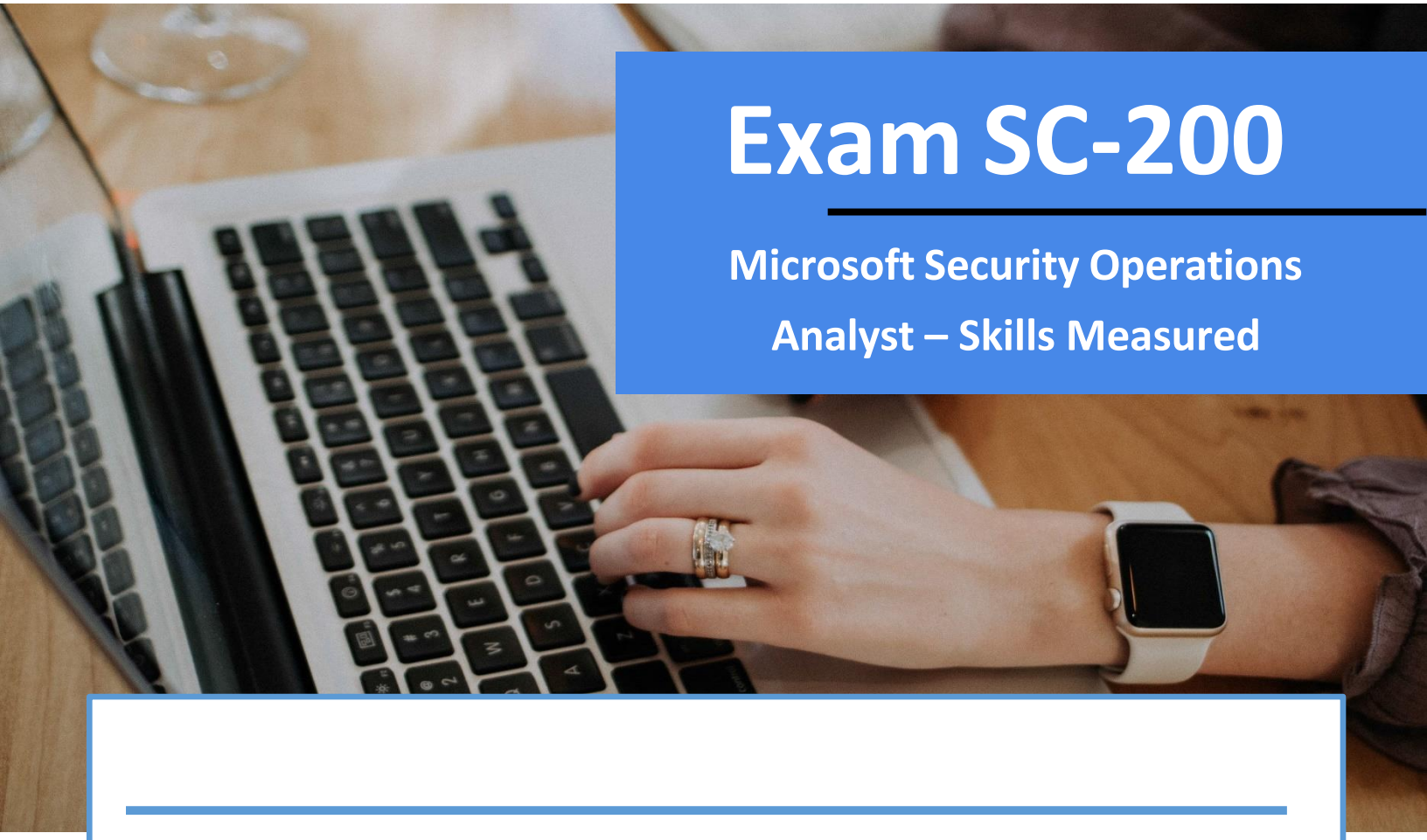
THE QUILL CONSULTANCY



Exam SC-200

Microsoft Security Operations Analyst – Skills Measured

Address
Level 1, 42 Murray Street, Hobart,
Tasmania 7000 Australia

Phone
03 6234 3883

Email
quill@quill.com.au

Web
www.quill.com.au

Audience Profile

The Microsoft security operations analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders.

Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender, and third-party security products. Since the security operations analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

You may be eligible for ACE college credit if you pass this certification exam. See ACE college credit for certification exams for details.

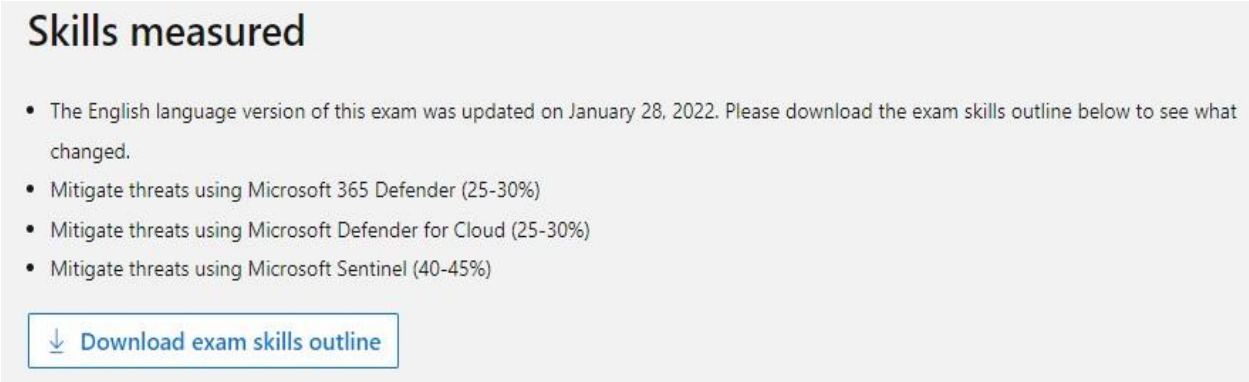
Contents

Contents

How to use this guide

This guide is here to help you prepare and take the exam. It is designed to complement your existing learning and to help guide you in the areas of focus for the exam. You should use this as a framework to help fill in the blanks on information that you have.

We have developed the following content in direct alignment to the current Learning objectives. These can be viewed directly, by selecting the "Download exam skills outline" from the exam page at: https://docs.microsoft.com/en-us/learn/certifications/exams/sc-200



There are loads of exciting and interesting topics we can begin to follow on from these core objectives, but remember for the exam we do need to stay focused and constrain ourselves to these key topics.

In the exam

The exam itself is quite straight forward with no complicated case studies or longwinded questions. The majority of the questions will be "Multiple Choice" or "Choose all that apply" type of questions. You may also come across some "Drag and Drop" questions where you need to place answers in order. The key thing to note is that all of the questions will have the answer in front of you.

Remembering that all of the answers are presented to you, you need to make sure that you answer each question. There is no loss of marks for incorrect answers, so even if you don't know the answer, you should attempt it.

The exam itself will have between 40 and 50 questions, depending on the pool of questions that have been allocated. You will have 60 minutes to complete the exam. As you can see you will need to move at a steady pace throughout. Don't get too stuck on any question, instead select your answer and then mark the question for "Review". Then if you have time at the end of the exam you can go back and review these questions.

Key Learning Objectives

Mitigate threats using Microsoft 365 Defender (25-30%)

Analyze threat data across domains and rapidly remediate threats with built-in orchestration and automation in Microsoft 365 Defender. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

You can access the Microsoft Learn materials online content here:
https://docs.microsoft.com/en-us/learn/paths/sc-200-mitigate-threats-using-microsoft-365-defender/

Detect, investigate, respond, and remediate threats to the productivity environment by using Microsoft Defender for Office 365

Detect, investigate, respond, and remediate threats to Microsoft Teams, SharePoint, and OneDrive

Remediation actions

Threat protection features in Microsoft Defender for Office 365 include certain remediation actions. Such remediation actions can include:

- Soft delete email messages or clusters
- Block URL (time-of-click)
- Turn off external mail forwarding
- Turn off delegation

Threats and remediation actions

Microsoft Defender for Office 365 includes remediation actions to address various threats. Automated investigations often result in one or more remediation actions to review and approve. In some cases, an automated investigation does not result in a specific remediation action. To further investigate and take appropriate actions, use the guidance in the following table.

Category	Threat/risk	Remediation action(s)
Email	Malware	Soft delete email/cluster If more than a handful of email messages in a cluster contain malware, the cluster
Email	Malicious URL (A malicious URL was detected by Safe Links.)	Soft delete email/cluster Block URL (time-of-click verification) Email that contains a malicious URL is considered to be malicious.
Email	Phish	Soft delete email/cluster If more than a handful of email messages in a cluster contain phishing attempts, the whole cluster is considered a phishing

Email	Zapped phish (Email messages were delivered and then zapped.)	Soft delete email/cluster Reports are available to view zapped messages.
Email	Missed phish email reported by a user	Automated investigation triggered by the user's report
Email	Volume anomaly (Recent email quantities exceed the previous 7-10 days for matching criteria.)	Automated investigation does not result in a specific pending action. Volume anomaly is not a clear threat, but is merely an indication of larger email volumes in recent days compared to the last 7-10 days. Although a high volume of email can indicate potential issues, confirmation is needed in terms of either malicious verdicts or a manual review of email messages/clusters.
Email	No threats found (The system did not find any threats based on files, URLs, or analysis of email cluster verdicts.)	Automated investigation does not result in a specific pending action. Threats found and zapped after an investigation is complete are not reflected in an investigation's numerical findings, but such threats are viewable in Threat Explorer.
User	A user clicked a malicious URL (A user navigated to a page that was later found to be malicious, or a user bypassed a Safe Links warning page to get to a malicious page.)	Automated investigation does not result in a specific pending action. Block URL (time-of-click) Use Threat Explorer to view data about URLs and click verdicts. If your organization is using Microsoft Defender for Endpoint, consider investigating the user to

User	A user is sending malware/phish	Automated investigation does not result in a specific pending action. The user might be reporting malware/phish, or someone could be spoofing the user as part of an attack. Use Threat Explorer to view and handle email containing malware or phish.
User	Email forwarding (Mailbox forwarding rules are configured, chch could be used for data exfiltration.)	Remove forwarding rule Use mail flow insights, including the Autofowarded messages report, to view more specific details about forwarded email.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/air-remediation-actions?view=o365-worldwide

Safe Attachments in Microsoft Defender for Office 365

Safe Attachments in Microsoft Defender for Office 365 provides an additional layer of protection for email attachments that have already been scanned by anti-malware protection in Exchange Online Protection (EOP). Specifically, Safe Attachments uses a virtual environment to check attachments in email messages before they're delivered to recipients (a process known as *detonation*).

Safe Attachments protection for email messages is controlled by Safe Attachments policies. Although there's no default Safe Attachments policy, the **Built-in protection** preset security policy provides Safe Attachments protection to all recipients (users who aren't defined in custom Safe Attachments policies). For more information, see Preset security policies in EOP and Microsoft Defender for Office 365. You can also create Safe Attachments policies that apply to specific users, group, or domains. For instructions, see Set up Safe Attachments policies in Microsoft Defender for Office 365.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

Detect, investigate, respond, remediate threats to email by using Defender for Office 365

Microsoft Defender for Office 365 includes powerful automated investigation and response (AIR) capabilities that can save your security operations team time and effort. As alerts are triggered, it's up to your security operations team to review, prioritize, and respond to those alerts. Keeping up with the volume of incoming alerts can be overwhelming. Automating some of those tasks can help.

AIR enables your security operations team to operate more efficiently and effectively. AIR capabilities include automated investigation processes in response to well-known threats that exist today. Appropriate remediation actions await approval, enabling your security operations team to respond effectively to detected threats. With AIR, your security operations team can focus on higher-priority tasks without losing sight of important alerts that are triggered.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-air?view=o365-worldwide

Manage data loss prevention policy alerts

Data loss prevention (DLP) policies can take protective actions to prevent unintentional sharing of sensitive items. When an action is taken on a sensitive item, you can be notified by configuring alerts for DLP. This article shows you how to define rich alert policies that are linked to your data loss prevention (DLP) policies. You'll see how to use the DLP alert management dashboard in the Microsoft 365 compliance center to view alerts, events, and associated metadata for DLP policy violations.

Licensing for alert configuration options

Single-event alert configuration: Organizations that have an E1, F1, or G1 subscription or an E3 or G3 subscription can create alert policies only where an alert is triggered every time an activity occurs.

Aggregated alert configuration: To configure aggregate alert policies based on a threshold, you must one of these licensing configurations:

- An E5 or G5 subscription
- An E1, F1, or G1 subscription or an E3 or G3 subscription that includes one of the following features:
- Office 365 Advanced Threat Protection Plan 2
- Microsoft 365 E5 Compliance
- Microsoft 365 eDiscovery and Audit add-on license

Roles
If you want to view the DLP alert management dashboard or to edit the alert configuration options in a DLP policy, you must be a member of one of these role groups:

- Compliance Administrator
- Compliance Data Administrator
- Security Administrator
- Security Operator
- Security Reader

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-alerts-dashboard-get-started?view=o365-worldwide?WT.mc_id=ES-MVP-4039827

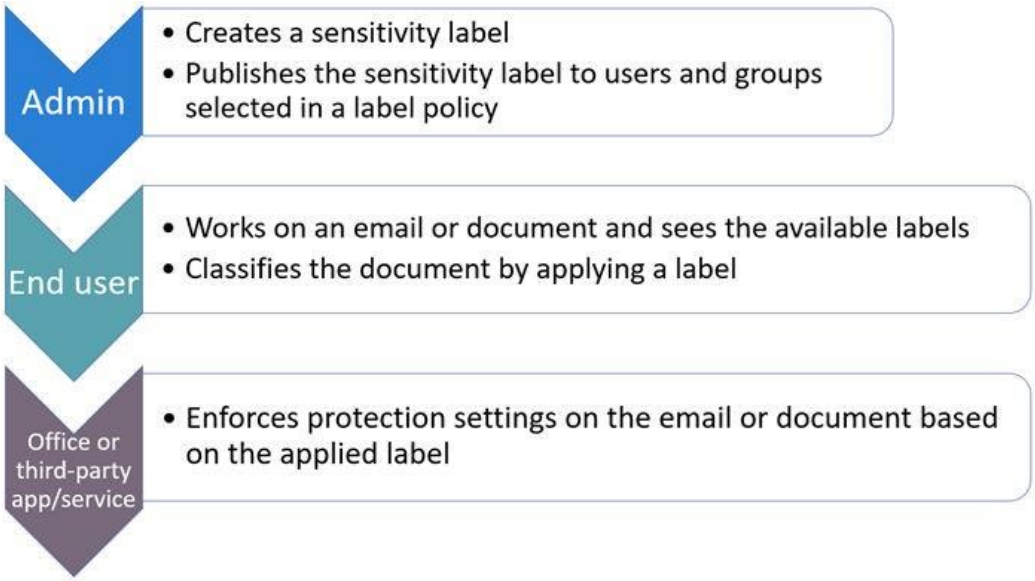
Assess and recommend sensitivity labels

Sensitivity labels from the Microsoft Information Protection solution let you classify and protect your organization's data, while making sure that user productivity and their ability to collaborate isn't hindered.

When you're ready to start protecting your organization's data by using sensitivity labels:

1. **Create the labels.** Create and name your sensitivity labels according to your organization's classification taxonomy for different sensitivity levels of content. Use common names or terms that make sense to your users. If you don't already have an established taxonomy, consider starting with label names such as Personal, Public, General, Confidential, and Highly Confidential. You can then use sublabels to group similar labels by category. When you create a label, use the tooltip text to help users select the appropriate label.
For more extensive guidance for defining a classification taxonomy, download the white paper,

2. **Define what each label can do.** Configure the protection settings you want associated with each label. For example, you might want lower sensitivity content (such as a "General" label) to have just a header or footer applied, while higher sensitivity content (such as a "Confidential" label) should have a watermark and encryption.
3. **Publish the labels.** After your sensitivity labels are configured, publish them by using a label policy. Decide which users and groups should have the labels and what policy settings to use. A single label is reusable—you define it once, and then you can include it in several label policies assigned to different users. So for example, you could pilot your sensitivity labels by assigning a label policy to just a few users. Then when you're ready to roll out the labels across your organization, you can create a new label policy for your labels and this time, specify all users.
The basic flow for deploying and applying sensitivity labels:



https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide

Assess and recommend insider risk policies

Insider risk management is a compliance solution in Microsoft 365 that helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization. Insider risk policies allow you to define the types of risks to identify and detect in your organization, including acting on cases and escalating cases to Microsoft Advanced eDiscovery if needed. Risk analysts in your organization can quickly take appropriate actions to make sure users are compliant with your organization's compliance standards.

