SC-200T00 Microsoft Security Operations Analyst

Model 1 Mitigate threats using Microsoft 365 Defender

S.No	Text	URL
1	Instead simply click the link here1 to launch this demonstration	https://aka.ms/M365Defender-InteractiveGuide
2	The Microsoft 365 Defender portal (https://security.microsoft.com/)	https://security.microsoft.com/?azure-portal=true
3	Guided Demonstration - Defender for Office 365. instead simply click the link here3 to launch this demonstration.	https://aka.ms/MSDO-IG
4	Guided Demonstration - Microsoft Defender for Identity	https://aka.ms/MSDefenderforIdentity-IG
5	Guided demonstration - Cloud App Security	https://aka.ms/DetectThreats-ManageAlerts-MCAS_InteractiveGuide
6	In the Microsoft 365 compliance center https://compliance.microsoft.com, go to Data Loss Prevention	https://compliance.microsoft.com?azure-portal=true
7	Microsoft 365 licensing guidance for security & compliance	Microsoft 365 guidance for security & compliance - Service Descriptions | Microsoft Docs
8	Crowd Research Partners, Insider Threat Report	https://crowdresearchpartners.com/portfolio/insider-threat-report/?azure-portal=true
9	Carnegie Mellon CERT study: The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures	https://resources.sei.cmu.edu/asset_files/TechnicalReport/2008_005_001_14981.pdf?azure-portal=true
10	Carnegie Mellon University: Insider Threats in Healthcare	Insider Threats in Healthcare (Part 7 of 9: Insider Threats Across Industry Sectors) (cmu.edu)

11	Turn Office 365 audit log search on or off	https://docs.microsoft.com/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide?azure-portal=true
12	Set up a connector to import HR data	https://docs.microsoft.com/microsoft-365/compliance/import-hr-data?view=o365-worldwide?azure-portal=true
13	Create, test, and tune a DLP policy	https://docs.microsoft.com/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide?azure-portal=true
14	Create an insider risk policy	Get started with insider risk management - Microsoft 365 Compliance | Microsoft Docs
15	Compare Microsoft 365 Enterprise Plans	Compare Microsoft Enterprise Software Plans | Microsoft 365
16	Enable permissions for insider risk management	Get started with insider risk management - Microsoft 365 Compliance | Microsoft Docs
17	Create, test, and tune a DLP policy	Create, test, and tune a DLP policy - Microsoft 365 Compliance | Microsoft Docs
18	Guided demonstration - Insider risk management	Minimize internal risks with insider risk management in Microsoft 365 (cloudguides.com)
19	SC-200 GitHub repository	https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst

Module 2 Mitigate threats using Microsoft Defender for Endpoint

S.No	Text	URL
1	Microsoft 365 Defender portal (https://security.microsoft.com)	https://security.microsoft.com/?azure-portal=true
2	Attack surface reduction rules	Use attack surface reduction rules to prevent malware infection | Microsoft Docs
3	Manage Microsoft Defender for Endpoint alerts	https://docs.microsoft.com/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide
4	Create indicator for files	https://docs.microsoft.com/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide
5	Create indicators for IPs and URLs/ domains	https://docs.microsoft.com/microsoft-365/security/defender-endpoint/indicator-ip-domain?view=o365-worldwide

6	SC-200 GitHub repository	GitHub - MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst

Module 3 Mitigate threats using Azure Defender

S.No	Text	URL
1	Guided Demonstration - Azure Security Center	1https://mslearn.cloudguides.com/guides/Protect%20your%20hybrid%20cloud%20with%20Azure%20Security%20Center
2	Install the Log Analytics agent for Windows	https://docs.microsoft.com/azure/virtual-machines/extensions/oms-windows?azure-portal=true
3	Install the Log Analytics agent for Linux	https://docs.microsoft.com/azure/virtual-machines/extensions/oms-linux?azure-portal=true
4	Collect data about Azure Virtual Machines	https://docs.microsoft.com/azure/azure-monitor/learn/quick-collect-azurevm?azure-portal=true
5	For Windows machines	https://docs.microsoft.com/azure/virtual-machines/extensions/oms-windows?toc=/azure/azure-monitor/toc.json?azure-portal=true
6	For Linux machines	https://docs.microsoft.com/azure/virtual-machines/extensions/oms-linux?toc=/azure/azure-monitor/toc.json?azure-portal=true
7	Security alerts - a reference guide	https://docs.microsoft.com/azure/security-center/alerts-reference?azure-portal=true
8	SC-200 GitHub repository	https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst

Module 4 Create queries for Azure Sentinel using Kusto Query Language

S.No	Text	URL
1	Access the Log Analytics demo environment	https://aka.ms/lademo?azure-portal=true
2	KQL quick reference | Microsoft Docs	https://docs.microsoft.com/azure/data-explorer/kql-quick-reference?azure-portal=true
3	Microsoft Tech Community Security Webinars	https://techcommunity.microsoft.com/t5/microsoft-security-and/security-community-webinars/ba-p/927888?azure-portal=true
4	Become an Azure Sentinel Ninja4	Become a Microsoft Sentinel Ninja: The complete level 400 training - Microsoft Tech Community
5	SC-200 GitHub repository	https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst

Module 5 Configure your Azure Sentinel environment

S.No	Text	URL
1	Azure portal	https://portal.azure.com/?azure-portal=true
2	SC-200 GitHub repository	https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst

Module 6 Connect logs to Azure Sentinel

S.No	Text	URL

1	event set (All, Common, or Minimal)	https://docs.microsoft.com/azure/sentinel/connect-windows-security-events?azure-portal=true
2	SC-200 GitHub repository	https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst

Module 7 Create detections and perform investigations using Azure Sentinel

S.No	Text	URL
1	Advanced multistage attack detection in Azure Sentinel	https://docs.microsoft.com/azure/sentinel/fusion
2	refer to the Query Language	https://docs.microsoft.com/azure/kusto/query/
3	Azure Sentinel documentation	https://docs.microsoft.com/azure/sentinel?azure-portal=true
4	Quickstart: On-board Azure Sentinel	https://docs.microsoft.com/azure/sentinel/quickstart-onboard?azure-portal=true
5	Azure Sentinel pricing	https://azure.microsoft.com/pricing/details/azure-sentinel?azure-portal=true
6	Permissions in Azure Sentinel	https://docs.microsoft.com/azure/sentinel/roles?azure-portal=true
7	Tutorial: Visualize and monitor your data	https://docs.microsoft.com/azure/sentinel/tutorial-monitor-your-data?azure-portal=true
8	Quickstart: Get started with Azure Sentinel	8 https://docs.microsoft.com/azure/sentinel/quickstart-get-visibility?azure-portal=true
9	What is Azure Lighthouse?	https://docs.microsoft.com/azure/lighthouse/overview?azure-portal=true
10	Extend Azure Sentinel across workspaces and tenants	https://docs.microsoft.com/azure/sentinel/extend-sentinel-across-workspaces-tenants#cross-workspace-monitoring?azure-portal=true

11	What is Azure Resource Manager?	https://docs.microsoft.com/azure/azure-resource-manager/management/overview?azure-portal=true
12	Azure Foundation 4-Week Implementation	https://azuremarketplace.microsoft.com/marketplace/consulting-services/servent.servent-azure-foundation?azure-portal=true
13	Tutorial: Detect threats out-of-the-box	https://docs.microsoft.com/azure/sentinel/tutorial-detect-threats-built-in?azure-portal=true
14	Connect data sources	https://docs.microsoft.com/azure/sentinel/connect-data-sources?azure-portal=true
15	Azure Sentinel repository on GitHub	https://github.com/Azure/Azure-Sentinel
16	custom alerts using analytics rules	https://docs.microsoft.com/azure/sentinel/tutorial-detect-threats-custom?azure-portal=true
17	SC-200 GitHub repository	https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst

Module 8 Perform threat hunting in Azure Sentinel

S.No	Text	URL
1	msticpy	https://msticpy.readthedocs.io/?azure-portal=true
2	Azure-Sentinel-Notebooks	Azure-Sentinel-Notebooks/A Getting Started Guide For Azure Sentinel ML Notebooks.ipynb at 8122bca32387d60a8ee9c058ead9d3ab8f4d61e6 · Azure/Azure-Sentinel-Notebooks · GitHub
3	SC-200 GitHub repository3	https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst