## Exam Objectives

The following are the learning objectives for the exam. Inline with each objective are links to Microsoft documentation around the specific concept or service. In addition to the documentation, there are also online courses from Microsoft Learn and the Microsoft Partner virtual training series available for additional learning resources. Access to the exam objectives can be found on Microsoft Learn:  <https://docs.microsoft.com/en-us/learn/certifications/exams/sc-300>

### Objective: Implement an Identity Management Solution (25-30%)

Implement Initial Configuration of Azure Active Directory

* Configure and manage Azure AD directory roles  
  [Understand roles in Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/roles/concept-understand-roles)  
  [Configure and manage Azure Active Directory roles](https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/2-configure-manage-roles)
* Configure and manage custom domains  
  [Add a custom domain name to Azure Active Directory](https://docs.microsoft.com/en-us/learn/modules/add-custom-domain-name-azure-active-directory/)  
  [Configure and manage custom domains](https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/4-configure-manage-custom-domains)
* Configure and manage device registration options  
  [Configure and manage device registration](https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/5-configure-manage-device-registration)
* Configure delegation by using administrative units  
  [Administrative units in Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units)
* Configure tenant-wide settings  
  [Configuration in a tenant](https://docs.microsoft.com/en-us/microsoft-365/education/deploy/intro-azure-active-directory#configuration-in-a-tenant)  
  [Configure tenant-wide setting](https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/7-configure-tenant-wide-options)

### Mitigate Threats Using Microsoft 365 Defender (25-30%)

Detect, Investigate, Respond, and Remediate Threats to the Productivity Environment by Using Microsoft Defender for Office 365

* Detect, investigate, respond, remediate Microsoft Teams, SharePoint, and OneDrive for Business threats
  + [Threat Explorer and Real-time detections](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/threat-explorer?view=o365-worldwide)
  + [Threat investigation and response](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-ti?view=o365-worldwide)
  + [Threat intelligence to protect, detect & respond to threats](https://www.microsoft.com/en-us/itshowcase/microsoft-uses-threat-intelligence-to-protect-detect-and-respond-to-threats)
  + [Remediate malicious email delivered in Office 365](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/remediate-malicious-email-delivered-office-365?view=o365-worldwide)
* Detect, investigate, respond, remediate threats to email by using Defender for Office 365
  + [Threat Explorer and Real-time detections](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/threat-explorer?view=o365-worldwide)
  + [Automated investigation & response in Defender for Office 365](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/automated-investigation-response-office?view=o365-worldwide)
  + [AIR in Microsoft Defender for Office 365](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-air?view=o365-worldwide)
  + [Remediation actions in Microsoft Defender for Office 365](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/air-remediation-actions?view=o365-worldwide)
* Manage data loss prevention policy alerts
  + [Review and manage Microsoft DLP alerts](https://techcommunity.microsoft.com/t5/microsoft-security-and/introducing-an-exciting-new-way-to-review-and-manage-microsoft/ba-p/1807990)
  + [Configure and view alerts for DLP policies](https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide)
* Assess and recommend sensitivity labels
  + [Use sensitivity labels to prioritize incident response](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-investigation)
* Assess and recommend insider risk policies
  + [Insider risk management policies](https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-policies?view=o365-worldwide)

Detect, Investigate, Respond, and Remediate Endpoint Threats by Using Microsoft Defender for Endpoint