Understand requirements and dependencies

Policy template requirements: Depending on the policy template you choose, there are requirements that you need to understand and plan for prior to configuring insider risk management in your organization:

- When using the **Data theft by departing users** template, you must configure a Microsoft 365 HR connector to periodically import resignation and termination date information for users in your organization. See the Import data with the HR connector article for step-by-step guidance to configure the Microsoft 365 HR connector for your organization.
- When using **Data leaks** templates, you must configure at least one Data Loss Prevention (DLP) policy to define sensitive information in your organization and to receive insider risk alerts for High Severity DLP policy alerts. See the Create, test, and tune a DLP policy article for step-by-step guidance to configure DLP policies for your organization.
- When using **Security policy violation** templates, you must enable Microsoft Defender for Endpoint for insider risk management integration in the Defender Security Center to import security violation alerts. For step-by-step guidance to enable Defender for Endpoint integration with insider risk management, see Configure advanced features in Microsoft Defender for Endpoint.
- When using **Disgruntled user** templates, you must configure a Microsoft 365 HR connector to periodically import performance or demotion status information for users in your organization. See the Import data with the HR connector article for step-by-step guidance

https://docs.microsoft.com/en-us/microsoft-365/compliance

/insider-risk-management-plan?view=o365-worldwide

Detect, investigate, respond, and remediate endpoint threats by using Microsoft Defender for Endpoint

Manage data retention, alert notification, and advanced features

During the onboarding process, a wizard takes you through the data storage and retention settings of Defender for Endpoint.

After completing the onboarding, you can verify your selection in the data retention settings page.

Verify data storage location

During the Set up phase, you would have selected the location to store your data.
You can verify the data location by navigating to **Settings** > **Endpoints** > **Data retention** (under **General**).

Update data retention settings

You can update the data retention settings. By default, the retention period is 180 days.

1. In the navigation pane, select **Settings** > **Endpoints** > **Data retention** (under **General**).
2. Select the data retention duration from the drop-down list.
3. Click **Save preferences**.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/data-retention-settings?view=o365-worldwide

Configure alert notifications in Microsoft Defender for Endpoint

You can configure Defender for Endpoint to send email notifications to specified recipients for new alerts. This feature enables you to identify a group of individuals who will immediately be informed and can act on alerts based on their severity.

You can set the alert severity levels that trigger notifications. You can also add or remove recipients of the email notification. New recipients get notified about alerts triggered after they're added.

If you're using role-based access control (RBAC), recipients will only receive notifications based on the device groups that were configured in the notification rule. Users with the proper permission can only create, edit, or delete notifications that are limited to their device group management scope. Only users assigned to the Global administrator role can manage notification rules that are configured for all device groups.

The email notification includes basic information about the alert and a link to the portal where you can do further investigation.

Create rules for alert notifications

1. In the navigation pane, select **Settings > Endpoints > General > Email notifications.**
2. Click Add item.
3. Specify the General information:
   - **Rule name** - Specify a name for the notification rule.
   - **Include organization name** - Specify the customer name that appears on the email notification.
   - **Include tenant-specific portal link** - Adds a link with the tenant ID to allow access to a specific tenant.
   - **Include device information -** Includes the device name in the email alert body.
   - **Devices** - Choose whether to notify recipients for alerts on all devices (Global administrator role only) or on selected device groups.
   - **Alert severity** - Choose the alert severity level.
4. Click **Next**.
5. Enter the recipient's email address then click **Add recipient**. You can add multiple email addresses.
6. Check that email recipients can receive the email notifications by selecting **Send test email**.

7.Click **Save notification rule**.

Edit a notification rule

1. Select the notification rule you'd like to edit.
2. Update the General and Recipient tab information.
3. Click **Save notification rule**.

Delete notification rule

1. Select the notification rule you'd like to delete.
2. Click **Delete**.

Troubleshoot email notifications for alerts

This section lists various issues that you may encounter when using email notifications for alerts.

Problem: Intended recipients report they're not getting the notifications.

Solution: Make sure that the notifications aren't blocked by email filters:

Check that the Defender for Endpoint email notifications aren't sent to the Junk Email folder. Mark them as Not junk.
1. Check that the Defender for Endpoint email notifications aren't sent to the Junk Email folder. Mark them as Not junk.
2. Check that your email security product isn't blocking the email notifications from Defender for Endpoint.
3. Check your email application rules that might be catching and moving your Defender for Endpoint email notifications.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide

Configure advanced features in Defender for Endpoint

Depending on the Microsoft security products that you use, some advanced features might be available for you to integrate Defender for Endpoint with.

Enable advanced features

1. In the navigation pane, select **Settings** > **Endpoints** > **Advanced features**.
2. Select the advanced feature you want to configure and toggle the setting between **On** and **Off**.
3. Click **Save preferences**.

Use the following advanced features to get better protected from potentially malicious files and gain better insight during security investigations.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/advanced-features?view=o365-worldwide

Configure device attack surface reduction rules

Why attack surface reduction rules are important

Your organization's attack surface includes all the places where an attacker could compromise your organization's devices or networks. Reducing your attack surface means protecting your organization's devices and network, which leaves attackers with fewer ways to perform attacks. Configuring attack surface reduction rules in Microsoft Defender for Endpoint can help!

Attack surface reduction rules target certain software behaviors, such as:

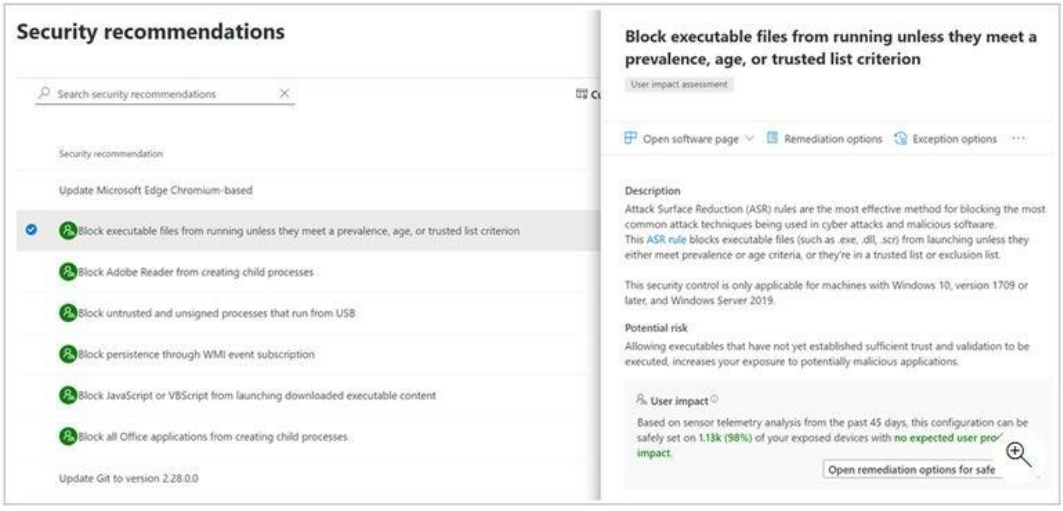
- Launching executable files and scripts that attempt to download or run files
- Running obfuscated or otherwise suspicious scripts
- Performing behaviors that apps don't usually initiate during normal day-to-day work

Such software behaviors are sometimes seen in legitimate applications. However, these behaviors are often considered risky because they are commonly abused by attackers through malware. Attack surface reduction rules can constrain software-based risky behaviors and help keep your organization safe.

For more information about configuring attack surface reduction rules, see Enable attack surface reduction rules.

Assess rule impact before deployment

You can assess how an attack surface reduction rule might affect your network by opening the security recommendation for that rule in threat and vulnerability management.



Advanced hunting and attack surface reduction events

You can use advanced hunting to view attack surface reduction events. To streamline the volume of incoming data, only unique processes for each hour are viewable with advanced hunting. The time of an attack surface reduction event is the first time that event is seen within the hour.

Attack surface reduction features across Windows versions

You can set attack surface reduction rules for devices that are running any of the following editions and versions of Windows:

- Windows 10 Pro, version 1709 or later
- Windows 10 Enterprise, version 1709 or later
- Windows Server, version 1803 (Semi-Annual Channel) or later
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide

Configure attack surface reduction capabilities

To configure attack surface reduction in your environment, follow these steps:

1. Enable hardware-based isolation for Microsoft Edge.
2. Enable application control.
    A. Review base policies in Windows. See Example Base Policies.
    B. See the Windows Defender Application Control design guide.
    C. Refer to Deploying Windows Defender Application Control (WDAC) policies.
3. Enable controlled folder access.
4. Turn on Network protection.
5. Enable exploit protection.
6. Deploy attack surface reduction rules.
7. Set up your network firewall.
    A. Get an overview of Windows Defender Firewall with advanced security.
    B. Use the Windows Defender Firewall design guide to decide how you want to design your firewall policies.
    C. Use the Windows Defender Firewall deployment guide to set up your organization's firewall with advanced security.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?view=o365-worldwide

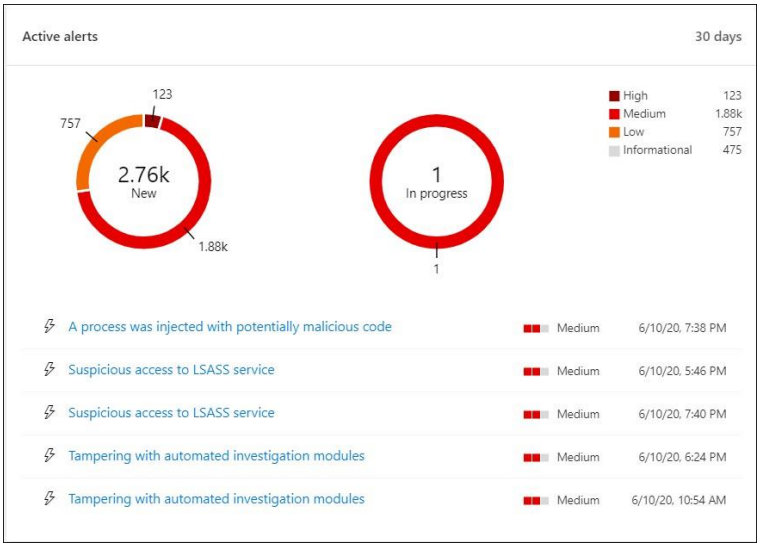
Configure and manage custom detections and alerts

The **Security operations dashboard** is where the endpoint detection and response capabilities are surfaced. It provides a high level overview of where detections were seen and highlights where response actions are needed.

The dashboard displays a snapshot of:

- Active alerts
- Devices at risk
- Sensor health
- Service health
- Daily devices reporting
- Active automated investigations
- Automated investigations statistics
- Users at risk
- Suspicious activities

You can view the overall number of active alerts from the last 30 days in your network from the tile. Alerts are grouped into **New** and **In progress**



Each group is further sub-categorized into their corresponding alert severity levels. Click the number of alerts inside each alert ring to see a sorted view of that category's queue (**New** or **In progress**).

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/security-operations-dashboard?view=o365-worldwide

Respond to incidents and alerts

The **Incidents queue** shows a collection of incidents that were flagged from devices in your network. It helps you sort through incidents to prioritize and create an informed cybersecurity response decision.

By default, the queue displays incidents seen in the last 30 days, with the most recent incident showing at the top of the list, helping you see the most recent incidents first.

On the top navigation you can:

- Customize columns to add or remove columns
- Modify the number of items to view per page
- Select the items to show per page
- Batch-select the incidents to assign
- Navigate between pages
- Apply filters

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/view-incidents-queue?view=o365-worldwide

The **Alerts queue** shows a list of alerts that were flagged from devices in your network. By default, the queue displays alerts seen in the last 30 days in a grouped view. The most recent alerts are shown at the top of the list helping you see the most recent alerts first.

There are several options you can choose from to customize the alerts view.

On the top navigation you can:

- Customize columns to add or remove columns
- Apply filters
- Display the alerts for a particular duration like 1 Day, 3 Days, 1 Week, 30 Days, and 6 Months
- Export the alerts list to excel
- Manage Alerts

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue?view=o365-worldwide

Manage automated investigations and remediations Assess and recommend endpoint configurations to reduce and remediate vulnerabilities by using Microsoft's Threat and Vulnerability Management solution.

To configure automated investigation and remediation:

1. Turn on the features; and
2. Set up device groups.

Turn on automated investigation and remediation

1. As a global administrator or security administrator, go to the Microsoft 365 Defender portal (https://security.microsoft.com) and sign in.
2. In the navigation pane, choose Settings.
3. In the **General** section, select **Advanced features**.
4. Turn on both **Automated Investigation** and **Automatically resolve alerts**.

Set up device groups

1. **I**n the Microsoft 365 Defender portal (https://security.microsoft.com), on the **Settings** page, under **Permissions**, select **Device groups**.
2. Select **+ Add device group**.
3. Create at least one device group, as follows:
   - Specify a name and description for the device group.
   - In the **Automation level list**, select a level, such as **Full - remediate threats automatically**. The automation level determines whether remediation actions are taken automatically, or only upon approval. To learn more, see Automation levels in automated investigation and remediation.
   - In the **Members** section, use one or more conditions to identify and include devices.
   - On the **User access** tab, select the Azure Active Directory groups who should have access to the device group you're creating.
4. Select **Done** when you're finished setting up your device group.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-automated-investigations-remediation?view=o365-worldwide

Manage Microsoft Defender for Endpoint threat indicators

Indicator of compromise (IoCs) matching is an essential feature in every endpoint protection solution. This capability gives SecOps the ability to set a list of indicators for detection and for blocking (prevention and response).

Create indicators that define the detection, prevention, and exclusion of entities. You can define the action to be taken as well as the duration for when to apply the action as well as the scope of the device group to apply it to.

Currently supported sources are the cloud detection engine of Defender for Endpoint, the automated investigation and remediation engine, and the endpoint prevention engine (Microsoft Defender Antivirus).

When creating a new indicator (IoC), one or more of the following actions are available:

- Allow – the IoC will be allowed to run on your devices.
- Audit – an alert will be triggered when the IoC runs.
- Warn – the IoC will prompt a warning that the user can bypass
- Block execution - the IoC will not be allowed to run.
- Block and remediate - the IoC will not be allowed to run and a remediation action will be applied to the IoC.

You can create an indicator for:

- Files
- IP addresses, URLs/domains
- Certificates

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-indicators?view=o365-worldwide

Analyze Microsoft Defender for Endpoint threat analytics

With more sophisticated adversaries and new threats emerging frequently and prevalently, it's critical to be able to quickly:

- Assess the impact of new threats
- Review your resilience against or exposure to the threats
- Identify the actions you can take to stop or contain the threats

- Threat analytics is a set of reports from expert Microsoft security researchers covering the most relevant threats, including:
- Active threat actors and their campaigns
- Popular and new attack techniques
- Critical vulnerabilities
- Common attack surfaces
- Prevalent malware

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/threat-analytics?view=o365-worldwide

Detect, investigate, respond, and remediate identity threats

Identify and remediate security risks related to sign-in risk policies

As we learned in the previous article, Identity Protection policies we have two risk policies that we can enable in our directory.

- Sign-in risk policy
- User risk policy

Both policies work to automate the response to risk detections in your environment and allow users to self-remediate when risk is detected.

Organizations can choose to block access when risk is detected. Blocking sometimes stops legitimate users from doing what they need to. A better solution is to allow self-remediation using Azure AD Multi-Factor Authentication (MFA) and self-service password reset (SSPR).

- When a sign-in risk policy triggers:
  - ◊ Azure AD MFA can be triggered, allowing to user to prove it is them by using one of their registered authentication methods, resetting the sign-in risk.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

Identify and remediate security risks related to Conditional Access events

The Conditional Access insights and reporting workbook enables you to understand the impact of Conditional Access policies in your organization over time. During sign-in, one or more Conditional Access policies may apply, granting access if certain grant controls are satisfied or denying access otherwise. Because multiple Conditional Access policies may be evaluated during each sign-in, the insights and reporting workbook lets you examine the

impact of an individual policy or a subset of all policies.

To configure a Conditional Access policy in report-only mode:

1. Sign into the Azure portal as a Conditional Access administrator, security administrator, or global administrator.
2. Browse to Azure Active Directory > Security > Conditional Access.
3. Select an existing policy or create a new policy.
4. Under Enable policy set the toggle to Report-only mode.
5. Select Save

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting

Identify and remediate security risks related to Azure Active Directory

The identity secure score is percentage that functions as an indicator for how aligned you are with Microsoft's best practice recommendations for security. Each improvement action in identity secure score is tailored to your specific configuration.

The score helps you to:

- Objectively measure your identity security posture
- Plan identity security improvements
- Review the success of your improvements

You can access the score and related information on the identity secure score dashboard. On this dashboard, you find: Your identity secure score

- A comparison graph showing how your Identity secure score compares to other tenants in the same industry and similar size
- A trend graph showing how your Identity secure score has changed over time
- A list of possible improvements

By following the improvement actions, you can:

- Improve your security posture and your score

Take advantage the features available to your organization as part of your identity investments

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score

Identify and remediate security risks using Secure Score

Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more improvement actions taken. It can be found at https://security.microsoft.com/securescore in the Microsoft 365 Defender portal.

Following the Secure Score recommendations can protect your organization from threats. From a centralized dashboard in the Microsoft 365 Defender portal, organizations can monitor and work on the security of their Microsoft 365 identities, apps, and devices.

Secure Score helps organizations:

- Report on the current state of the organization's security posture.
- Improve their security posture by providing discoverability, visibility, guidance, and control.

Compare with benchmarks and establish key performance indicators (KPIs).

https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide

Identify, investigate, and remediate security risks related to privileged identities

Privileged Identity Management (PIM) generates alerts when there is suspicious or unsafe activity in your Azure Active Directory (Azure AD) organization. When an alert is triggered, it shows up on the Privileged Identity Management dashboard. Select the alert to see a report that lists the users or roles that triggered the alert.

This section lists all the security alerts for Azure AD roles, along with how to fix and how to prevent. Severity has the following meaning:

- **High**: Requires immediate action because of a policy violation.
- **Medium**: Does not require immediate action but signals a potential policy violation.
- **Low**: Does not require immediate action but suggests a preferable policy change.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts

Configure detection alerts in Azure AD Identity Protection

Azure AD Identity Protection sends two types of automated notification emails to help you manage user risk and risk detections:

- Users at risk detected email
- Weekly digest email

Configure users at risk detected alerts

As an administrator, you can set:

- **The user risk level that triggers the generation of this email** - By default, the risk level is set to “High” risk.
- **The recipients of this email** - Users in the Global administrator, Security administrator, or Security reader roles are automatically added to this list. We attempt to send emails to the first 20 members of each role. If a user is enrolled in PIM to elevate to one of these roles on demand, then **they will only receive emails if they are elevated at the time the email is sent**.
- Optionally you can **Add custom email here** users defined must have the appropriate permissions to view the linked reports in the Azure portal.

Configure the users at risk email in the **Azure portal** under **Azure Active Directory** > **Security** > **Identity Protection** > **Users at risk detected alerts**.

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

Microsoft Defender for Identity security alerts explain the suspicious activities detected by Defender for Identity sensors on your network, and the actors and computers involved in each threat. Alert evidence lists contain direct links to the involved users and computers, to help make your investigations easy and direct.

Defender for Identity security alerts are divided into the following categories or phases, like the phases seen in a typical cyber-attack kill chain. Learn more about each phase, the alerts designed to detect each attack, and how to use the alerts to help protect your network using the following links:

1. Reconnaissance phase alerts
2. Compromised credential phase alerts
3. Lateral movement phase alerts
4. Domain dominance phase alerts
5. Exfiltration phase alerts

https://docs.microsoft.com/en-us/defender-for-identity/suspicious-activity-guide?view=o365-worldwide

Detect, investigate, respond, and remediate application threats

Identify, investigate, and remediate security risks by using Microsoft Cloud Application Security (MCAS)

Security operations teams are challenged to monitor user activity, suspicious or otherwise, across all dimensions of the identity attack surface, using multiple security solutions that often aren't connected. While many companies now have hunting teams to proactively identify threats in their environments, knowing what to look for across the vast amount of data can be a challenge. Microsoft Defender for Cloud Apps now simplifies this by taking away the need to create complex correlation rules, and lets you look for attacks that span across your cloud and on-premises network.

Defender for Cloud Apps uses the following to measure risk:

- **Alert scoring**
  The alert score represents the potential impact of a specific alert on each user. Alert scoring is based on severity, user impact, alert popularity across users, and all entities in the organization.

- **Activity scoring**
  The activity score determines the probability of a specific user performing a specific activity, based on behavioral learning of the user and their peers. Activities identified as the most abnormal receive the highest scores.

- **Blast radius (Preview)**
  Blast radius adds an additional score factor to the investigation priority calculations, based on multiple factors that determine the potential impact a compromised user has on the organization.

Phase 1: Connect to the apps you want to protect

Phase 2: Identify top risky users

Phase 3: Further investigate users

Phase 4: Protect your organization

https://docs.microsoft.com/en-us/defender-cloud-apps/tutorial-ueba

Detect suspicious user activity with UEBA

Microsoft Defender for Cloud Apps provides best-of-class detections across the attack kill chain for compromised users, insider threats, exfiltration, ransomware, and more. Our comprehensive solution is achieved by combining multiple detection methods, including anomaly, behavioral analytics (UEBA), and rule-based activity detections, to provide a broad view of how your users use apps in your environment.

So why is it important to detect suspicious behavior? The impact of a user able to alter your cloud environment can be significant and directly impact your ability to run your business. For instance, key corporate resources like the servers running your public website or service you're providing to customers can be compromised.

Using data captured from several sources, Defender for Cloud Apps analyzes the data to extract app and user activities in your organization giving your security analysts visibility into cloud use. The collected data is correlated, standardized, and enriched with threat intelligence, location, and many other details to provide an accurate, consistent view of suspicious activities.

How to tune user activity detections to identify true compromises and reduce alert fatigue resulting from handling large volumes of false positive detections:

* Configure IP address ranges
* Tune anomaly detection policies
* Tune cloud discovery anomaly detection policies
* Tune rule-based detection policies
* Configure alerts
* Investigate and remediate

https://docs.microsoft.com/en-us/defender-cloud-apps/tutorial-suspicious-activity

Investigate and remediate risky OAuth apps

OAuth is an open standard for token-based authentication and authorization. OAuth enables a user's account information to be used by third-party services, without exposing the user's password. OAuth acts as an intermediary on behalf of the user, providing the service with an access token that authorizes specific account information to be shared.

Our recommended approach is to investigate the apps by using the abilities and information provided in the Defender for Cloud Apps portal to filter out apps with a low chance of being risky, and focus on the suspicious apps.

- **Detect risky OAuth apps**

Detecting a risky OAuth app can be accomplished using:
Alerts: React to an alert triggered by an existing policy.
Hunting: Search for a risky app among all the available apps, without concrete suspicion of a risk.

Investigate risky OAuth apps

- After you determine that an app is suspicious and you want to investigate it, we recommend the following key principles for efficient investigation:
- The more common and used an app is, either by your organization or online, the more likely it is to be safe.
- An app should require only permissions that are related to the app's purpose. If that's not the case, the app might be risky.
- Apps that require high privileges or admin consent are more likely to be risky.
  Remediate risky OAuth apps

How to remediate suspicious OAuth apps

After you determine that an OAuth app is risky, Defender for Cloud Apps provides the following remediation options:

- Manual remediation: You can easily ban revoke an app from the OAuth apps page
- Automatic remediation: You can create a policy that automatically revokes an app or revokes a specific user from an app.

https://docs.microsoft.com/en-us/defender-cloud-apps/investigate-risky-oauth

Configure MCAS to generate alerts and reports to detect threats

Alerts are the entry points to understanding your cloud environment more deeply. You might want to create new policies based on what you find. For example, you might see an administrator signing in from Greenland, and no one in your organization ever signed in from Greenland before. You can create a policy that automatically suspends an admin account when it's used to sign in from that location.

It's a good idea to review all of your alerts and use them as tools for modifying your policies. If harmless events are being considered violations to existing policies, refine your policies so that you receive fewer unnecessary alerts.

https://docs.microsoft.com/en-us/defender-cloud-apps/managing-alerts

Manage cross-domain investigations in Microsoft 365 Defender portal

Manage incidents across Microsoft 365 Defender products

Incident management is critical to ensuring that incidents are named, assigned, and tagged to optimize time in your incident workflow and more quickly contain and address threats.

Here are the ways you can manage your incidents:

- Edit the incident name
- Add incident tags
- Assign the incident to a user account
- Resolve them
- Specify its classification
- Add comments

https://docs.microsoft.com/en-us/microsoft-365/security/defender/manage-incidents?view=o365-worldwide

Manage actions pending approval across products

It's important to approve (or reject) pending actions as soon as possible so that your automated investigations can proceed and complete in a timely manner.

1. Go to Microsoft 365 Defender portal and sign in.
2. In the navigation pane, choose Action center.
3. In the Action center, on the Pending tab, select an item in the list. Its flyout pane opens.
4. Review the information in the flyout pane, and then take one of the following steps:
   - Select Open investigation page to view more details about the investigation.
   - Select Approve to initiate a pending action.
   - Select Reject to prevent a pending action from being taken.
   - Select Go hunt to go into Advanced hunting.

https://docs.microsoft.com/en-us/microsoft-365/security/defender/m365d-autoir-actions?view=o365-worldwide

Perform advanced threat hunting

With advanced hunting in Microsoft 365 Defender, you can create queries that locate individual artifacts associated with ransomware activity. You can also run more sophisticated queries that can look for signs of activity and weigh those signs to find devices that require immediate attention.

Check for individual signs of ransomware activity

Many activities that constitute ransomware behavior, including the activities described in the preceding section, can be benign. When using the following queries to locate ransomware, run more than one query to check whether the same devices are exhibiting various signs of possible ransomware activity.

- Stopping multiple processes using taskkill.exe
- Stopping processes using net stop
- Deletion of data on multiple drives using cipher.exe
- Clearing of forensic evidence from event logs using wevtutil
- Turning off services using sc.exe
- Turning off System Restore
- Backup deletion

Check for multiple signs of ransomware activity

Instead of running several queries separately, you can also use a comprehensive query that checks for multiple signs of ransomware activity to identify affected devices. The following consolidated query:

- Looks for both relatively concrete and subtle signs of ransomware activity
- Weighs the presence of these signs
- Identifies devices with a higher chance of being targets of ransomware

When run, this consolidated query returns a list of devices that have exhibited multiple signs of attack. The count of each type of ransomware activity is also shown. To run this consolidated query, copy it directly to the advanced hunting query editor.

https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-find-ransomware?view=o365-worldwide

Mitigate threats using Microsoft Defender for Cloud (25-30%)

Use Microsoft Defender for Cloud, for Azure, hybrid cloud, and on-premises workload protection and security. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

You can access the Microsoft Learn materials online content here:
https://docs.microsoft.com/en-us/learn/paths/sc-200-mitigate-threats-using-azure-defender/

Design and configure a Microsoft Defender for Cloud implementation

Plan and configure Microsoft Defender for Cloud settings, including selecting target subscriptions and workspace

Use management groups to efficiently manage access, policies, and reporting on **groups of subscriptions**, as well as effectively manage the entire Azure estate by performing actions on the root management group. You can organize subscriptions into management groups and apply your governance policies to the management groups. All subscriptions within a management group automatically inherit the policies applied to the management group.

The root management group is created automatically when you do any of the following actions:

- Open **Management Groups** in the Azure portal.
- Create a management group with an API call.
- Create a management group with PowerShell. For PowerShell instructions, see Create management groups for resource and organization management.

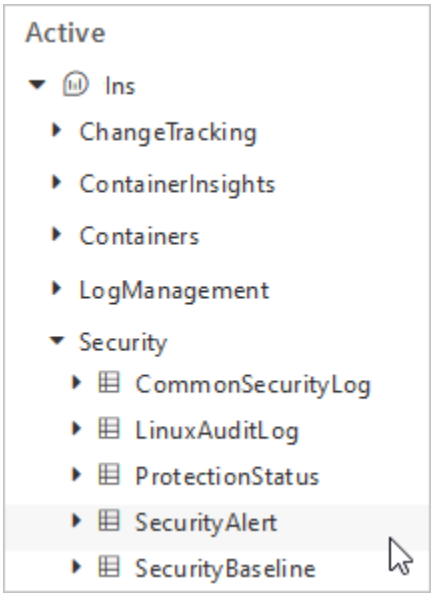
Information about exporting to a Log Analytics workspace

If you want to analyze Microsoft Defender for Cloud data inside a Log Analytics workspace or use Azure alerts together with Defender for Cloud alerts, set up continuous export to your Log Analytics workspace.

Log Analytics tables and schemas

Security alerts and recommendations are stored in the Security Alert and Security Recommendation tables respectively.

The name of the Log Analytics solution containing these tables depends on whether you have enabled the enhanced security features: Security ('Security and Audit') or SecurityCenterFree.



https://docs.microsoft.com/en-us/azure/defender-for-cloud/continuous-export

Configure Microsoft Defender for Cloud roles

Defender for Cloud uses Azure role-based access control (Azure RBAC), which provides built-in roles that can be assigned to users, groups, and services in Azure.

Defender for Cloud assesses the configuration of your resources to identify security issues and vulnerabilities. In Defender for Cloud, you only see information related to a resource when you are assigned the role of Owner, Contributor, or Reader for the subscription or the resource's resource group.

In addition to the built-in roles, there are two roles specific to Defender for Cloud:

- **Security Reader**: A user that belongs to this role has viewing rights to Defender for Cloud. The user can view recommendations, alerts, a security policy, and security states, but cannot make changes.
- **Security Admin**: A user that belongs to this role has the same rights as the Security Reader and can also update the security policy and dismiss alerts and recommendations.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

Configure data retention policies

The following steps describe how to configure how long log data is kept by in your workspace. Data retention at the workspace level can be configured from 30 to 730 days (2 years) for all workspaces unless they're using the legacy Free Trial pricing tier. Retention for individual data types can be set as low as 4 days. Learn more about pricing for longer data retention. To retain data longer than 730 days, consider using Log Analytics workspace data export.

Workspace level default retention
To set the default retention for your workspace:

1. In the Azure portal, from your workspace, select Usage and estimated costs in the left pane.
2. On the Usage and estimated costs page, select Data Retention at the top of the page.
3. On the pane, move the slider to increase or decrease the number of days, and then select OK. If you're on the free tier, you can't modify the data retention period; you need to upgrade to the paid tier to control this setting.

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/manage-cost-storage

Assess and recommend cloud workload protection

Defender for Cloud's recommendations are based on the Azure Security Benchmark. Azure Security Benchmark is the Microsoft-authored, Azure-specific set of guidelines for security and compliance best practices based on common compliance frameworks. This widely respected benchmark builds on the controls from the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) with a focus on cloud-centric security.

Tip

If a recommendation's description says "No related policy", it's usually because that recommendation is dependent on a different recommendation and *its* policy. For example, the recommendation "Endpoint protection health failures should be remediated...", relies on the recommendation that checks whether an endpoint protection solution is even *installed* ("Endpoint protection solution should be installed..."). The underlying recommendation *does* have a policy. Limiting the policies to only the foundational recommendation simplifies policy management.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference

Plan and implement the use of data connectors for ingestion of data sources in Microsoft Defender for Cloud

Identify data sources to be ingested for Microsoft Defender for Cloud

This document helps you to manage security solutions already connected to Microsoft Defender for Cloud and add new ones.

Integrated Azure security solutions

Defender for Cloud makes it easy to enable integrated security solutions in Azure. Benefits include:

- **Simplified deployment**: Defender for Cloud offers streamlined provisioning of integrated partner solutions. For solutions like antimalware and vulnerability assessment, Defender for Cloud can provision the agent on your virtual machines. For firewall appliances, Defender for Cloud can take care of much of the network configuration required.

- **Integrated detections**: Security events from partner solutions are automatically collected, aggregated, and displayed as part of Defender for Cloud alerts and incidents. These events also are fused with detections from other sources to provide advanced threat-detection capabilities.
- **Unified health monitoring and management**: Customers can use integrated health events to monitor all partner solutions at a glance. Basic management is available, with easy access to advanced setup by using the partner solution.

Defender for Cloud also offers vulnerability analysis for your:
SQL databases
Azure Container Registry images

https://docs.microsoft.com/en-us/azure/defender-for-cloud/partner-integration

Configure automated onboarding for Azure resources

Microsoft Defender for Cloud collects data from your resources using the relevant agent or extensions for that resource and the type of data collection you've enabled. Use the procedures below to ensure your resources have the necessary agents and extensions used by Defender for Cloud.

Defender for Cloud collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.

Data collection is required to provide visibility into missing updates, misconfigured OS security settings, endpoint protection status, and health and threat protection. Data collection is only needed for compute resources such as VMs, virtual machine scale sets, IaaS containers, and non-Azure computers.

Data is collected using:

- The **Log Analytics agent**, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.
- **Security extensions**, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Defender for Cloud regarding specialized resource types.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection

Connect on-premises computers

Defender for Cloud can monitor the security posture of your non-Azure computers, but first you need to connect them to Azure.

You can connect your non-Azure computers in any of the following ways:

- Using Azure Arc-enabled servers (**recommended**)
- From Defender for Cloud's pages in the Azure portal (**Getting started** and **Inventory**)

https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines

Connect AWS cloud resources

With cloud workloads commonly spanning multiple cloud platforms, cloud security services must do the same.
Microsoft Defender for Cloud protects workloads in Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

To protect your AWS-based resources, you can connect an account with one of two mechanisms:

- **Classic cloud connectors experience** - As part of the initial multi-cloud offering, we introduced these cloud connectors as a way to connect your AWS and GCP projects. If you've already configured an AWS connector through the classic cloud connectors experience, we recommend deleting these connectors (as explained in Remove classic connectors), and connecting the account again using the newer mechanism. If you don't do this before creating the new connector through the environment settings page, do so afterwards to avoid seeing duplicate recommendations.

- **Environment settings page** - This preview page provides a greatly improved, simpler, onboarding experience (including auto provisioning). This mechanism also extends Defender for Cloud's enhanced security features to your AWS resources:

    - ◊ **Defender for Cloud's CSPM features** extends to your AWS resources.
    - ◊ **Microsoft Defender for Containers** brings threat detection and advanced defenses to your Amazon EKS clusters. Microsoft Defender for servers brings threat detection and advanced defenses to your GCP VM instances
    - ◊ **Microsoft Defender for servers** brings threat detection and advanced defenses to your Windows and Linux EC2 instances.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws

Connect GCP cloud resources

To protect your GCP-based resources, you can connect an account in two different ways:

- **Classic cloud connectors experience** - As part of the initial multi-cloud offering, we introduced these cloud connectors as a way to connect your AWS and GCP projects.

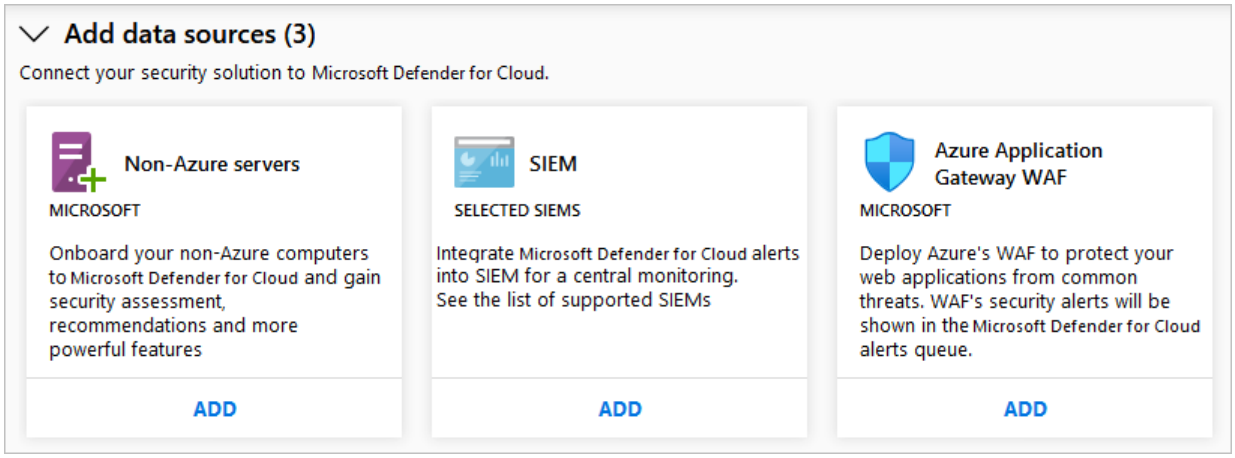
- **Environment settings page** (Recommended) - This page provides the onboarding experience (including auto provisioning). This mechanism also extends Defender for Cloud's enhanced security features to your GCP resources:

    - ◊ **Defender for Cloud's CSPM features** extends to your GCP resources.
    - ◊ **Microsoft Defender for Containers** - Microsoft Defender for Containers brings threat detection and advanced defenses to your Google's Kubernetes Engine (GKE) Standard clusters
    - ◊ **Microsoft Defender for servers** brings threat detection and advanced defenses to your GCP VM instances

https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp

Configure data collection

The Add data sources section includes other available data sources that can be connected. For instructions on adding data from any of these sources, click ADD.



https://docs.microsoft.com/en-us/azure/defender-for-cloud/partner-integration

Manage Microsoft Defender for Cloud alert rules

Validate alert configuration

Defender for Cloud generates alerts for resources deployed on your Azure, on-premises, and hybrid cloud environments.

Alerts are the notifications that Defender for Cloud generates when it detects threats on your resources. Defender for Cloud prioritizes and lists the alerts, along with the information needed for you to quickly investigate the problem. Defender for Cloud also provides detailed steps to help you remediate attacks. Alerts data is retained for 90 days.

A **security incident** is a collection of related alerts, instead of listing each alert individually. Defender for Cloud uses Cloud smart alert correlation (incidents) to correlate different alerts and low fidelity signals into security incidents.

Using incidents, Defender for Cloud provides you with a single view of an attack campaign and all of the related alerts. This view enables you to quickly understand what actions the attacker took, and what resources were affected.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview

Setup email notifications

Use Defender for Cloud's **Email notifications** settings page to define preferences for notification emails including:

- ***who should be notified*** - Emails can be sent to select individuals or to anyone with a specified Azure role for a subscription.
- ***what they should be notified about*** **-** Modify the severity levels for which Defender for Cloud should send out notifications.

To avoid alert fatigue, Defender for Cloud limits the volume of outgoing mails. For each subscription, Defender for Cloud sends:
approximately **four emails per day** for **high-severity alerts**
approximately **two emails per day** for **medium-severity alerts**
approximately **one email per day** for **low-severity alerts**

https://docs.microsoft.com/en-us/azure/defender-for-cloud/configure-email-notifications

Create and manage alert suppression rules

The various Microsoft Defender plans detect threats in any area of your environment and generate security alerts.

When a single alert isn't interesting or relevant, you can manually dismiss it. Alternatively, use the suppression rules feature to automatically dismiss similar alerts in the future. Typically, you'd use a suppression rule to:

- Suppress alerts that you've identified as false positives
- Suppress alerts that are being triggered too often to be useful

Your suppression rules define the criteria for which alerts should be automatically dismissed.

There are a few ways you can create rules to suppress unwanted security alerts:

- To suppress alerts at the management group level, use Azure Policy
- To suppress alerts at the subscription level, you can use the Azure portal or the REST API

https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules

Configure automation and remediation

Configure automated responses in Microsoft Defender for Cloud

Every security program includes multiple workflows for incident response. These processes might include notifying relevant stakeholders, launching a change management process, and applying specific remediation steps. Security experts recommend that you automate as many steps of those procedures as you can. Automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

This article describes the workflow automation feature of Microsoft Defender for Cloud. This feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance. For example, you might want Defender for Cloud to email a specific user when an alert occurs.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

Design and configure workflow automation in Microsoft Defender for Cloud

Every security program includes multiple workflows for incident response. These processes might include notifying relevant stakeholders, launching a change management process, and applying specific remediation steps. Security experts recommend that you automate as many steps of those procedures as you can. Automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

This article describes the workflow automation feature of Microsoft Defender for Cloud. This feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance. For example, you might want Defender for Cloud to email a specific user when an alert occurs. You'll also learn how to create Logic Apps using Azure Logic Apps.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

Remediate incidents by using Microsoft Defender for Cloud recommendations

Using the policies, Defender for Cloud periodically analyzes the compliance status of your resources to identify potential security misconfigurations and weaknesses. It then provides you with recommendations on how to remediate those issues. Recommendations are the result of assessing your resources against the relevant policies and identifying resources that aren't meeting your defined requirements.

Defender for Cloud makes its security recommendations based on your chosen initiatives. When a policy from your initiative is compared against your resources and finds one or more that aren't compliant it is presented as a recommendation in Defender for Cloud.

Recommendations are actions for you to take to secure and harden your resources. Each recommendation provides you with the following information:

- A short description of the issue
- The remediation steps to carry out in order to implement the recommendation
- The affected resources

https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept

Create an automatic response using an Azure Resource Manager template

An ARM template is a JavaScript Object Notation (JSON) file that defines the infrastructure and configuration for your project. The template uses declarative syntax. In declarative syntax, you describe your intended deployment without writing the sequence of programming commands to create the deployment.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-automation-alert

Investigate Microsoft Defender for Cloud alerts and incidents

Describe alert types for Azure workloads

Defender for Cloud generates alerts for resources deployed on your Azure, on-premises, and hybrid cloud environments.

Security alerts are triggered by advanced detections and are available only with enhanced security features enabled. You can upgrade from the Environment settings page, as described in QuickStart: Enable enhanced security features.

Defender for Cloud assigns a severity to alerts, to help you prioritize the order in which you attend to each alert, so that when a resource is compromised, you can get to it right away. The severity is based on how confident Defender for Cloud is in the finding or the analytic used to issue the alert as well as the confidence level that there was malicious intent behind the activity that led to the alert.

Severity	Recommended response
High	There is a high probability that your resource is compromised. You should look into it right away. Defender for Cloud has high confidence in both the malicious intent and in the findings used to issue the alert. For example, an alert that detects the execution of a known malicious tool such as Mimikatz, a common tool used for credential theft.
Medium	This is probably a suspicious activity might indicate that a resource is compromised. Defender for Cloud's confidence in the analytic or finding is medium and the confidence of the malicious intent is medium to high. These would usually be machine learning or anomaly-based detections. For example, a sign-in attempt from an anomalous location.
Low	This might be a benign positive or a blocked attack. Defender for Cloud isn't confident enough that the intent is malicious and the activity might be innocent. For example, log clear is an action that might happen when an attacker tries to hide their tracks, but in many cases is a routine operation performed by admins. Defender for Cloud doesn't usually tell you when attacks were blocked, unless it's an interesting case that we suggest you look into.
Informational	An incident is typically made up of a number of alerts, some of which might appear on their own to be only informational, but in the context of the other alerts might be worthy of a closer look.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview

Manage security alerts

Microsoft Defender for Cloud continuously analyzes your hybrid cloud workloads using advanced analytics and threat intelligence to alert you about potentially malicious activities in your cloud resources. You can also integrate alerts from other security products and services into Defender for Cloud. Once an alert is raised, swift action is needed to investigate and remediate the potential security issue.

Triage security alerts

Defender for Cloud provides a unified view of all security alerts. Security alerts are ranked based on the severity of the detected activity.

Triage your alerts from the Security alerts page

Use this page to review the active security alerts in your environment to decide which alert to investigate first.

When triaging security alerts, prioritize alerts based on the alert severity by addressing alerts with higher severity first.

Investigate a security alert

When you've decided which alert to investigate first:

1. Select the desired alert.
2. From the alert overview page, select the resource to investigate first.
3. Begin your investigation from the left pane, which shows the high-level information about the security alert.
4. For more detailed information that can help you investigate the suspicious activity, examine the Alert details tab.
5. When you've reviewed the information on this page, you may have enough to proceed with a response. If you need further details:

Respond to a security alert

1. Open the Take action tab to see the recommended responses.
2. Review the Mitigate the threat section for the manual investigation steps necessary to mitigate the issue.
3. To harden your resources and prevent future attacks of this kind, remediate the security recommendations in the Prevent future attacks section.
4. To trigger a logic app with automated response steps, use the Trigger automated response section.
5. If the detected activity isn't malicious, you can suppress future alerts of this kind using the Suppress similar alerts section.
6. When you've completed the investigation into the alert and responded in the appropriate way, change the status to Dismissed.
7. We encourage you to provide feedback about the alert to Microsoft.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-incident

Manage security incidents

Triaging and investigating security alerts can be time consuming for even the most skilled security analysts. For many, it's hard to know where to begin.

Defender for Cloud uses analytics to connect the information between distinct security alerts. Using these connections, Defender for Cloud can provide a single view of an attack campaign and its related alerts to help you understand the attacker's actions and the affected resources.

What is a security incident?

In Defender for Cloud, a security incident is an aggregation of all alerts for a resource that align with kill chain patterns. Incidents appear in the Security alerts page. Select an incident to view the related alerts and get more information.

Managing security incidents

1. On Defender for Cloud's alerts page, use the Add filter button to filter by alert name to the alert name Security incident detected on multiple resources.
2. To view details of an incident, select one from the list. A side pane appears with more details about the incident.
3. To view more details, select View full details.

To switch to the Take action tab, select the tab or the button on the bottom of the right pane. Use this tab to take further actions such as:

- Mitigate the threat - provides manual remediation steps for this security incident
- Prevent future attacks - provides security recommendations to help reduce the attack surface, increase security posture, and prevent future attacks
- Trigger automated response - provides the option to trigger a Logic App as a response to this security incident
- Suppress similar alerts - provides the option to suppress future alerts with similar characteristics if the alert isn't relevant for your organization

4. To remediate the threats in the incident, follow the remediation steps provided with each alert.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/incidents

Analyze Microsoft Defender for Cloud threat intelligence

Defender for Cloud's threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats.

When Defender for Cloud identifies a threat, it triggers a security alert, which contains detailed information regarding the event, including suggestions for remediation. To help incident response teams investigate and remediate threats, Defender for Cloud provides threat intelligence reports containing information about detected threats. The report includes information such as:

- Attacker's identity or associations (if this information is available)
- Attackers' objectives
- Current and historical attack campaigns (if this information is available)
- Attackers' tactics, tools, and procedures
- Associated indicators of compromise (IoC) such as URLs and file hashes
- Victimology, which is the industry and geographic prevalence to assist you in determining if your Azure resources are at risk
- Mitigation and remediation information

Defender for Cloud has three types of threat reports, which can vary according to the attack. The reports available are:

- Activity Group Report: provides deep dives into attackers, their objectives, and tactics.
- Campaign Report: focuses on details of specific attack campaigns.
- Threat Summary Report: covers all of the items in the previous two reports.

This type of information is useful during the incident response process, where there's an ongoing investigation to understand the source of the attack, the attacker's motivations, and what to do to mitigate this issue in the future.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports

Respond to Microsoft Defender for Cloud for Key Vault alerts

When you receive an alert from Microsoft Defender for Key Vault, we recommend you investigate and respond to the alert as described below. Microsoft Defender for Key Vault protects applications and credentials, so even if you're familiar with the application or user that triggered the alert, it's important to verify the situation surrounding every alert.
Alerts from Microsoft Defender for Key Vault includes these elements:

- Object ID
- User Principal Name or IP address of the suspicious resource

Depending on the type of access that occurred, some fields might not be available. For example, if your key vault was accessed by an application, you won't see an associated User Principal Name. If the traffic originated from outside of Azure, you won't see an Object ID.

Step 1. Identify the source
Step 2. Respond accordingly
Step 3. Measure the impact
Step 4. Take action

Manage user data discovered during an investigation

Searching for and identifying personal data

A Defender for Cloud user can view their personal data through the Azure portal. Defender for Cloud only stores security contact details such as email addresses and phone numbers.

In the Azure portal, a user can view allowed IP configurations using Defender for Cloud's just-in-time VM access feature and a user can view security alerts provided by Defender for Cloud including IP addresses and attacker details

Classifying personal data

You don't need to classify personal data found in Defender for Cloud's security contact feature. The data saved is an email address (or multiple email addresses) and a phone number. Contact data is validated by Defender for Cloud.

You don't need to classify the IP addresses and port numbers saved by Defender for Cloud's just-in-time feature.

Only a user assigned the role of Administrator can classify personal data by viewing alerts in Defender for Cloud.

Securing and controlling access to personal data

A Defender for Cloud user assigned the role of Reader, Owner, Contributor, or Account Administrator can access security contact data, can access their just-in-time policies and can view their alerts.

Updating personal data

A Defender for Cloud user assigned the role of Owner, Contributor, or Account Administrator can update security contact data via the Azure portal and can update their just-in-time policies.

An Account Administrator can't edit alert incidents. An alert incident is considered security data and is read only.

Deleting personal data

A Defender for Cloud user assigned the role of Owner, Contributor, or Account Administrator can delete security contact data and the just-in-time policies via the Azure portal.

A Defender for Cloud user can't delete alert incidents. For security reasons, an alert incident is considered read-only data.

Exporting personal data

A Defender for Cloud user assigned the role of Reader, Owner, Contributor, or Account Administrator can export security contact data by:

- Copying from the Azure portal
- Executing the Azure REST API call, GET HTTP:

A Defender for Cloud user assigned the role of Account Administrator can export the just-in-time policies containing the IP addresses by:

- Copying from the Azure portal
- Executing the Azure REST API call, GET HTTP:

An Account Administrator can export the alert details by:

- Copying from the Azure portal
- Executing the Azure REST API call, GET HTTP:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/privacy

Mitigate threats using Microsoft Sentinel (40-45%)

Design and configure an Microsoft Sentinel Workspace

Plan a Microsoft Sentinel Workspace

Use the Log Analytics workspaces menu to create a Log Analytics workspace in the Azure portal. Log Analytics workspace is the environment for Azure Monitor log data. Each workspace has its own data repository and configuration, and data sources and solutions are configured to store their data in a particular workspace. A workspace has unique workspace ID and resource ID. You can reuse the same workspace name when in different resource groups.

You require a Log Analytics workspace if you intend on collecting data from the following sources:

- Azure resources in your subscription
- On-premises computers monitored by System Center Operations Manager
- Device collections from Configuration Manager
- Diagnostics or log data from Azure storage

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace

Azure Monitor stores log data in a Log Analytics workspace, which is an Azure resource and a container where data is collected, aggregated, and serves as an administrative boundary. While you can deploy one or more workspaces in your Azure subscription, there are several considerations you should understand in order to ensure your initial deployment is following our guidelines to provide you with a cost effective, manageable, and scalable deployment meeting your organization's needs.

Data in a workspace is organized into tables, each of which stores different kinds of data and has its own unique set of properties based on the resource generating the data. Most data sources will write to their own tables in a Log Analytics workspace.

A Log Analytics workspace provides:

- A geographic location for data storage.
- Data isolation by granting different users access rights following one of our recommended design strategies.

Scope for configuration of settings like pricing tier, retention, and data capping.

Workspaces are hosted on physical clusters. By default, the system is creating and managing these clusters. Customers that ingest more than 4TB/day are expected to create their own dedicated clusters for their workspaces - it enables them better control and higher ingestion rate.

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/design-logs-deployment

Configure Microsoft Sentinel roles

Microsoft Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure.

Use Azure RBAC to create and assign roles within your security operations team to grant appropriate access to Microsoft Sentinel. The different roles give you fine-grained control over what users of Microsoft Sentinel can see and do. Azure roles can be assigned in the Microsoft Sentinel workspace directly (see note below), or in a subscription or resource group that the workspace belongs to, which Microsoft Sentinel will inherit.

Microsoft Sentinel-specific roles

All Microsoft Sentinel built-in roles grant read access to the data in your Microsoft Sentinel workspace.

- Microsoft Sentinel Reader can view data, incidents, workbooks, and other Microsoft Sentinel resources.
- Microsoft Sentinel Responder can, in addition to the above, manage incidents (assign, dismiss, etc.)
- Microsoft Sentinel Contributor can, in addition to the above, create and edit workbooks, analytics rules, and other Microsoft Sentinel resources.
- Microsoft Sentinel Automation Contributor allows Microsoft Sentinel to add playbooks to automation rules. It is not meant for user accounts.

Additional roles and permissions

Users with particular job requirements may need to be assigned additional roles or specific permissions in order to accomplish their tasks.

- Working with playbooks to automate responses to threats
- Connecting data sources to Microsoft Sentinel
- Guest users assigning incidents
- Creating and deleting workbooks

Other roles you might see assigned

Azure roles: Owner, Contributor, and Reader. Azure roles grant access across all your Azure resources, including Log Analytics workspaces and Microsoft Sentinel resources.
Log Analytics roles: Log Analytics Contributor and Log Analytics Reader. Log Analytics roles grant access to your Log Analytics workspaces.

For example, a user who is assigned the **Microsoft Sentinel Reader** role, but not the Microsoft **Sentinel Contributor role**, will still be able to edit items in Microsoft Sentinel if assigned the Azure-level Contributor role. Therefore, if you want to grant permissions to a user only in Microsoft Sentinel, you should carefully remove this user's prior permissions, making sure you do not break any needed access to another resource.

https://docs.microsoft.com/en-us/azure/sentinel/roles

Design Microsoft Sentinel data storage

Azure Monitor Logs is designed to scale and support collecting, indexing, and storing massive amounts of data per day from any source in your enterprise or deployed in Azure. Although this might be a primary driver for your organization, cost-efficiency is ultimately the underlying driver. To that end, it's important to understand that the cost of a Log Analytics workspace isn't based only on the volume of data collected; it's also dependent on the selected plan, and how long you stored data generated from your connected sources.

The default pricing for Log Analytics is a **Pay-As-You-Go** model that's based on ingested data volume and, optionally, for longer data retention. Data volume is measured as the size of the data that will be stored in GB (10^9 bytes). Each Log Analytics workspace is charged as a separate service and contributes to the bill for your Azure subscription. The amount of data ingestion can be considerable, depending on the following factors:

- The set of management solutions enabled and their configuration
- The number and type of monitored resources
- Type of data collected from each monitored resource

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/manage-cost-storage

Configure security settings and access for Microsoft Sentinel

This security baseline applies guidance from the Azure Security Benchmark version 2.0 to Microsoft Sentinel. The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Azure Security Benchmark and the related guidance applicable to Microsoft Sentinel.

Network Security

NS-1: Implement security for internal traffic

Identity Management

IM-1: Standardize Azure Active Directory as the central identity and authentication system

IM-3: Use Azure AD single sign-on (SSO) for application access

Privileged Access

PA-3: Review and reconcile user access regularly

PA-6: Use privileged access workstations

PA-7: Follow just enough administration (least privilege principle)

Data Protection

DP-4: Encrypt sensitive information in transit

DP-5: Encrypt sensitive data at rest

Asset Management

AM-1: Ensure security team has visibility into risks for assets

AM-2: Ensure security team has access to asset inventory and metadata

AM-3: Use only approved Azure services

https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/sentinel-security-baseline

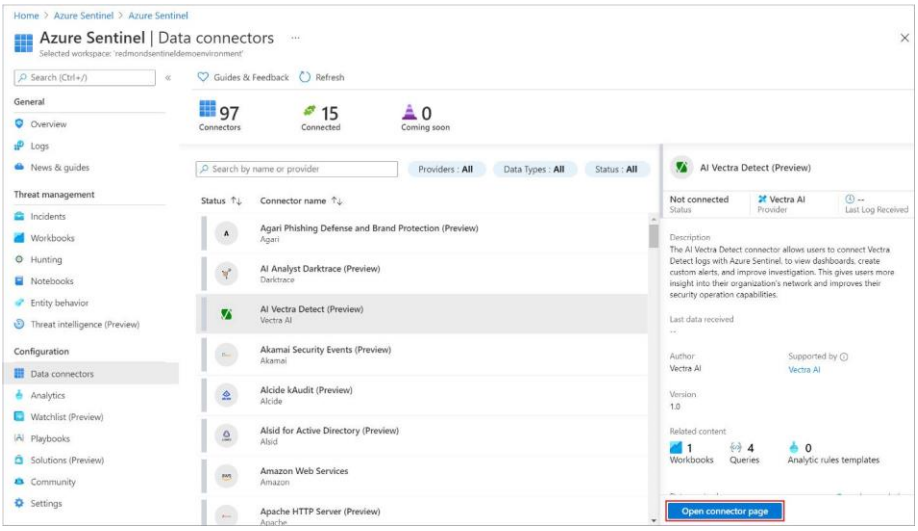
Plan and Implement the use of Data Connectors for Ingestion of Data Sources in Microsoft Sentinel

Identify data sources to be ingested for Microsoft Sentinel

After onboarding Microsoft Sentinel into your workspace, connect data sources to start ingesting your data into Microsoft Sentinel. Microsoft Sentinel comes with many connectors for Microsoft products, available out of the box and providing real-time integration. For example, service-to-service connectors include Microsoft 365 Defender connectors and Microsoft 365 sources, such as Office 365, Azure Active Directory (Azure AD), Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps.

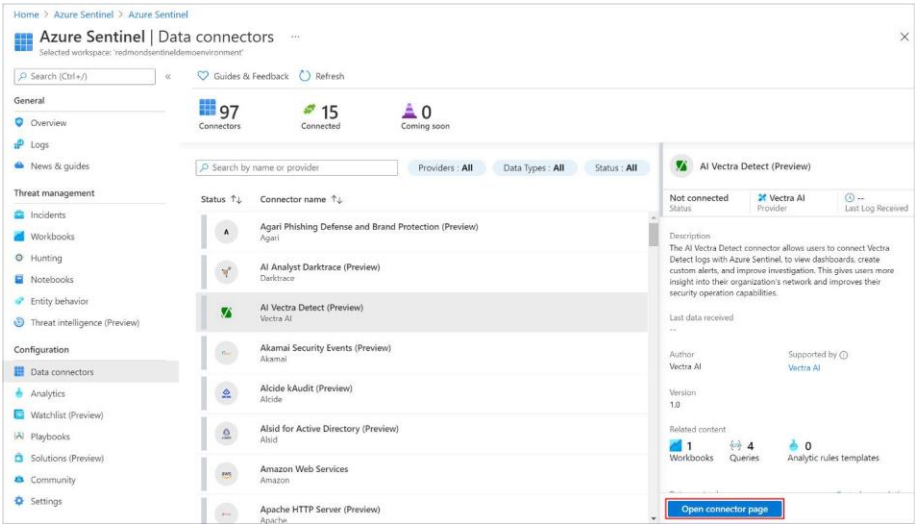
You can also enable out-of-the-box connectors to the broader security ecosystem for non-Microsoft products. For example, you can use Syslog, Common Event Format (CEF), or REST APIs to connect your data sources with Microsoft Sentinel.

The **Data connectors** page, accessible from the Microsoft Sentinel navigation menu, shows the full list of connectors that Microsoft Sentinel provides, and their status in your workspace. Select the connector you want to connect, and then select Open connector page.

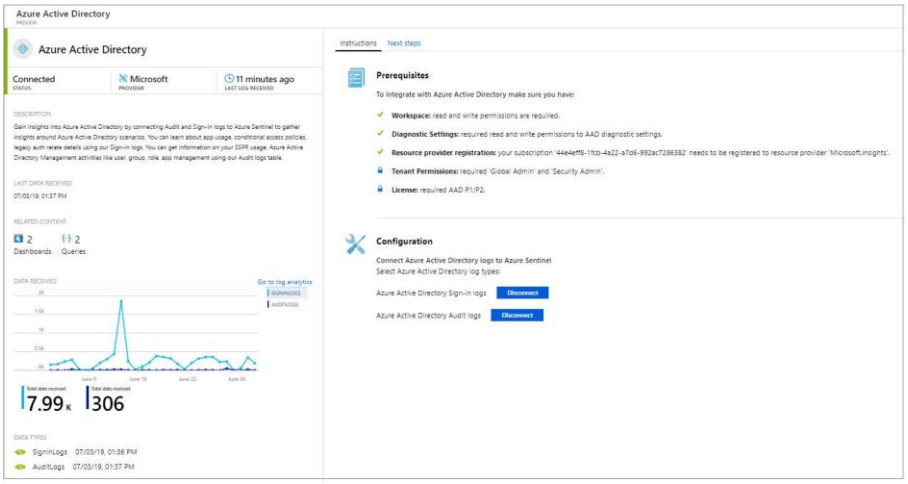


Identify the prerequisites for a data connector

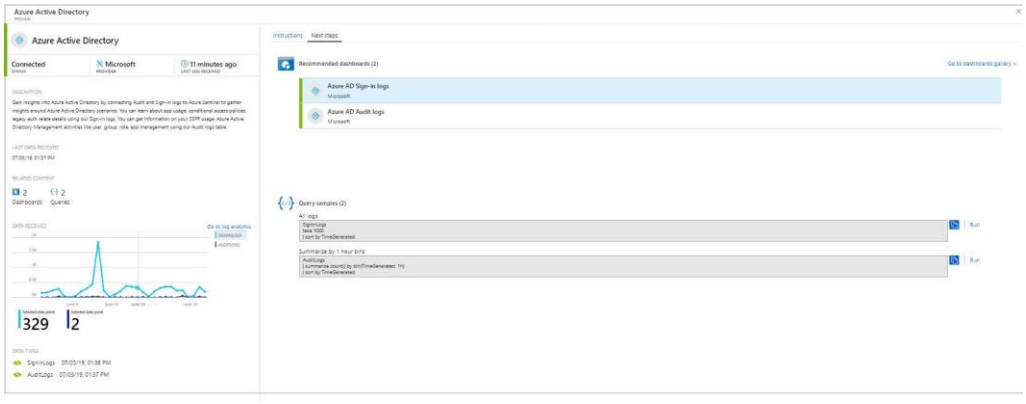
The Data connectors page, accessible from the Microsoft Sentinel navigation menu, shows the full list of connectors that Microsoft Sentinel provides, and their status. Select the connector you want to connect, and then select Open connector page.



You'll need to have fulfilled all the prerequisites, and you'll see complete instructions on the connector page to ingest the data to Microsoft Sentinel. It may take some time for data to start arriving. After you connect, you see a summary of the data in the Data received graph, and the connectivity status of the data types.



In the Next steps tab, you'll see additional content that Microsoft Sentinel provides for the specific data type - sample queries, visualization workbooks, and analytics rule templates to help you detect and investigate threats.



https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

Configure and use Microsoft Sentinel data connectors

Microsoft Sentinel provides a wide range of built-in connectors for Azure services and external solutions, and also supports ingesting data from some sources without a dedicated connector.

If you're unable to connect your data source to Microsoft Sentinel using any of the existing solutions available, consider creating your own data source connector.

Custom connector methods

The following table compares essential details about each method for creating custom connectors described in this article.

