt for threats using the Azure Sentinel portal
Create custom hunting queries
Run hunting queries manually
Monitor hunting queries by using Livestream
Track query results with bookmarks
Use hunting bookmarks for data investigations
Convert a hunting query to an analytics rule
Perform advanced hunting with notebooks
Thought experiment
Security operations at Contoso Ltd
Thought experiment answers
Chapter Summary
Index