

# Exam Ref SC-200 Microsoft Security Operations Analyst, Second Edition

## List of URLs

---

### Chapter 1: Manage a security operations environment

<https://security.microsoft.com>

<https://portal.azure.com>

<https://admin.microsoft.com>

<https://learn.microsoft.com/en-us/defender-endpoint/web-content-filtering>

<https://learn.microsoft.com/en-us/defender-vulnerability-management/defender-vulnerability-management-capabilities>

<https://learn.microsoft.com/en-us/security-exposure-management/prerequisites>

<https://aka.ms/mssentinelmssp>

<https://azure.microsoft.com/pricing/details/microsoft-sentinel/>

<https://docs.microsoft.com/azure/sentinel/roles>

<https://azure.microsoft.com/en-us/pricing/calculator/?service=azure-sentinel>

<https://docs.microsoft.com/en-us/graph/security-concept-overview>

<https://docs.microsoft.com/en-us/azure/sentinel/normalization#installing-a-parser>

<https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-security-events>

<https://learn.microsoft.com/en-us/azure/azure-monitor/logs/logs-ingestion-api-overview>

<https://learn.microsoft.com/en-us/azure/sentinel/unified-connector-cef-device>

<https://learn.microsoft.com/en-us/azure/sentinel/unified-connector-6>

## Chapter 2: Configure protections and detections

<https://security.microsoft.com>

<https://learn.microsoft.com/en-us/defender-office-365/eop-about#features-in-the-default-email-protections-for-cloud-mailboxes>

<https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference>

<https://portal.azure.com>

<https://learn.microsoft.com/en-us/defender-cloud-apps/control-cloud-apps-with-policies>

<https://learn.microsoft.com/en-us/defender-office-365/how-policies-and-protections-are-combined>

<https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-deployment>

<https://youtube.com/watch?v=xoEP7SFEnJc&si=k1fafcP4-FLhqwrn>

<https://learn.microsoft.com/en-us/azure/sentinel/entities-reference>

<https://uncoder.io/>

## Chapter 3: Manage incident response

<https://learn.microsoft.com/en-us/defender-endpoint/live-response-command-examples>

<https://security.microsoft.com/auditlogsearch>

<https://purview.microsoft.com/>

<https://graph.microsoft.com/v1.0/auditLogs/signIns>

<https://portal.azure.com>

<https://security.azure.com>

<https://securitycopilot.microsoft.com>

<https://security.microsoft.com>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference>

<https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk>

<https://learn.microsoft.com/en-us/defender-for-identity/what-is>

<https://learn.microsoft.com/en-us/defender-for-identity/alerts-overview>

<https://learn.microsoft.com/en-us/defender-endpoint/respond-machine-alerts>

<https://learn.microsoft.com/en-us/defender-xdr/investigate-incidents>

<https://docs.microsoft.com/en-us/connectors/connector-reference/connector-reference-logicapps-connectors>

<https://learn.microsoft.com/en-us/purview/dlp-alerts-get-started>

## Chapter 4: Manage security threats

<https://security.microsoft.com>

<https://portal.azure.com>

<https://learn.microsoft.com/en-us/kusto/query/>

<https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-overview#get-access>

<https://attack.mitre.org>

## Chapter 5: SC-200 Microsoft Security Operations Analyst exam updates

<https://learn.microsoft.com/en-us/credentials/certifications/resources/study-guides/sc-200>