Method description	Capability	Serverless	Complexity
Codeless Connector Platform (CCP) Best for less technical audiences to create SaaS connectors using a configuration file instead of advanced	Supports all capabilities available with the code.	Yes	Low; simple, codeless development
Log Analytics Agent Best for collecting files from on-premises and IaaS sources	File collection only	No	Low
Logstash Best for on-premises and IaaS sources, any source for which a plugin is available, and organizations	Available plugins, plus custom plugin, capabilities provide significant flexibility.	No; requires a VM or VM cluster to run	Low; supports many scenarios with plugins
Logic Apps High cost; avoid for high-volume data Best for low-volume cloud sources	Codeless programming allows for limited flexibility, without support for implementing algorithms. If no available action already supports your requirements, creating a custom action may add complexity.	Yes	Low; simple, codeless development
PowerShell Best for prototyping and periodic file uploads	Direct support for file collection. PowerShell can be used to collect more sources, but will require coding and configuring the script as a ser-	No	Low
Log Analytics API Best for ISVs implementing integration, and for unique collection re-	Supports all capabilities available with the code.	Depends on the implementation	High
Azure Functions Best for high-volume cloud sources, and for unique collection require-	Supports all capabilities available with the code.	Yes	High; requires programming knowledge

https://docs.microsoft.com/en-us/azure/sentinel/create-custom-connector

Configure data connectors by using Azure Policy

The configuration of some connectors of this type is managed by Azure Policy. Select the Azure Policy tab below for instructions. For the other connectors of this type, select the Standalone tab.

Prerequisites
To ingest data into Microsoft Sentinel:

- You must have read and write permissions on the Microsoft Sentinel workspace.
- To use Azure Policy to apply a log streaming policy to your resources, you must have the Owner role for the policy assignment scope.

Instructions
Connectors of this type use Azure Policy to apply a single diagnostic settings configuration to a collection of resources of a single type, defined as a scope. You can see the log types ingested from a given resource type on the left side of the connector page for that resource, under Data types.

1. From the Microsoft Sentinel navigation menu, select **Data connectors**.
2. Select your resource type from the data connectors gallery, and then **select Open Connector Page on the preview pane**.
3. In the Configuration section of the connector page, expand any expanders you see there and select the **Launch Azure Policy Assignment** wizard button.

The policy assignment wizard opens, ready to create a new policy, with a policy name pre-populated.

a. In the **Basics** tab, select the button with the three dots under Scope to choose your subscription (and, optionally, a resource group). You can also add a description.
b. In the **Parameters** tab:
   - Clear the **Only show parameters that require input** check box.
   - If you see **Effect** and **Setting name** fields, leave them as is.
   - Choose your Microsoft Sentinel workspace from the **Log Analytics workspace** drop-down list.
   - The remaining drop-down fields represent the available diagnostic log types. Leave marked as "True" all the log types you want to ingest.
c. The policy will be applied to resources added in the future. To apply the policy on your existing resources as well, select the **Remediation tab** and mark the **Create a remediation task** check box.
d. In the **Review + create** tab, click **Create**. Your policy is now assigned to the scope you chose.

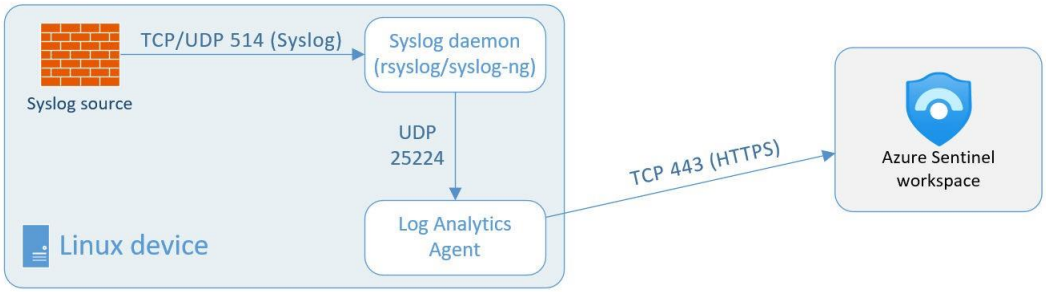
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-windows-microsoft-services

Design and configure Syslog and CEF event collections

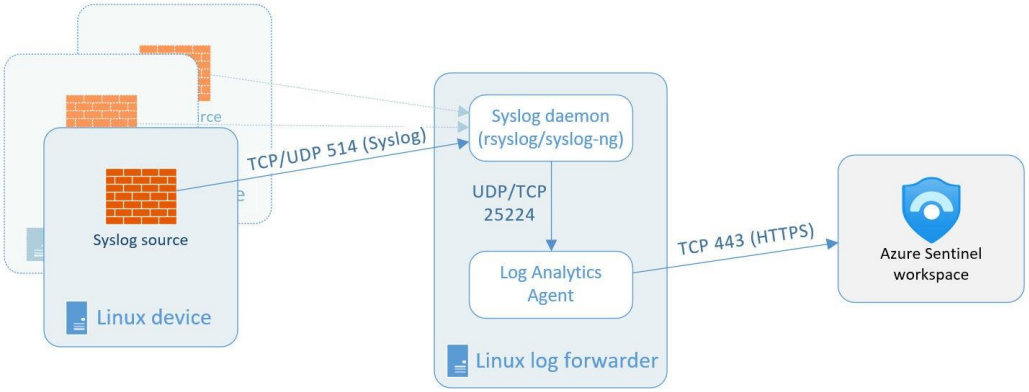
Syslog is an event logging protocol that is common to Linux. You can use the Syslog daemon built into Linux devices and appliances to collect local events of the types you specify, and have it send those events to Microsoft Sentinel using the Log Analytics agent for Linux (formerly known as the OMS agent).

Architecture

When the Log Analytics agent is installed on your VM or appliance, the installation script configures the local Syslog daemon to forward messages to the agent on UDP port 25224. After receiving the messages, the agent sends them to your Log Analytics workspace over HTTPS, where they are ingested into the Syslog table in Microsoft Sentinel > Logs.



For some device types that don't allow local installation of the Log Analytics agent, the agent can be installed instead on a dedicated Linux-based log forwarder. The originating device must be configured to send Syslog events to the Syslog daemon on this forwarder instead of the local daemon. The Syslog daemon on the forwarder sends events to the Log Analytics agent over UDP. If this Linux forwarder is expected to collect a high volume of Syslog events, its Syslog daemon sends events to the agent over TCP instead. In either case, the agent then sends the events from there to your Log Analytics workspace in Microsoft Sentinel.



•

There are three steps to configuring Syslog collection:

- **Configure your Linux device or appliance**. This refers to the device on which the Log Analytics agent will be installed, whether it is the same device that originates the events or a log collector that will forward them.

- **Configure your application's logging settings** corresponding to the location of the Syslog daemon that will be sending events to the agent.

- **Configure the Log Analytics agent itself**. This is done from within Microsoft Sentinel, and the configuration is sent to all installed agents.

https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

Design and Configure Windows Security events collections

Microsoft Sentinel can apply machine learning (ML) to Security events data to identify anomalous Remote Desktop Protocol (RDP) login activity. Scenarios include:

- **Unusual IP** - the IP address has rarely or never been observed in the last 30 days

- **Unusual geo-location** - the IP address, city, country, and ASN have rarely or never been observed in the last 30 days

- **New user** - a new user logs in from an IP address and geo-location, both or either of which were not expected to be seen based on data from the 30 days prior.

Configuration instructions

1. You must be collecting RDP login data (Event ID 4624) through the **Security events** or **Windows Security Events** data connectors. Make sure you have selected an event set besides "None", or created a data collection rule that includes this event ID, to stream into Microsoft Sentinel.

2. From the Microsoft Sentinel portal, select **Analytics**, and then select the **Rule templates** tab. Choose the **(Preview) Anomalous RDP Login Detection** rule, and move the **Status** slider to **Enabled**.

https://docs.microsoft.com/en-us/azure/sentinel/data-connectors-reference#windows-security-events-via-ama

Configure custom threat intelligence connectors

Many organizations use threat intelligence platform (TIP) solutions to aggregate threat indicator feeds from a variety of sources, to curate the data within the platform, and then to choose which threat indicators to apply to various security solutions such as network devices, EDR/XDR solutions, or SIEMs such as Microsoft Sentinel. The Threat Intelligence Platforms data connector allows you to use these solutions to import threat indicators into Microsoft Sentinel.

Because the TIP data connector works with the Microsoft Graph Security tiIndicators API to accomplish this, you can use the connector to send indicators to Microsoft Sentinel (and to other Microsoft security solutions like Microsoft 365 Defender) from any other custom threat intelligence platform that can communicate with that API.

Follow these steps to import threat indicators to Microsoft Sentinel from your integrated TIP or custom threat intelligence solution:

1. Obtain an Application ID and Client Secret from your Azure Active Directory
2. Input this information into your TIP solution or custom application
3. Enable the Threat Intelligence Platforms data connector in Microsoft Sentinel

https://docs.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence-ti

Microsoft Sentinel provides a wide range of built-in connectors for Azure services and external solutions, and also supports ingesting data from some sources without a dedicated connector. If you're unable to connect your data source to Microsoft Sentinel using any of the existing solutions available, consider creating your own data source connector.

Custom Connector Methods

Codeless Connector Platform (CCP)

- Log Analytics Agent
- Logstash
- Logic Apps
- PowerShell
- Log Analytics API
- Azure Functions

https://docs.microsoft.com/en-us/azure/sentinel/create-custom-connector

Create custom logs in Azure Log Analytics to store custom data

Azure Monitor stores log data in a Log Analytics workspace, which is an Azure resource and a container where data is collected, aggregated, and serves as an administrative boundary. While you can deploy one or more workspaces in your Azure subscription, there are several considerations you should understand in order to ensure your initial deployment is following our guidelines to provide you with a cost effective, manageable, and scalable deployment meeting your organization's needs.

Data in a workspace is organized into tables, each of which stores different kinds of data and has its own unique set of properties based on the resource generating the data. Most data sources will write to their own tables in a Log Analytics workspace.

A Log Analytics workspace provides:

- A geographic location for data storage.
- Data isolation by granting different users access rights following one of our recommended design strategies.
- Scope for configuration of settings like pricing tier, retention, and data capping.

Workspaces are hosted on physical clusters. By default, the system is creating and managing these clusters. Customers that ingest more than 4TB/day are expected to create their own dedicated clusters for their workspaces - it enables them better control and higher ingestion rate.
This article provides a detailed overview of the design and migration considerations, access control overview, and an understanding of the design implementations we recommend for your IT organization.

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/design-logs-deployment

Manage Microsoft Sentinel analytics rules

Design and configure analytics rules

After you've connected your data sources to Microsoft Sentinel, you'll want to be notified when something suspicious occurs. That's why Microsoft Sentinel provides out-of-the-box, built-in templates to help you create threat detection rules.

Use built-in analytics rules

This procedure describes how to use built-in analytics rules templates.

To use built-in analytics rules:

1.In the Microsoft Sentinel > Analytics > Rule templates page, select a template name, and then select the Create rule button on the details pane to create a new active rule based on that template.

Each template has a list of required data sources. When you open the template, the data sources are automatically checked for availability. If there is an availability issue, the Create rule button may be disabled, or you may see a warning to that effect.

2.Selecting Create rule opens the rule creation wizard based on the selected template. All the details are autofilled, and with the Scheduled or Microsoft security templates, you can customize the logic and other rule settings to better suit your specific needs. You can repeat this process to create additional rules based on the built-in template. After following the steps in the rule creation wizard to the end, you will have finished creating a rule based on the template. The new rules will appear in the Active rules tab.

https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-built-in

Create custom analytics rules to detect threats

After connecting your data sources to Microsoft Sentinel, create custom analytics rules to help discover threats and anomalous behaviors in your environment.

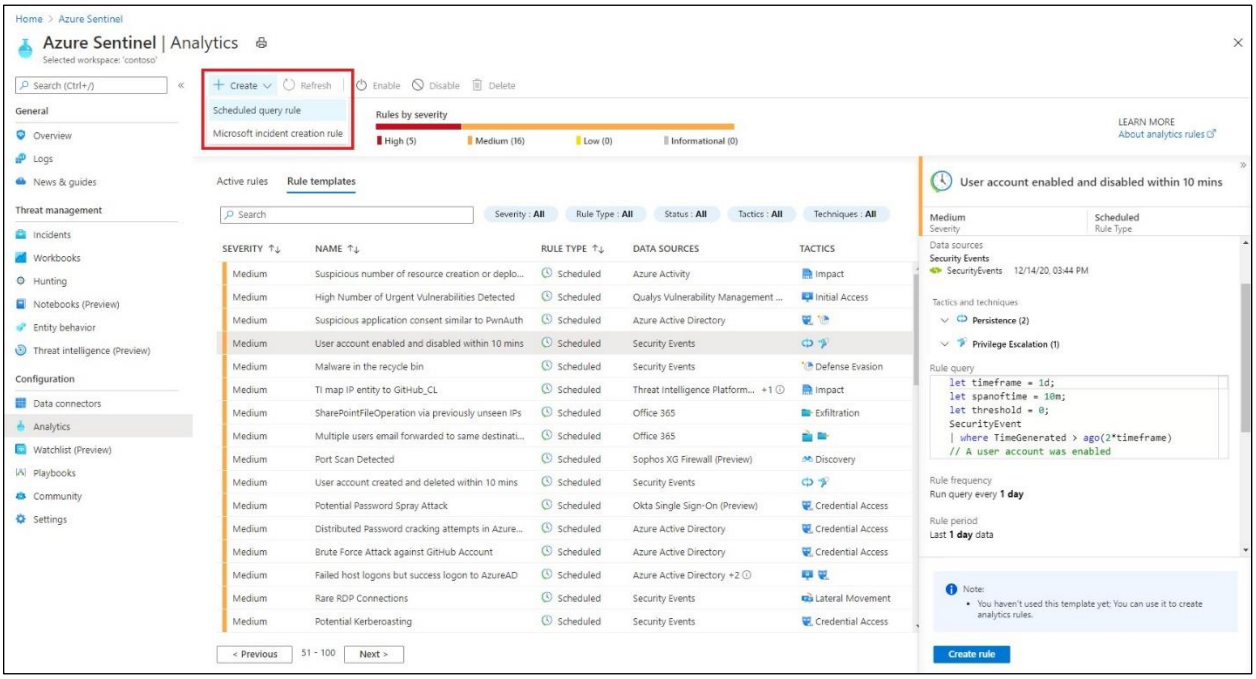
Analytics rules search for specific events or sets of events across your environment, alert you when certain event thresholds or conditions are reached, generate incidents for your SOC to triage and investigate, and respond to threats with automated tracking and remediation processes.

- ✓Create analytics rules
- ✓Define how events and alerts are processed
- ✓Define how alerts and incidents are generated
- ✓Choose automated threat responses for your rules

Create a custom analytics rule with a scheduled query

From the Microsoft Sentinel navigation menu, select Analytics.

In the action bar at the top, select +Create and select Scheduled query rule. This opens the Analytics rule wizard.



- Provide a unique Name and a Description.
- In the Tactics and techniques field, you can choose from among categories of attacks by which to classify the rule. These are based on the tactics and techniques of the MITRE ATT&CK framework.
- Incidents created from alerts that are detected by rules mapped to MITRE ATT&CK tactics and techniques automatically inherit the rule's mapping.
- Set the alert Severity as appropriate.
- When you create the rule, its Status is Enabled by default, which means it will run immediately after you finish creating it. If you don't want it to run immediately, select Disabled, and the rule will be added to your Active rules tab and you can enable it from there when you need it.

https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

Define incident creation logic

To view all analytics rules and detections in Microsoft Sentinel, go to Analytics > Rule templates. This tab contains all the Microsoft Sentinel built-in rules. The alerts generated by these rules will create incidents that you can assign and investigate in your environment.

Rule type	Description
Microsoft security	Microsoft security templates automatically create Microsoft Sentinel incidents from the alerts generated in other Microsoft security solutions, in real time. You can use Microsoft security rules as a template to create new rules with similar logic.
Fusion (some detections in Preview)	Microsoft Sentinel uses the Fusion correlation engine, with its scalable machine learning algorithms, to detect advanced multistage attacks by correlating many low-fidelity alerts and events across multiple products into high-fidelity and actionable incidents. Fusion is enabled by default. Because the logic is hidden and therefore not customizable, you can only create one rule with this template..
Machine learning (ML) behavioral analytics	ML behavioral analytics templates are based on proprietary Microsoft machine learning algorithms, so you cannot see the internal logic of how they work and when they run. Because the logic is hidden and therefore not customizable, you can only create one rule with each template of this type.
Anomaly (Preview)	Anomaly rule templates use machine learning to detect specific types of anomalous behavior. Each rule has its own unique parameters and thresholds, appropriate to the behavior being analyzed. While the configurations of out-of-the-box rules can't be changed or fine-tuned, you can duplicate a rule and then change and fine-tune the duplicate. In such cases, run the duplicate in **Flighting** mode and the original concurrently in **Production** mode. Then compare results, and switch the duplicate to **Production** if and when its fine-tuning is to your liking.