* Manage data retention, alert notification, and advanced features
* Data Retention
  + [What is Microsoft’s data retention policy?](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/data-storage-privacy#how-long-will-microsoft-store-my-data-what-is-microsofts-data-retention-policy)
  + [Update data retention settings for Endpoint](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/data-retention-settings#update-data-retention-settings)
* Alert notifications
  + [Configure alert notifications](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/configure-email-notifications)
  + [Manage Microsoft Defender for Endpoint alerts](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts)
* Advanced features
  + [Configure advanced features in Defender for Endpoint](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-features)
* Configure device attack surface reduction rules
  + [Enable attack surface reduction rules](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-attack-surface-reduction)
  + [Use attack surface reduction rules to prevent malware infection](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction)
* Configure and manage custom detections and alerts
  + [Custom detections overview](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/overview-custom-detections)
  + [Create custom detection rules](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules)
  + [Review alerts in Microsoft Defender for Endpoint](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/review-alerts)
* Respond to incidents and alerts
  + [Take response actions on a device](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/respond-machine-alerts)
* Manage automated investigations and remediations
  + [Overview of automated investigations](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/automated-investigations)
  + [Configure automated investigation & remediation capabilities](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/configure-automated-investigations-remediation)
* Assess and recommend endpoint configurations to reduce and remediate vulnerabilities by using Microsoft’s Threat and Vulnerability Management solution
  + [Microsoft’s Threat & Vulnerability Management](https://www.microsoft.com/security/blog/2019/07/02/microsofts-threat-vulnerability-management-now-helps-thousands-of-customers-to-discover-prioritize-and-remediate-vulnerabilities-in-real-time/)
  + [Threat and vulnerability management](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/next-gen-threat-and-vuln-mgt)
  + [Remediate vulnerabilities with threat & vulnerability management](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/tvm-remediation)
* Manage Microsoft Defender for Endpoint threat indicators
  + [Manage indicators](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/indicator-manage)
* Analyze Microsoft Defender for Endpoint threat analytics
  + [Understand the analyst report in threat analytics](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/threat-analytics-analyst-reports)

Detect, Investigate, Respond, and Remediate Identity Threats

* Identify and remediate security risks related to sign-in risk policies
  + [Unblocking based on sign-in risk](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock#unblocking-based-on-sign-in-risk)
* Identify and remediate security risks related to Conditional Access events
  + [Configure Conditional Access in Microsoft Defender](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/configure-conditional-access)
* Identify and remediate security risks related to Azure Active Directory
  + [Remediate risks in Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock)
  + [Remediate users flagged for risk in Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-remediate-users-flagged-for-risk)
* Identify and remediate security risks using Secure Score
  + [Remediate recommendations in Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/security-center-remediate-recommendations)
* Identify, investigate, and remediate security risks related to privileged identities
  + [Lower exposure of privileged accounts](https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices#lower-exposure-of-privileged-accounts)
* Configure detection alerts in Azure AD Identity Protection
  + [Detect risks with Azure AD Identity Protection policies](https://docs.microsoft.com/en-us/learn/modules/protect-identities-with-aad-idp/3-detect-risks-with-policies)
  + [Azure Active Directory Identity Protection notifications](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-notifications)
* Identify and remediate security risks related to Active Directory Domain Services using Microsoft Defender for Identity
  + [Investigate a domain](https://docs.microsoft.com/en-us/learn/modules/perform-evidence-entities-investigations-microsoft-defender-for-endpoint/5-investigate-domain)
  + [Microsoft Defender for Identity FAQs](https://docs.microsoft.com/en-us/defender-for-identity/technical-faq)
* Identify, investigate, and remediate security risks by using Microsoft Cloud Application Security (MCAS)
  + [Investigate cloud app risks & suspicious activity](https://docs.microsoft.com/en-us/cloud-app-security/investigate)
* Configure MCAS to generate alerts and reports to detect threats
  + [Manage alerts](https://docs.microsoft.com/en-us/cloud-app-security/managing-alerts)
  + [Generate data management reports](https://docs.microsoft.com/en-us/cloud-app-security/built-in-reports)

Manage Cross-domain Investigations in Microsoft 365 Defender Portal

* Manage incidents across Microsoft 365 Defender products
  + [Manage incidents in Microsoft 365 Defender](https://docs.microsoft.com/en-us/microsoft-365/security/mtp/manage-incidents?view=o365-worldwide)
* Manage actions pending approval across products
  + [The Action center](https://docs.microsoft.com/en-us/microsoft-365/security/mtp/mtp-action-center?view=o365-worldwide)
  + [View and manage actions in the Action center](https://docs.microsoft.com/en-us/microsoft-365/security/mtp/mtp-autoir-actions?view=o365-worldwide)
* Perform advanced threat hunting
  + [Hunt threats with advanced hunting in Microsoft 365 Defender](https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-overview?view=o365-worldwide)
  + [Proactively hunt for threats with advanced hunting](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-hunting-overview)

