

Exam Ref SC-200 Microsoft Security Operations Analyst

List of URLs

Front Matter

<http://www.microsoft.com/learn>

docs.microsoft.com

<http://aka.ms/examlist>

<http://microsoft.com/learn>

<http://aka.ms/practicetests>

MicrosoftPressStore.com/ExamRefSC200/errata

MicrosoftPressStore.com/Support

<http://support.microsoft.com>

<http://twitter.com/MicrosoftPress>

Chapter 1

<https://security.microsoft.com>

<https://security.microsoft.com>

fespiresec.mail.onmicrosoft.com

fespiresec.onmicrosoft.com

bobsmith@fabrikam.com

contoso.com

bobsmith@CONTOSO.com
<https://security.microsoft.com>
<https://compliance.microsoft.com>
<https://portal.azure.com>
<https://portal.atp.azure.com>
<https://portal.cloudappsecurity.com>
<https://docs.microsoft.com/en-us/microsoft-365/security/defender/custom-roles?view=o365-worldwide>
https://aka.ms/sc200_setupsafelinks
https://aka.ms/sc200_SLglobalsettings
https://aka.ms/sc200_setupsafeattach
https://aka.ms/sc200_safeattach4sps
https://aka.ms/sc200_safedocs
https://aka.ms/sc200_antiphishrecommended
https://aka.ms/sc200_antiphishpol
https://aka.ms/sc200_attacksimtraining
https://aka.ms/sc200_sensitivelabels
https://aka.ms/sc200_dlppol
https://aka.ms/sc200_insiderisk
https://aka.ms/sc200_mdoremediate
https://aka.ms/sc200_mdeintegrations
https://aka.ms/sc200_mdeprivacy
https://aka.ms/sc200_mdeconfigwiz
https://aka.ms/sc200_mderbac
https://aka.ms/sc200_mderbacadv
https://aka.ms/sc200_mdenotify
https://aka.ms/sc200_mdeadvfeatures
<https://attack.mitre.org/>
https://aka.ms/sc200_mdealertapi
<https://GitHub.com/microsoft/Microsoft-365-Defender-Hunting-Queries>
https://aka.ms/sc200_m365customdetect

https://aka.ms/sc200_mdeioc
https://aka.ms/sc200_tvm
https://aka.ms/sc200_tvmremedy
https://aka.ms/sc200_tvmexception
https://aka.ms/sc200_idrisks
https://aka.ms/sc200_idpnotify
https://aka.ms/sc200_idppol
https://aka.ms/sc200_setupmdi
https://aka.ms/sc200_mdiplaybook
https://aka.ms/sc200_mdihoney
https://aka.ms/sc200_mdiportal
https://aka.ms/sc200_mcasrbac
https://aka.ms/sc200_mcasalertmgmt
https://aka.ms/sc200_mcasalerttune
https://aka.ms/sc200_ta
https://aka.ms/sc200_m365secoverview

Chapter 2

<http://aka.ms/ascbooklawbp>
http://aka.ms/SC200_CustomRole
<https://azure.microsoft.com/en-us/pricing/details/monitor/>
<http://aka.ms/ascdatabcollection>
<https://attack.mitre.org/versions/v7/>
http://aka.ms/SC200_WFARM
http://aka.ms/sc200_azdefwindows
http://aka.ms/sc200_azdeflinux
<https://aka.ms/azdforaks>
https://aka.ms/sc200_azdefappservice
https://aka.ms/sc200_azdefstorage
https://aka.ms/sc200_azdsqli
<http://aka.ms/AzDefKeyVaultAlerts>

<http://aka.ms/ASCBookAzDefARMAAlerts>
<http://aka.ms/ASCBookAzDefDNSAlerts>
<http://aka.ms/azurerbac>
<https://portal.azure.com>
<http://aka.ms/ascbookaws>
<http://aka.ms/ascbookarc>
<http://aka.ms/ascbookspn>
<https://attack.mitre.org/techniques/T1086/>

Chapter 3

<https://portal.azure.com>
<https://github.com/Azure/Azure-Sentinel>
<https://aka.ms/azsentinelmssp>
<https://azure.microsoft.com/pricing/details/azure-sentinel/>
<https://azure.microsoft.com/pricing/calculator/>
<https://techcommunity.microsoft.com/t5/azure-sentinel/using-azure-data-explorer-for-long-term-retention-of-azure/ba-p/1883947>
<https://docs.microsoft.com/azure/sentinel/roles>
<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/azure-monitor/agents/agent-linux>
<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/gateway>
<https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-security-events>
<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/data-collector-api#concepts>
<https://uncoder.io/>
<https://docs.microsoft.com/en-us/connectors/connector-reference/connector-reference-logicapps-connectors>
<https://github.com/Azure/Azure-Sentinel/tree/master/playbooks>
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/>