Scheduled	Scheduled analytics rules are based on built-in queries written by Microsoft security experts. You can see the query logic and make changes to it. You can use the scheduled rules template and customize the query logic and scheduling settings to create new rules. Several new scheduled analytics rule templates produce alerts that are correlated by the Fusion engine with alerts from other systems to produce high-fidelity incidents. We recommend being mindful of when you enable a new or edited analytics rule to ensure that the rules will get the new stack of incidents in time. For example, you might want to run a rule in synch with when your SOC analysts begin their workday, and enable the rules then.
Near-real-time (NRT) (Preview)	NRT rules are limited set of scheduled rules, designed to run once every minute, in order to supply you with information as up-to-the-minute as possible. They function mostly like scheduled rules and are configured similarly, with some limitations.

https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-built-in

Configure Security Orchestration Automation and Response (SOAR) in Microsoft Sentinel

Create Microsoft Sentinel playbooks

A playbook is a collection of these remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help **automate and orchestrate your threat response**; it can be run manually or set to run automatically in response to specific alerts or incidents, when triggered by an analytics rule or an automation rule, respectively.

For example, if an account and machine are compromised, a playbook can isolate the machine from the network and block the account by the time the SOC team is notified of the incident.

Playbooks can be used within the subscription to which they belong, but the **Playbooks** tab (in the **Automation** blade) displays all the playbooks available across any selected subscriptions.

A playbook template is a pre-built, tested, and ready-to-use workflow that can be customized to meet your needs. Templates can also serve as a reference for best practices when developing playbooks from scratch, or as inspiration for new automation scenarios.

Playbook templates are not active playbooks themselves, until you create a playbook (an editable copy of the template) from them.

You can get playbook templates from the following sources:

- The **Playbook templates** tab (under **Automation**) presents the leading scenarios contributed by the Microsoft Sentinel community. Multiple active playbooks can be created from the same template.
- When a new version of the template is published, the active playbooks created from that template (in the **Playbooks** tab) will be labeled with a notification that an update is available.
- Playbook templates can also be obtained as part of a Microsoft Sentinel solution in the context of a specific product. The deployment of the solution produces active playbooks.
- The Microsoft Sentinel GitHub repository contains many playbook templates. They can be deployed to an Azure subscription by selecting the **Deploy to Azure** button.

Technically, a playbook template is an ARM template which consists of several resources: an Azure Logic Apps workflow and API connections for each connection involved.

https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

Configure rules and incidents to trigger playbooks

Playbooks can be run either manually or automatically.

Running them manually means that when you get an alert, you can choose to run a playbook on-demand as a response to the selected alert. Currently this feature is generally available for alerts, and in preview for incidents.

Running them automatically means to set them as an automated response in an analytics rule (for alerts), or as an action in an automation rule (for incidents)

Set an automated response

Security operations teams can significantly reduce their workload by fully automating the routine responses to recurring types of incidents and alerts, allowing you to concentrate more on unique incidents and alerts, analyzing patterns, threat hunting, and more.

Setting automated response means that every time an analytics rule is triggered, in addition to creating an alert, the rule will run a playbook, which will receive as an input the alert created by the rule.

If the alert creates an incident, the incident will trigger an automation rule which may in turn run a playbook, which will receive as an input the incident created by the alert.

Alert creation automated response

For playbooks that are triggered by alert creation and receive alerts as their inputs (their first step is “When a Microsoft Sentinel Alert is triggered”), attach the playbook to an analytics rule:

1. Edit the analytics rule that generates the alert you want to define an automated response for.
2. Under Alert automation in the Automated response tab, select the playbook or playbooks that this analytics rule will trigger when an alert is created.

Incident creation automated response

For playbooks that are triggered by incident creation and receive incidents as their inputs (their first step is “When a Microsoft Sentinel Incident is triggered”), create an automation rule and define a Run playbook action in it. This can be done in 2 ways:

Edit the analytics rule that generates the incident you want to define an automated response for. Under Incident automation in the Automated response tab, create an automation rule. This will create a automated response only for this analytics rule.

From the Automation rules tab in the Automation blade, create a new automation rule and specify the appropriate conditions and desired actions. This automation rule will be applied to any analytics rule that fulfills the specified conditions.

https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

Use playbooks to remediate threats

Playbooks are collections of procedures that can be run from Microsoft Sentinel in response to an alert or incident. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively. It can also be run manually on-demand.

Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps, which means that you get all the power, customizability, and built-in templates of Logic Apps. Each playbook is created for the specific subscription to which it belongs, but the Playbooks display shows you all the playbooks available across any selected subscriptions.

For example, if you want to stop potentially compromised users from moving around your network and stealing information, you can create an automated, multifaceted response to incidents generated by rules that detect compromised users. You start by creating a playbook that takes the following actions:

1. When the playbook is called by an automation rule passing it an incident, the playbook opens a ticket in ServiceNow or any other IT ticketing system.
2. It sends a message to your security operations channel in Microsoft Teams or Slack to make sure your security analysts are aware of the incident.
3. It also sends all the information in the incident in an email message to your senior network admin and security admin. The email message will include Block and Ignore user option buttons.
4. The playbook waits until a response is received from the admins, then continues with its next steps.
5. If the admins choose Block, it sends a command to Azure AD to disable the user, and one to the firewall to block the IP address.
6. If the admins choose Ignore, the playbook closes the incident in Microsoft Sentinel, and the ticket in ServiceNow.

In order to trigger the playbook, you'll then create an automation rule that runs when these incidents are generated. That rule will take these steps:

1. The rule changes the incident status to Active.
2. It assigns the incident to the analyst tasked with managing this type of incident.
3. It adds the "compromised user" tag.
4. Finally, it calls the playbook you just created. (Special permissions are required for this step.)

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Use playbooks to manage incidents

You use a playbook to respond to an incident by creating an automation rule that will run when the incident is generated, and in turn it will call the playbook.

To create an automation rule:

1. From the **Automation** blade in the Microsoft Sentinel navigation menu, select **Create** from the top menu and then **Add new rule**.
2. The **Create new automation rule** panel opens. Enter a name for your rule.
3. If you want the automation rule to take effect only on certain analytics rules, specify which ones by modifying the **If Analytics rule name** condition.
4. Add any other conditions you want this automation rule's activation to depend on. Click **Add condition** and choose conditions from the drop-down list. The list of conditions is populated by alert detail and entity identifier fields.
5. Choose the actions you want this automation rule to take. Available actions include **Assign owner, Change status, Change severity, Add tags,** and **Run playbook**. You can add as many actions as you like.
6. If you add a **Run playbook** action, you will be prompted to choose from the drop-down list of available playbooks. Only playbooks that start with the **incident trigger** can be run from automation rules, so only they will appear in the list.
7. Set an expiration date for your automation rule if you want it to have one.
8. Enter a number under **Order** to determine where in the sequence of automation rules this rule will run.
9. Click **Apply**. You're done!

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Use playbooks across Microsoft Defender solutions

Microsoft Sentinel's Microsoft 365 Defender incident integration allows you to stream all Microsoft 365 Defender incidents into Microsoft Sentinel and keep them synchronized between both portals. Incidents from Microsoft 365 Defender (formerly known as Microsoft Threat Protection or MTP) include all associated alerts, entities, and relevant information, providing you with enough context to perform triage and preliminary investigation in Microsoft Sentinel. Once in Sentinel, incidents will remain bi-directionally synced with Microsoft 365 Defender, allowing you to take advantage of the benefits of both portals in your incident investigation.

This integration gives Microsoft 365 security incidents the visibility to be managed from within Microsoft Sentinel, as part of the primary incident queue across the entire organization, so you can see – and correlate – Microsoft 365 incidents together with those from all of your other cloud and on-premises systems. At the same time, it allows you to take advantage of the unique strengths and capabilities of Microsoft 365 Defender for in-depth investigations and a Microsoft 365-specific experience across the Microsoft 365 ecosystem. Microsoft 365 Defender enriches and groups alerts from multiple Microsoft 365 products, both reducing the size of the SOC's incident queue and shortening the time to resolve. The component services that are part of the Microsoft 365 Defender stack are:

- **Microsoft Defender for Endpoint** (formerly Microsoft Defender ATP)
- **Microsoft Defender for Identity** (formerly Azure ATP)
- **Microsoft Defender for Office 365** (formerly Office 365 ATP)
- **Microsoft Defender for Cloud Apps** (formerly Microsoft Cloud App Security)

In addition to collecting alerts from these components, Microsoft 365 Defender generates alerts of its own. It creates incidents from all of these alerts and sends them to Microsoft Sentinel.

https://docs.microsoft.com/en-us/azure/sentinel/microsoft-365-defender-sentinel-integration

Manage Microsoft Sentinel Incidents

Investigate incidents in Microsoft Sentinel

This article helps you investigate incidents with Microsoft Sentinel. After you connected your data sources to Microsoft Sentinel, you want to be notified when something suspicious happens. To enable you to do this, Microsoft Sentinel lets you create advanced alert rules, that generate incidents that you can assign and investigate.

This article covers:

- ✓ Investigate incidents
- ✓ Use the investigation graph
- ✓ Respond to threats

An incident can include multiple alerts. It's an aggregation of all the relevant evidence for a

specific investigation. An incident is created based on analytics rules that you created in the **Analytics** page. The properties related to the alerts, such as severity and status, are set at the incident level. After you let Microsoft Sentinel know what kinds of threats you're looking for and how to find them, you can monitor detected threats by investigating incidents.

How to investigate incidents

1. Select Incidents. The Incidents page lets you know how many incidents you have, how many are open, how many you've set to In progress, and how many are closed. For each incident, you can see the time it occurred, and the status of the incident. Look at the severity to decide which incidents to handle first.

2. You can filter the incidents as needed, for example by status or severity. For more information, see Search for incidents.

3. To begin an investigation, select a specific incident. On the right, you can see detailed information for the incident including its severity, summary of the number of entities involved, the raw events that triggered this incident, the incident's unique ID, and any mapped MITRE ATT&CK tactics or techniques.

4. To view more details about the alerts and entities in the incident, select View full details in the incident page and review the relevant tabs that summarize the incident information.

5. If you're actively investigating an incident, it's a good idea to set the incident's status to In progress until you close it.

6. Incidents can be assigned to a specific user. For each incident you can assign an owner, by setting the Incident owner field. All incidents start as unassigned. You can also add comments so that other analysts will be able to understand what you investigated and what your concerns are around the incident.

7.Select Investigate to view the investigation map.

https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

Triage incidents in Microsoft Sentinel

As a Security Operations Center (SOC) manager, you need to have overall efficiency metrics and measures at your fingertips to gauge the performance of your team. You'll want to see incident operations over time by many different criteria, like severity, MITRE tactics, mean time to triage, mean time to resolve, and more. Microsoft Sentinel now makes this data

available to you with the new Security Incident table and schema in Log Analytics and the accompanying Security operations efficiency workbook. You'll be able to visualize your team's performance over time and use this insight to improve efficiency. You can also write and use your own KQL queries against the incident table to create customized workbooks that fit your specific auditing needs and KPIs.

Respond to incidents in Microsoft Sentinel

Automation rules are a new concept in Microsoft Sentinel. This feature allows users to centrally manage the automation of incident handling. Besides letting you assign playbooks to incidents (not just to alerts as before), automation rules also allow you to automate responses for multiple analytics rules at once, automatically tag, assign, or close incidents without the need for playbooks, and control the order of actions that are executed. Automation rules will streamline automation use in Microsoft Sentinel and will enable you to simplify complex workflows for your incident orchestration processes.

Components
Automation rules are made up of several components:

Trigger
Automation rules are triggered by the creation of an incident.

To review – incidents are created from alerts by analytics rules, of which there are several types, as explained in the tutorial Detect threats with built-in analytics rules in Microsoft Sentinel.

Conditions
Complex sets of conditions can be defined to govern when actions (see below) should run. These conditions are typically based on the states or values of attributes of incidents and their entities, and they can include AND/OR/NOT/CONTAINS operators.

Actions
Actions can be defined to run when the conditions (see above) are met. You can define many actions in a rule, and you can choose the order in which they'll run (see below). The following actions can be defined using automation rules, without the need for the advanced functionality of a playbook:

- Changing the status of an incident, keeping your workflow up to date.
- When changing to "closed," specifying the closing reason and adding a comment. This helps you keep track of your performance and effectiveness, and fine-tune to reduce false positives.

- Changing the severity of an incident – you can reevaluate and reprioritize based on the presence, absence, values, or attributes of entities involved in the incident.

- Assigning an incident to an owner – this helps you direct types of incidents to the personnel best suited to deal with them, or to the most available personnel.

- Adding a tag to an incident – this is useful for classifying incidents by subject, by attacker, or by any other common denominator.

Also, you can define an action to **run a playbook**, in order to take more complex response actions, including any that involve external systems. **Only** playbooks activated by the **incident trigger** are available to be used in automation rules. You can define an action to include multiple playbooks, or combinations of playbooks and other actions, and the order in which they will run.

https://docs.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules

Investigate multi-workspace incidents

To take full advantage of Microsoft Sentinel's capabilities, Microsoft recommends using a single-workspace environment. However, there are some use cases that require having several workspaces, in some cases – for example, that of a Managed Security Service Provider (MSSP) and its customers – across multiple tenants. Multiple workspace view lets you see and work with security incidents across several workspaces at the same time, even across tenants, allowing you to maintain full visibility and control of your organization's security responsiveness.

Working with incidents

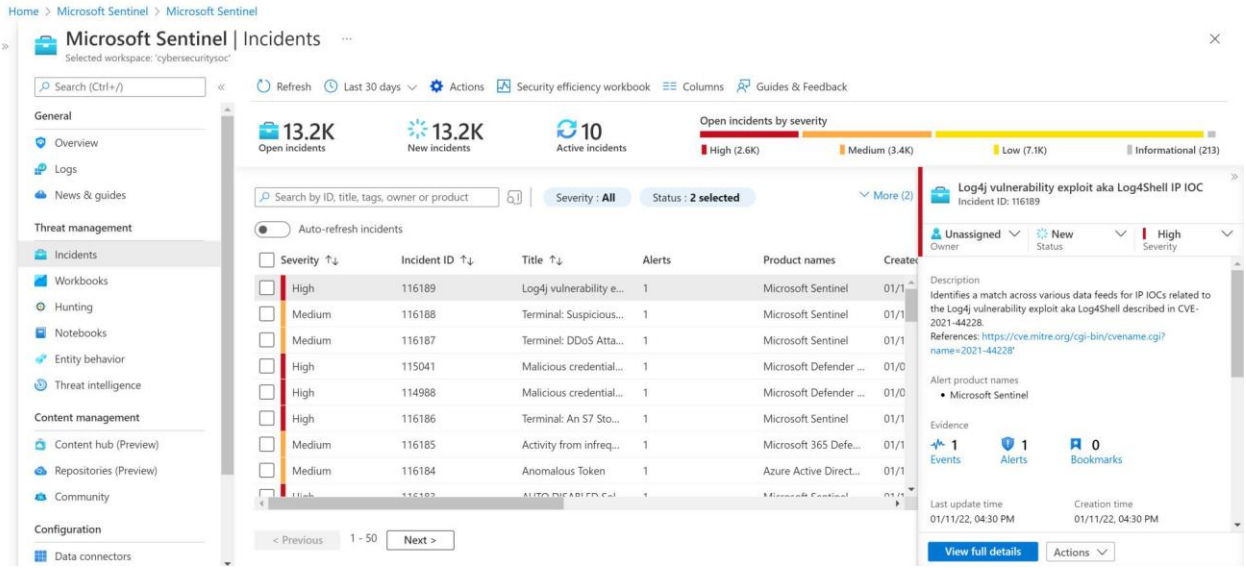
Multiple workspace view is currently available only for incidents. This page looks and functions in most ways like the regular Incidents page, with the following important differences:

- The counters at the top of the page - Open incidents, New incidents, Active incidents, etc. - show the numbers for all of the selected workspaces collectively.