### Mitigate Threats Using Azure Defender (25-30%)

Design and Configure an Azure Defender Implementation

* Plan and configure an Azure Defender workspace
  + [Enable Azure Defender](https://docs.microsoft.com/en-us/azure/security-center/enable-azure-defender)
* Configure Azure Defender roles
  + [Create & manage roles for role-based access control](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/user-roles?view=o365-worldwide)
  + [Manage portal access using RBAC](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide)
* Configure data retention policies
  + [Microsoft’s data retention policy](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/data-storage-privacy?view=o365-worldwide#how-long-will-microsoft-store-my-data-what-is-microsofts-data-retention-policy)
* Assess and recommend cloud workload protection
  + [Introduction to Azure Defender](https://docs.microsoft.com/en-us/azure/security-center/azure-defender)
  + [Cloud Workload Security](https://cloudsecurityalliance.org/blog/2021/01/07/cloud-workload-security-part-3-explaining-azure-s-security-features/)

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
  + [Categorize Microsoft alerts across data sources](https://techcommunity.microsoft.com/t5/azure-sentinel/categorizing-microsoft-alerts-across-data-sources-in-azure/ba-p/1503367)
* Configure Automated Onboarding for Azure resources
  + [Automate onboarding](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/azure-server-management/onboarding-automation)
  + [Automate onboarding of Azure Security Center](https://docs.microsoft.com/th-th/azure/security-center/security-center-powershell-onboarding)
* Connect non-Azure machine onboarding
  + [Connect non-Azure machines](https://docs.microsoft.com/en-us/learn/modules/connect-non-azure-machines-to-azure-defender/3-connect-non-azure-machines)
* Connect AWS cloud resources
  + [Connect your AWS accounts](https://docs.microsoft.com/en-us/learn/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts)
  + [Connect your AWS accounts to Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-aws)
* Connect GCP cloud resources
  + [Connect your GCP accounts](https://docs.microsoft.com/en-us/learn/modules/connect-non-azure-machines-to-azure-defender/5-connect-gcp-accounts)
  + [Connect your GCP accounts to Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp)
* Configure data collection
  + [Enable data collection](https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection)

Manage Azure Defender Alert Rules

* Validate alert configuration
  + [Validating Azure Defender for DNS alerts](https://techcommunity.microsoft.com/t5/azure-security-center/validating-azure-defender-for-dns-alerts/ba-p/2227845)
  + [Alert validation in Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation)
* Setup email notifications
  + [Configure email notifications for security alerts](https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details)
* Create and manage alert suppression rules
  + [Suppress alerts from Azure Defender](https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules)
  + [Manage suppression rules](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-suppression-rules?view=o365-worldwide)

Configure Automation and Remediation

* Configure automated responses in Azure Security Center
  + [Automate responses to Security Center triggers](https://docs.microsoft.com/en-us/azure/security-center/workflow-automation)
* Design and configure playbook in Azure Defender
  + [Reconnaissance playbook](https://docs.microsoft.com/en-us/defender-for-identity/playbook-reconnaissance)
* Remediate incidents by using Azure Defender recommendations
  + [Remediate recommendations in Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/security-center-remediate-recommendations)
* Create an automatic response using an Azure Resource Manager template
  + [Create an automatic response using an ARM template](https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert)

Investigate Azure Defender Alerts and Incidents

* Describe alert types for Azure workloads
  + [Security alerts – a reference guide](https://docs.microsoft.com/en-us/azure/security-center/alerts-reference)
* Manage security alerts
  + [What are security alerts?](https://docs.microsoft.com/en-us/azure/security-center/security-center-alerts-overview#what-are-security-alerts-and-security-incidents)
* Manage security incidents
  + [Incidents in Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/security-center-alerts-overview#cloud-smart-alert-correlation-in-azure-security-center-incidents)
* Analyze Azure Defender threat intelligence
  + [Threat intelligence](https://docs.microsoft.com/en-us/azure/security/fundamentals/threat-detection#threat-intelligence)
  + [Azure Defender powered by Microsoft threat intelligence](https://azure.microsoft.com/en-us/blog/azure-defender-for-storage-powered-by-microsoft-threat-intelligence/)
* Respond to Azure Defender for Key Vault alerts
  + [Respond to Azure Defender for Key Vault alerts](https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage)
* Manage user data discovered during an investigation
  + [How does Azure Security Center helps analyze attacks using Investigation?](https://azure.microsoft.com/en-in/blog/how-azure-security-center-helps-analyze-attacks-using-investigation-and-log-search/)

### Mitigate Threats Using Azure Sentinel (40-45%)

Design and Configure an Azure Sentinel Workspace

* Plan an Azure Sentinel workspace
  + [Plan for the Azure Sentinel workspace](https://docs.microsoft.com/en-us/learn/modules/create-manage-azure-sentinel-workspaces/2-plan-for-azure-sentinel-workspace)
* Configure Azure Sentinel roles
  + [Permissions in Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/roles)
* Design Azure Sentinel data storage
  + [Move Azure Sentinel logs to long-term storage](https://techcommunity.microsoft.com/t5/azure-sentinel/move-your-azure-sentinel-logs-to-long-term-storage-with-ease/ba-p/1407153)
  + [Use Azure Data Explorer for retention of Azure Sentinel logs](https://techcommunity.microsoft.com/t5/azure-sentinel/using-azure-data-explorer-for-long-term-retention-of-azure/ba-p/1883947)
* Configure Azure Sentinel service security
  + [Azure security baseline for Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/security-baseline)

Plan and Implement the Use of Data Connectors for Ingestion of Data Sources in Azure Sentinel

* Identify data sources to be ingested for Azure Sentinel
  + [Connect data sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources)
* Identify the prerequisites for a data connector
  + [On-board Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard)
* Configure and use Azure Sentinel data connectors
  + [Connect data to Azure Sentinel using data connectors](https://docs.microsoft.com/en-us/learn/modules/connect-data-to-azure-sentinel-with-data-connectors/)
* Design Syslog and CEF collections
  + [Collect data from Linux-based sources using Syslog](https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog)
  + [Connect your external solution using Common Event Format](https://docs.microsoft.com/en-us/azure/sentinel/connect-common-event-format)
  + [Best Practices for CEF collection in Azure Sentinel](https://techcommunity.microsoft.com/t5/azure-sentinel/best-practices-for-common-event-format-cef-collection-in-azure/ba-p/969990)
* Design and Configure Windows Events collections
  + [Connect Windows security events](https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-security-events)
* Configure custom threat intelligence connectors
  + [Connect data from threat intelligence providers](https://docs.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence)
* Create custom logs in Azure Log Analytics to store custom data
  + [Collect custom logs with Log Analytics agent](https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-custom-logs)

Manage Azure Sentinel Analytics Rules

* Design and configure analytics rules
  + [Define rule query logic & configure settings](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#define-the-rule-query-logic-and-configure-settings)
* Create custom analytics rules to detect threats
  + [Create a custom analytics rule with a scheduled query](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#create-a-custom-analytics-rule-with-a-scheduled-query)
* Activate Microsoft security analytical rules
  + [Using Microsoft Security incident creation analytics rules](https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts#using-microsoft-security-incident-creation-analytics-rules)
* Configure connector provided scheduled queries
  + [Azure Sentinel: The connectors grand](https://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-the-connectors-grand-cef-syslog-direct-agent/ba-p/803891)
  + [Operationalize Azure Sentinel: From log ingestion to incident detection](https://www.bridewellconsulting.com/operationalising-azure-sentinel-from-log-ingestion-to-incident-detection)
* Configure custom scheduled queries
  + [Create a custom analytics rule with a scheduled query](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#create-a-custom-analytics-rule-with-a-scheduled-query)
* Define incident creation logic
  + [Configure the incident creation settings](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#configure-the-incident-creation-settings)

Configure Security Orchestration Automation and Remediation (SOAR) in Azure Sentinel

* Create Azure Sentinel playbooks
  + [Use playbooks with automation rules in Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook)
* Configure rules and incidents to trigger playbooks
  + [Choose the trigger](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#choose-the-trigger)
  + [Automate threat response with playbooks in Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks)
* Use playbooks to remediate threats
  + [Use playbooks with automation rules in Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook)
* Use playbooks to manage incidents
  + [Configure security playbook in Azure Sentinel](https://www.youtube.com/watch?v=6Hha2UPRtI0)
* Use playbooks across Microsoft Defender solutions
  + [Security automation & orchestration](https://docs.microsoft.com/en-us/azure/sentinel/overview#security-automation--orchestration)
  + [Azure Sentinel Microsoft Defender ATP](https://medium.com/@antonio.formato/azure-sentinel-microsoft-defender-atp-automatic-advanced-hunting-56e6e0944d18)

Manage Azure Sentinel Incidents

* Investigate incidents in Azure Sentinel
  + [Investigate incidents with Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases)
* Triage incidents in Azure Sentinel
  + [Triage security alerts](https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-incident#triage-security-alerts)
* Respond to incidents in Azure Sentinel
  + [Respond to a security alert](https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-incident#respond-to-a-security-alert)
* Investigate multi-workspace incidents
  + [Work with incidents in many workspaces at once](https://docs.microsoft.com/bs-cyrl-ba/azure/sentinel/multiple-workspace-view)
  + [Cross workspace Hunting is now available](https://techcommunity.microsoft.com/t5/azure-sentinel/what-s-new-cross-workspace-hunting-is-now-available/ba-p/1519195)
* Identify advanced threats with User and Entity Behavior Analytics (UEBA)
  + [Identify advanced threats with UEBA in Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics)

Use Azure Sentinel Workbooks to Analyze and Interpret Data

* Activate and customize Azure Sentinel workbook templates
  + [Workbooks vs. workbook templates](https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview#workbooks-versus-workbook-templates)
  + [ARM template for deploying a workbook template](https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-automate#azure-resource-manager-template-for-deploying-a-workbook-template)
* Create custom workbooks
  + [Create new workbooks](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility#create-new-workbooks)
* Configure advanced visualizations
  + [Query and visualize data with Azure Sentinel Workbooks](https://docs.microsoft.com/en-us/learn/modules/query-data-sentinel/2-exercise-setup)
* View and analyze Azure Sentinel data using workbooks
  + [Visualize and monitor your data](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data)
  + [Visualize data in Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility#get-visualization)
* Track incident metrics using the security operations efficiency workbook
  + [Manage your SOC better with incident metrics](https://docs.microsoft.com/en-us/azure/sentinel/manage-soc-with-incident-metrics)

Hunt for Threats Using the Azure Sentinel Portal

* Create custom hunting queries
  + [Create custom queries to refine threat hunting](https://docs.microsoft.com/en-us/learn/modules/hunt-threats-sentinel/3-query-management-creation#create-custom-queries-to-refine-threat-hunting)
  + [Creating custom Azure Sentinel Hunting queries](https://blog.sec-labs.com/2019/03/creating-custom-azure-sentinel-hunting-queries/)
* Run hunting queries manually
  + [Hunt for threats by using Azure Sentinel](https://docs.microsoft.com/en-us/learn/modules/hunt-threats-sentinel/6-exercise-hunt-for-threats)
* Monitor hunting queries by using Livestream
  + [Manage hunting and Livestream queries in Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/hunting-with-rest-api)
* Perform advanced hunting with notebooks
  + [Use Jupyter Notebook to hunt for security threats](https://docs.microsoft.com/en-us/azure/sentinel/notebooks)
  + [Hunt for threats using notebooks in Azure Sentinel](https://docs.microsoft.com/en-us/learn/modules/perform-threat-hunting-sentinel-with-notebooks/)
* Track query results with bookmarks
  + [Track query results](https://docs.microsoft.com/en-us/azure/sentinel/bookmarks#add-a-bookmark)
* Use hunting bookmarks for data investigations
  + [Explore bookmarks in the investigation graph](https://docs.microsoft.com/en-us/azure/sentinel/bookmarks#exploring-bookmarks-in-the-investigation-graph)
* Convert a hunting query to an analytical rule
  + [Turning Hunting queries into Analytics Rules](https://azurecloudai.blog/2021/01/04/evolving-the-soc-with-azure-sentinel-hunting-queries/)
  + [Threat hunting vs Analytics rule](https://techcommunity.microsoft.com/t5/azure-sentinel/threat-hunting-vs-analytics-rule/m-p/1217252)