- You'll see incidents from all of the selected workspaces and directories (tenants) in a single unified list. You can filter the list by workspace and directory, in addition to the filters from the regular Incidents screen.

- You'll need to have read and write permissions on all the workspaces from which you've selected incidents. If you have only read permissions on some workspaces, you'll see warning messages if you select incidents in those workspaces. You won't be able to modify those incidents or any others you've selected together with those (even if you do have permissions for the others).

- If you choose a single incident and click View full details or Actions > Investigate, you will from then on be in the data context of that incident's workspace and no others.



Identify advanced threats with User and Entity Behavior Analytics (UEBA)

Identifying threats inside your organization and their potential impact - whether a compromised entity or a malicious insider - has always been a time-consuming and labor-intensive process. Sifting through alerts, connecting the dots, and active hunting all add up to massive amounts of time and effort expended with minimal returns, and the possibility of sophisticated threats simply evading discovery. Particularly elusive threats like zero-day, targeted, and advanced persistent threats can be the most dangerous to your organization, making their detection all the more critical.

The UEBA capability in Microsoft Sentinel eliminates the drudgery from your analysts' workloads and the uncertainty from their efforts, and delivers high-fidelity, actionable intelligence, so they can focus on investigation and remediation.

As Microsoft Sentinel collects logs and alerts from all of its connected data sources, it analyzes them and builds baseline behavioral profiles of your organization's entities (such as users, hosts, IP addresses, and applications) across time and peer group horizon. Using a variety of techniques and machine learning capabilities, Microsoft Sentinel can then identify anomalous activity and help you determine if an asset has been compromised. Not only that, but it can also figure out the relative sensitivity of particular assets, identify peer groups of assets, and evaluate the potential impact of any given compromised asset (its "blast radius"). Armed with this information, you can effectively prioritize your investigation and incident handling.

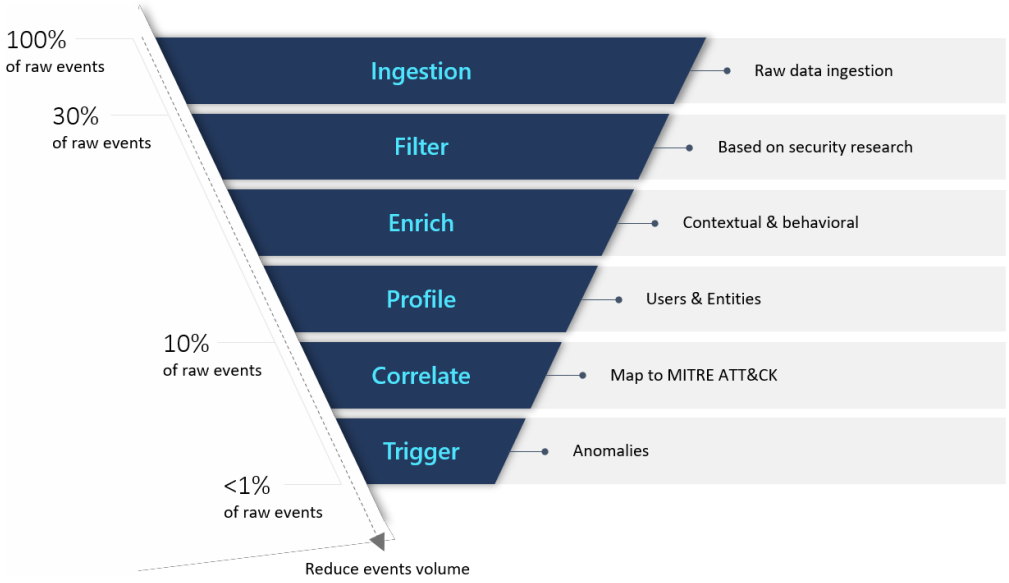
Security-driven analytics

Inspired by Gartner's paradigm for UEBA solutions, Microsoft Sentinel provides an "outside-in" approach, based on three frames of reference:

Use cases: By prioritizing for relevant attack vectors and scenarios based on security research aligned with the MITRE ATT&CK framework of tactics, techniques, and sub-techniques that puts various entities as victims, perpetrators, or pivot points in the kill chain; Microsoft Sentinel focuses specifically on the most valuable logs each data source can provide.

Data Sources: While first and foremost supporting Azure data sources, Microsoft Sentinel thoughtfully selects third-party data sources to provide data that matches our threat scenarios.

Analytics: Using various machine learning (ML) algorithms, Microsoft Sentinel identifies anomalous activities and presents evidence clearly and concisely in the form of contextual enrichments, some examples of which appear below.



Microsoft Sentinel presents artifacts that help your security analysts get a clear understanding of anomalous activities in context, and in comparison with the user's baseline profile. Actions performed by a user (or a host, or an address) are evaluated contextually, where a "true" outcome indicates an identified anomaly:

- across geographical locations, devices, and environments.
- across time and frequency horizons (compared to user's own history).
- as compared to peers' behavior.
- as compared to organization's behavior.

https://docs.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics

Use Microsoft Sentinel workbooks to analyze and interpret data

Activate and customize Microsoft Sentinel workbook templates

Use built-in workbooks

- ✓Go to Workbooks and then select Templates to see the full list of Microsoft Sentinel built-in workbooks.
- ✓Select View template to see the template populated with your data.
- ✓To edit the workbook, select Save, and then select the location where you want to save the JSON file for the template.
- ✓Select View saved workbook.

https://docs.microsoft.com/en-us/azure/sentinel/monitor-your-data

Create custom workbooks

Create new workbook

1. Go to Workbooks and then select Add workbook to create a new workbook from scratch.
2. To edit the workbook, select Edit, and then add text, queries, and parameters as necessary. For more information on how to customize the workbook, see how to Create interactive reports with Azure Monitor Workbooks.
3. When building a query, make sure the Data source is set to Logs and Resource type is set to Log Analytics, and then choose the relevant workspace(s).
4. After you create your workbook, save the workbook, making sure you save it under the subscription and resource group of your Microsoft Sentinel workspace.
5. If you want to let others in your organization use the workbook, under Save to select Shared reports. If you want this workbook to be available only to you, select My reports.
6. To switch between workbooks in your workspace, select Open in the toolbar of any workbook. The screen switches to a list of other workbooks you can switch to.

https://docs.microsoft.com/en-us/azure/sentinel/monitor-your-data

Configure advanced visualizations

In this article, you will learn how to quickly be able to view and monitor what's happening across your environment using Microsoft Sentinel. After you connected your data sources to Microsoft Sentinel, you get instant visualization and analysis of data so that you can know what's happening across all your connected data sources. Microsoft Sentinel gives you workbooks that provide you with the full power of tools already available in Azure as well as tables and charts that are built in to provide you with analytics for your logs and queries. You can either use built-in workbooks or create a new workbook easily, from scratch or based on an existing workbook.

To visualize and get analysis of what's happening on your environment, first, take a look at the overview dashboard to get an idea of the security posture of your organization. You can click on each element of these tiles to drill down to the raw data from which they are created. To help you reduce noise and minimize the number of alerts you have to review and investigate, Microsoft Sentinel uses a fusion technique to correlate alerts into incidents. Incidents are groups of related alerts that together create an actionable incident that you can investigate and resolve.

https://docs.microsoft.com/en-us/azure/sentinel/get-visibility

View and analyze Microsoft Sentinel data using workbooks

Once you have connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoption of Azure Monitor Workbooks, which provides versatility in creating custom dashboards. While the Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to create interactive reports with Azure Monitor Workbooks. Microsoft Sentinel allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

This article describes how to visualize your data in Microsoft Sentinel.

- ✓ Use built-in workbooks
- ✓ Create new workbooks

https://docs.microsoft.com/en-us/azure/sentinel/monitor-your-data

Track incident metrics using the security operations efficiency workbook

To complement the SecurityIncidents table, we've provided you an out-of-the-box security operations efficiency workbook template that you can use to monitor your SOC operations. The workbook contains the following metrics:

- ✓ Incident created over time
- ✓ Incidents created by closing classification, severity, owner, and status
- ✓ Mean time to triage
- ✓ Mean time to closure
- ✓ Incidents created by severity, owner, status, product, and tactics over time
- ✓ Time to triage percentiles
- ✓ Time to closure percentiles
- ✓ Mean time to triage per owner
- ✓ Recent activities

✓Recent closing classifications

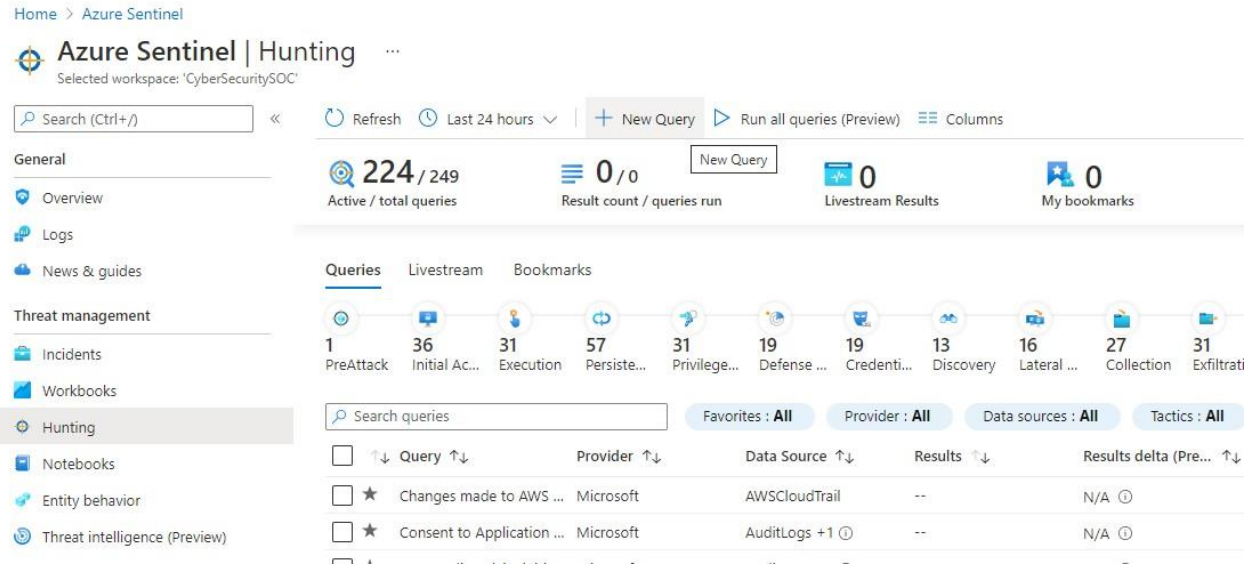
You can find this new workbook template by choosing Workbooks from the Microsoft Sentinel navigation menu and selecting the Templates tab. Choose Security operations efficiency from the gallery and click one of the View saved workbook and View template buttons.

https://docs.microsoft.com/en-us/azure/sentinel/manage-soc-with-incident-metrics

Hunt for threats using the Microsoft Sentinel portal

Create custom hunting queries

Create or modify a query and save it as your own query or share it with users who are in the same tenant.



To create a new query:

1. Select New query.
2. Fill in all the blank fields and select Create.
    a. Create entity mappings by selecting entity types, identifiers and columns.
    b. Map MITRE ATT&CK techniques to your hunting queries by selecting the tactic, technique and sub-technique (if applicable).

https://docs.microsoft.com/en-us/azure/sentinel/hunting

Run hunting queries manually

Kusto Query Language (KQL) is the query language used to perform analysis on data to create Analytics, Workbooks, and perform Hunting in Microsoft Sentinel. Understanding basic KQL statement structure provides the foundation to build more complex statements.

You are a Security Operations Analyst working at a company that is implementing Microsoft Sentinel. You are responsible for performing log data analysis to search for malicious activity, display visualizations, and perform threat hunting. To query log data, you use the Kusto Query Language (KQL).

To learn to write KQL, you start with the basic structure of a KQL statement. The basics include what table to query, how to apply a filter, and how to return specific columns.

The Query window has three primary sections:

- The left area is a reference list of the tables in the environment.
- The middle top area is the Query editor.
- The bottom area is the Query Results.

Before running a query, adjust the time range to scope the data. To change the result columns displayed, select the Columns box, and choose the required columns.

https://docs.microsoft.com/en-us/learn/paths/sc-200-utilize-kql-for-azure-sentinel/

Monitor hunting queries by using Livestream

Use hunting livestream to create interactive sessions that let you test newly created queries as events occur, get notifications from the sessions when a match is found, and launch investigations if necessary. You can quickly create a livestream session using any Log Analytics query.

- **Test newly created queries as events occur**

You can test and adjust queries without any conflicts to current rules that are being actively applied to events. After you confirm these new queries work as expected, it's easy to promote them to custom alert rules by selecting an option that elevates the session to an alert.

- **Get notified when threats occur**

You can compare threat data feeds to aggregated log data and be notified when a match occurs. Threat data feeds are ongoing streams of data that are related to potential or current threats, so the notification might indicate a potential threat to your organization. Create a livestream session instead of a custom alert rule when you want to be notified of a potential issue without the overheads of maintaining a custom alert rule.

- **Launch investigations**

If there is an active investigation that involves an asset such as a host or user, you can view specific (or any) activity in the log data as it occurs on that asset. You can be notified when that activity occurs.

https://docs.microsoft.com/en-us/azure/sentinel/livestream

Perform advanced hunting with notebooks

The foundation of Microsoft Sentinel is the data store; it combines high-performance querying, dynamic schema, and scales to massive data volumes. The Azure portal and all Microsoft Sentinel tools use a common API to access this data store.

The same API is also available for external tools such as Jupyter notebooks and Python. While many common tasks can be carried out in the portal, Jupyter extends the scope of what you can do with this data. It combines full programmability with a huge collection of libraries for machine learning, visualization, and data analysis. These attributes make Jupyter a compelling tool for security investigation and hunting.

For example, use notebooks to:

- Perform analytics that aren't provided out-of-the box in Microsoft Sentinel, such as some Python machine learning features
- Create data visualizations that aren't provided out-of-the box in Microsoft Sentinel, such as custom timelines and process trees
- Integrate data sources outside of Microsoft Sentinel, such as an on-premises data set.

https://docs.microsoft.com/en-us/azure/sentinel/notebooks

Track query results with bookmarks

If you find something that urgently needs to be addressed while hunting in your logs, you can easily create a bookmark and either promote it to an incident or add it to an existing incident. For more information about incidents, see Investigate incidents with Microsoft Sentinel.

If you found something worth bookmarking, but that isn't immediately urgent, you can create a bookmark and then revisit your bookmarked data at any time on the Bookmarks tab of the Hunting pane. You can use filtering and search options to quickly find specific data for your current investigation.

You can visualize your bookmarked data by selecting Investigate from the bookmark details. This launches the investigation experience in which you can view, investigate, and visually communicate your findings using an interactive entity-graph diagram and timeline.

https://docs.microsoft.com/en-us/azure/sentinel/bookmarks

Use hunting bookmarks for data investigations

1. In the Azure portal, navigate to Microsoft Sentinel > Threat management > Hunting > Bookmarks tab, and select the bookmark or bookmarks you want to investigate.
2. In the bookmark details, ensure that at least one entity is mapped.
3. Select Investigate to view the bookmark in the investigation graph.

For instructions to use the investigation graph, see Use the investigation graph to deep dive.

https://docs.microsoft.com/en-us/azure/sentinel/bookmarks

Convert a hunting query to an analytical rule

After connecting your data sources to Microsoft Sentinel, create custom analytics rules to help discover threats and anomalous behaviors in your environment.

Analytics rules search for specific events or sets of events across your environment, alert you when certain event thresholds or conditions are reached, generate incidents for your SOC to triage and investigate, and respond to threats with automated tracking and remediation processes.

Create a custom analytics rule with a scheduled query

1. From the Microsoft Sentinel navigation menu, select Analytics.
2. In the action bar at the top, select +Create and select Scheduled query rule. This opens the Analytics rule wizard.

https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom