

Integrate Microsoft Sentinel with Cohesity Data Cloud

Configure the Cohesity Data Cloud to Meet Your Security Requirements

Version 1.3

February 2026

ABSTRACT

The Cohesity Data cloud provides cyber resilience with modern data management and protection capabilities. Integrating it with a Cloud-Native SIEM/SOAR solution further enhances an organization's security operations by providing comprehensive visibility and automated incident response with improved threat detection, resulting in a more robust and efficient security posture.

This guide explains how you can integrate the Cloud-native Microsoft Sentinel platform with Cohesity Data Cloud to enhance the security visibility, investigation, and rapid response of Cohesity incidents to protect the customer-critical data with the Cohesity playbooks and automation capabilities.

Table of Contents

Introduction.....	4
Managing the Alerts without SOC Integration	5
Cohesity Security Integration for Microsoft Sentinel	6
Integrate Ransomware Alerts from Cohesity Data Cloud to Microsoft Sentinel....	7
Set Up Cohesity Data Cloud API Keys	7
<i>Create a Custom Role with Minimum Permissions</i>	<i>7</i>
<i>Create and Copy the API Keys.....</i>	<i>10</i>
Configure Workspace and Resource Group	12
Install Cohesity Security Integration Solution.....	13
Configure Cohesity Data Connectors.....	14
<i>Register Azure Application for Cohesity.....</i>	<i>14</i>
<i>Set Required Permissions to Create Microsoft Sentinel Incidents.....</i>	<i>15</i>
<i>Deploy Cohesity Data Connector</i>	<i>17</i>
Configure the Cohesity Playbooks	26
<i>Cohesity Incident Email Playbook</i>	<i>27</i>
<i>Cohesity Close Helios Incident.....</i>	<i>32</i>
<i>Cohesity Create or Update ServiceNow Incident.....</i>	<i>35</i>
<i>Delete Cohesity Incident Blobs.....</i>	<i>42</i>
<i>Restore From Last Cohesity Snapshot Playbook.....</i>	<i>46</i>
Investigate an Incident.....	50
Prerequisites.....	52
Customer Benefits.....	53
Conclusion.....	54
Appendix A.....	55
Set Required Permissions to Access Playbook	55
Grant KeyVault Permissions	57
Terminology	60

Your Feedback	61
About the Authors.....	61
Document Version History.....	61

Figures

Figure 1: Closed-loop ransomware detection and remediation with integrated Cohesity and Microsoft Sentinel.....	6
Figure 2: Configuration Workflow	7
Figure 3: Cohesity Playbooks use cases.....	26

Introduction

Ransomware attacks have increased exponentially, causing billions in losses, and putting lives at risk while damaging trust and reputations. As cybercriminals get more inventive, they're not only locking up production systems but also destroying backups and stealing sensitive data. This leaves your enterprise with no option but to pay a ransom.

Defense in depth is the key to minimizing risk. It's crucial to have a backup system that reliably and securely makes continuous or frequent backups, protects them from attack, and can immediately and safely put the data online at scale to support forensics and cyber recovery. Cohesity provides unique capabilities in those areas. Security is a team sport; Cohesity incorporates the leading security ecosystem technologies to help identify vulnerabilities in backed up VMs that would let attackers in if recovered, help mask sensitive data, and help detect the presence of attackers before they plant ransomware. Cohesity also applies leading ML-driven classification technology that leverages Natural Language Processing (NLP) methods to automatically discover and classify large sets of data at scale to help minimize risk and improve security posture.

Cohesity gathers rich telemetry collected during backup and applies multiple machine-learning models and algorithms to identify anomalies in the backup data can be your first warning of trouble if your other tools have failed to detect and block the attackers. (For more information, refer to [Accelerate Anomaly Detection with Cohesity](#) whitepaper. Cohesity enhances your organization's ability to react quickly in a coordinated manner by integrating with Microsoft Sentinel.

This solution tears down the silos between your IT and security operations teams to provide faster time for discovery, investigation, and recovery from ransomware attacks.

The coupling of the Cohesity security and data management platform with Microsoft Sentinel detects and aggregates anomaly events before orchestrating threat response, delivering intelligent backup data security analytics to your enterprise. The integrated solution brings data-driven insights from your ITOps and SecOps organizations together, boosting the teamwork required to assess an attack's scope most effectively and quickly remediate the threat.

Managing the Alerts without SOC Integration

The Cohesity platform provides cyber resilience with modern data management and protection capabilities which generates anomaly alerts based on suspicious activity on the Anti Ransomware dashboard. Without leading SOC integration support, organizations may have a few limitations while addressing the alerts:

- **Limited security visibility** – The Cohesity platform primarily focuses on data management and protection, which may result in limited visibility into security events and threats across the organization's IT infrastructure.
- **Incident response** – Security teams may need to investigate and respond to anomaly alerts and incidents, which can be time-consuming, error-prone, and lead to delays in incident resolution.
- **Lack of automation and orchestration** – Integrating a SOAR solution with Cohesity enables organizations to automate and orchestrate security processes and workflows.
- **Compliance and reporting challenges** – Organizations have mandatory regulatory compliance to adhere to gather all infrastructure logs in one centralized location.

Cohesity Security Integration for Microsoft Sentinel

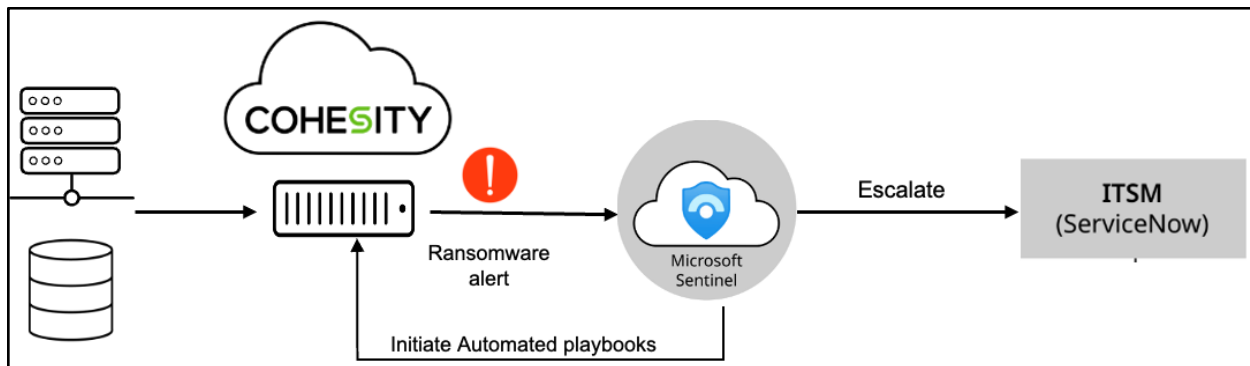
Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. By using the Cohesity Data Cloud integration with Microsoft Sentinel, you get a single solution for attack detection, threat visibility, proactive hunting, and threat response.

You can use this Cohesity Integration for Microsoft Sentinel Solution available on [Cohesity Marketplace](#) to configure automatically sending Cohesity Anomaly alerts directly to Microsoft Sentinel.

From Microsoft Sentinel, security analysts can investigate the incidents as ransomware detection events on the Microsoft Sentinel console, and if needed, initiate a snapshot recovery directly from Microsoft Sentinel or via ServiceNow, escalate the incident, or dismiss the alert.

The integration of Microsoft Sentinel with Cohesity helps accelerate how enterprises discover, investigate, and recover from ransomware attacks while improving IT-SecOps collaboration.

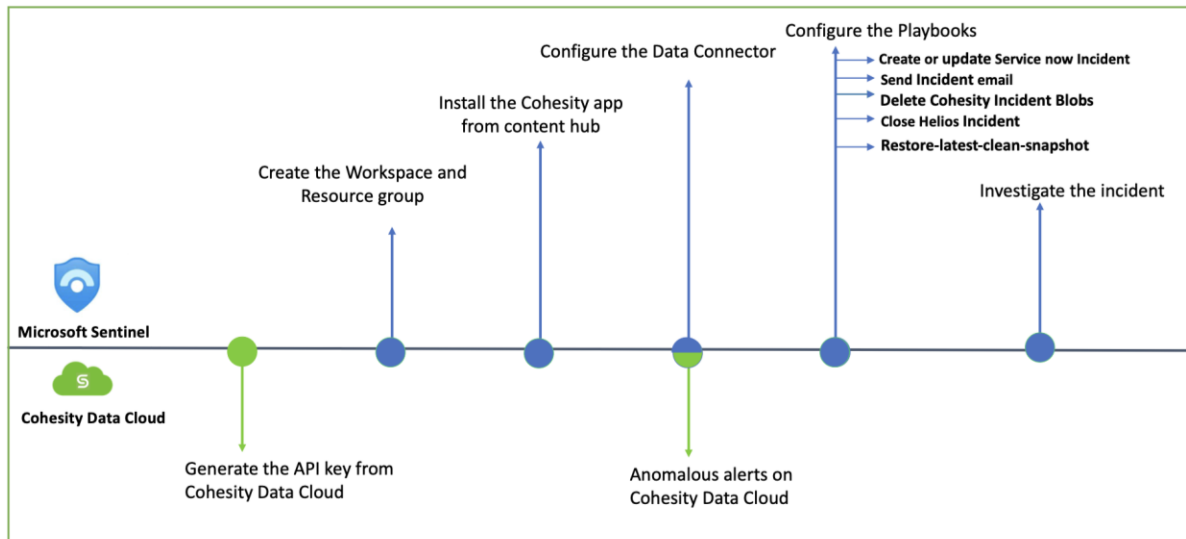
Figure 1: Closed-loop ransomware detection and remediation with integrated Cohesity and Microsoft Sentinel



Integrate Ransomware Alerts from Cohesity Data Cloud to Microsoft Sentinel

You can integrate Cohesity Data Cloud with Microsoft Sentinel to stay updated with the security alerts from your Cohesity environment and immediately respond to a ransomware attack or an incident. To integrate with Microsoft Sentinel, perform the following steps:

Figure 2: Configuration Workflow



Set Up Cohesity Data Cloud API Keys

You can use APIs to access Cohesity Data Cloud and perform your tasks on Cohesity Data Cloud and your local cluster. You must create a role with minimum permissions in Cohesity Helios.

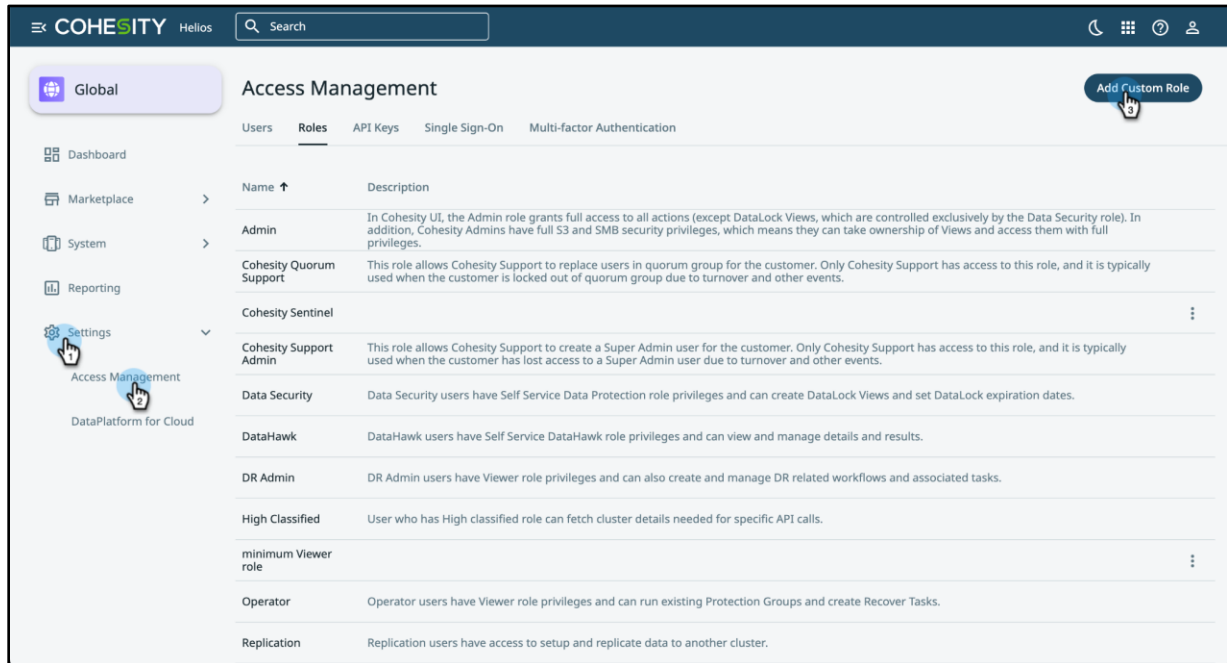
Create a Custom Role with Minimum Permissions

Cohesity Data Cloud allows you to create a role and choose its permissions. However, Cohesity recommends that you create a role with the minimum required permissions for data connection purposes.

To create a role:

1. Log in to [Cohesity Helios](#).
2. From the Global **Dashboard**, navigate to **Settings > Access Management**.

3. Select the **Roles** tab and click **Add Custom Role**.



4. In the **Add Role** page with role permissions options, enter the **Role Name** and a **Description** for the role.

5. To create a role with minimum permissions, select the following permissions:

- View Users
- View API Keys
- View Alert Details
- Allows access to Cohesity UI
- View Protection Groups
- View Protection Policies
- Manage Recover Tasks
- Reporting
- Enable or disable snapshot tagging feature
- Restore from tagged snapshots

The screenshot shows the 'Add Role' configuration page in the COHEXITY interface. The role is named 'Sentinel Analyst Role' and is described as 'MS Sentinel Integration'. The configuration is divided into three main sections: 'Access Management Privileges', 'Helios Privileges', and 'Multi-Cluster Privileges'. Each section has a 'Workflow' dropdown set to 'All' and a 'Privileges' section with various permissions. In 'Access Management Privileges', 'Manage Users' and 'Manage API Key' are checked. In 'Helios Privileges', 'Search Objects' and 'Configure Region' are checked. In 'Multi-Cluster Privileges', 'Unregister clusters' and 'Multi-cluster upgrade' are checked.

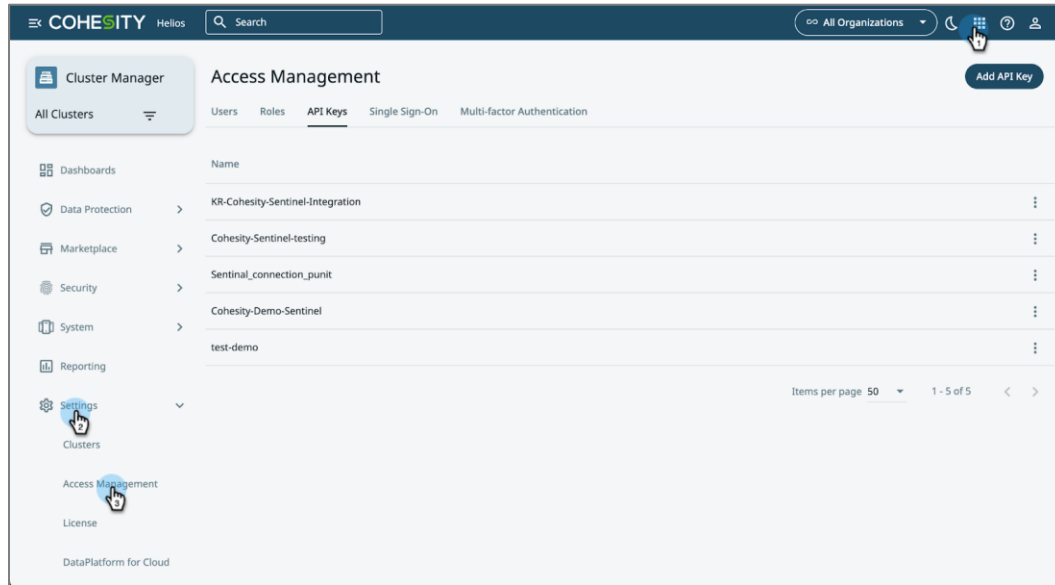
6. Click **Save**. A new role is created successfully.
7. Once the new role is created, you have to assign the created role to a user.
8. You have to log back into Cohesity Data Cloud as this user and then create an API key to authenticate an application.

NOTE: This API key has the minimum permissions because the user role who created this API key has minimum assigned permissions.

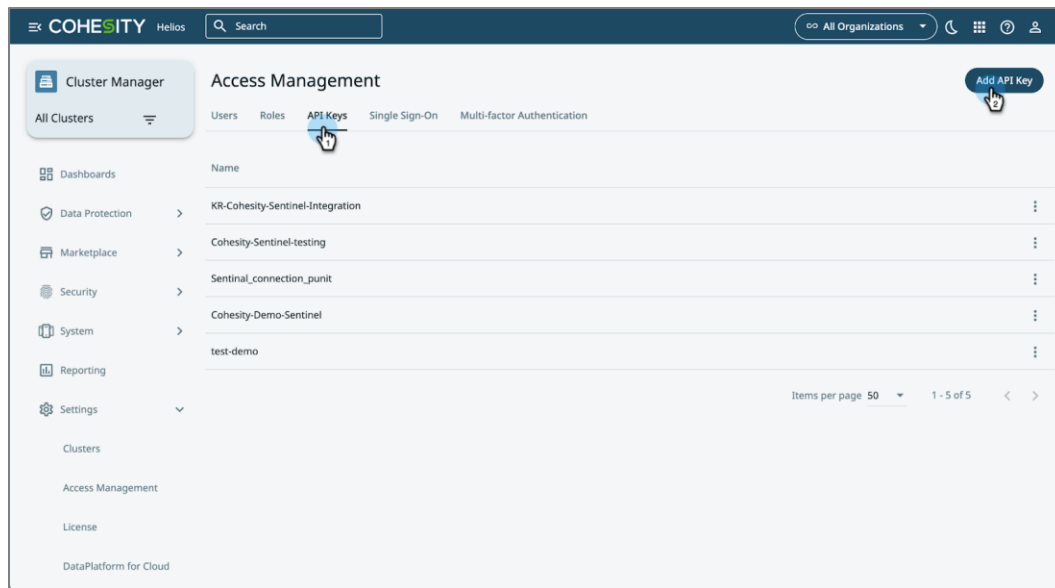
Create and Copy the API Keys

To create and copy the API keys:

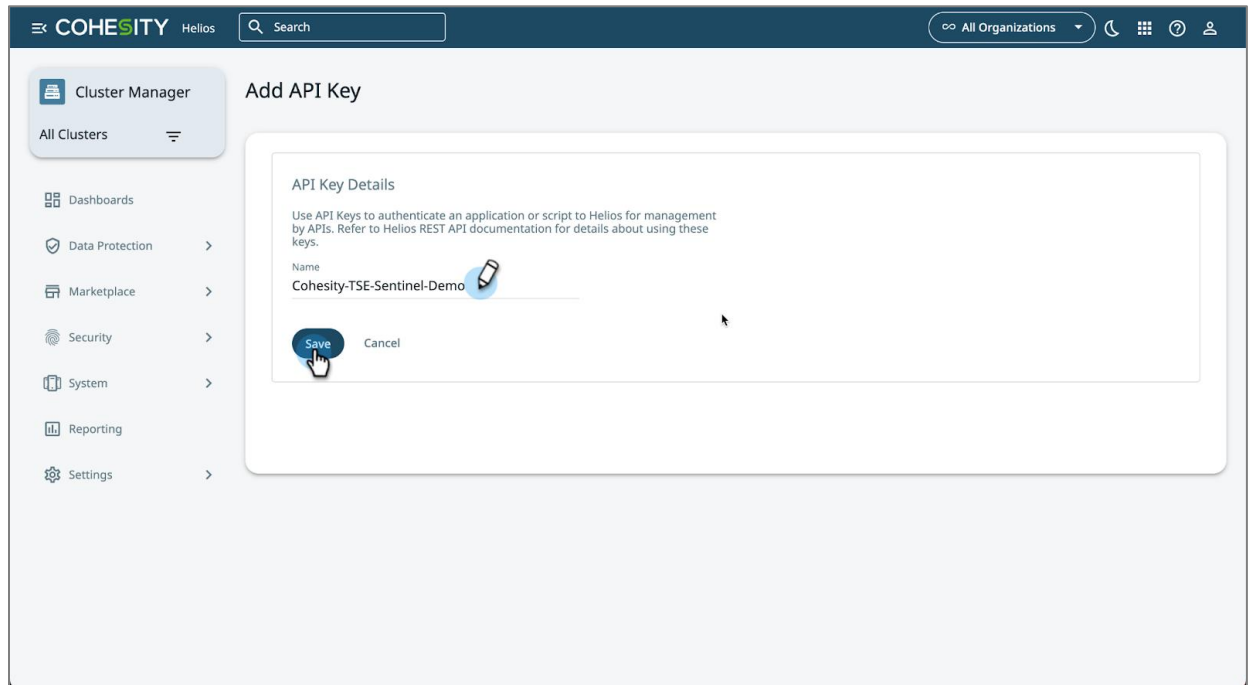
1. Log in to [Cohesity Helios](#).
2. From the **Global Dashboard**, navigate to **Settings > Access Management**.



3. From **Access Management**, select **API Keys >Add API Key**.

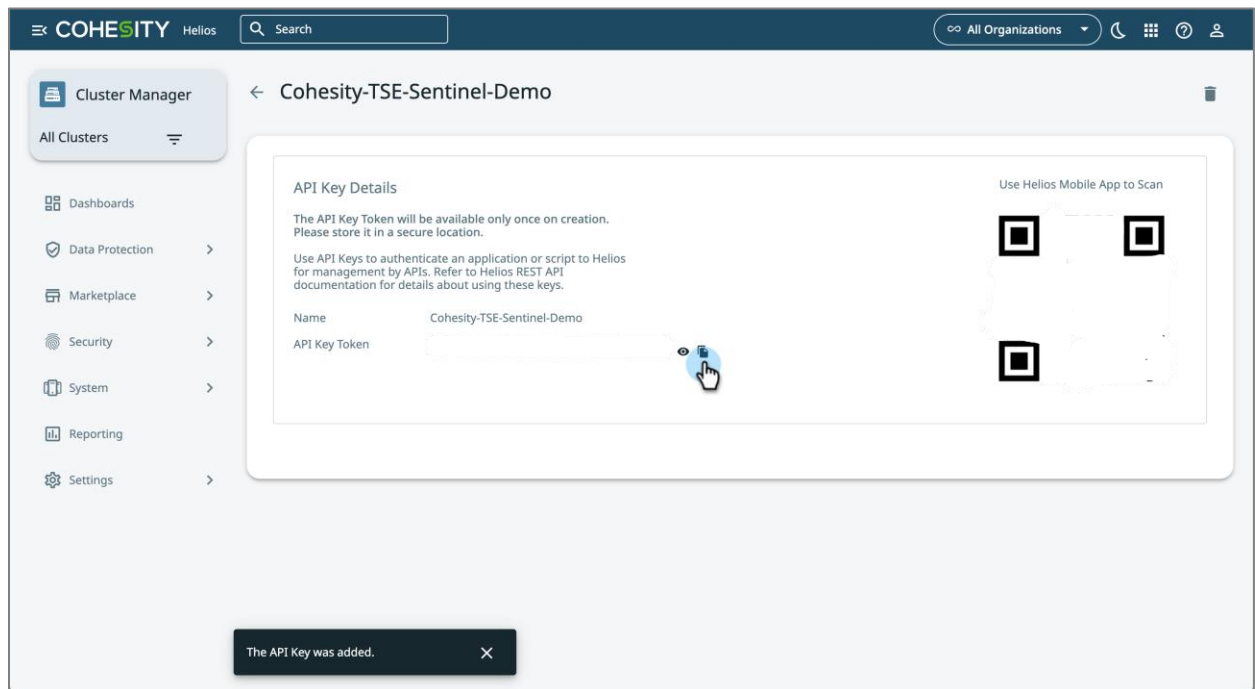


4. Enter a name for the API key and click **Save**.



5. The **API Key Token** is displayed.

NOTE: Ensure to copy and save the API Key token to later add it to the Data Connector page in Microsoft Sentinel.



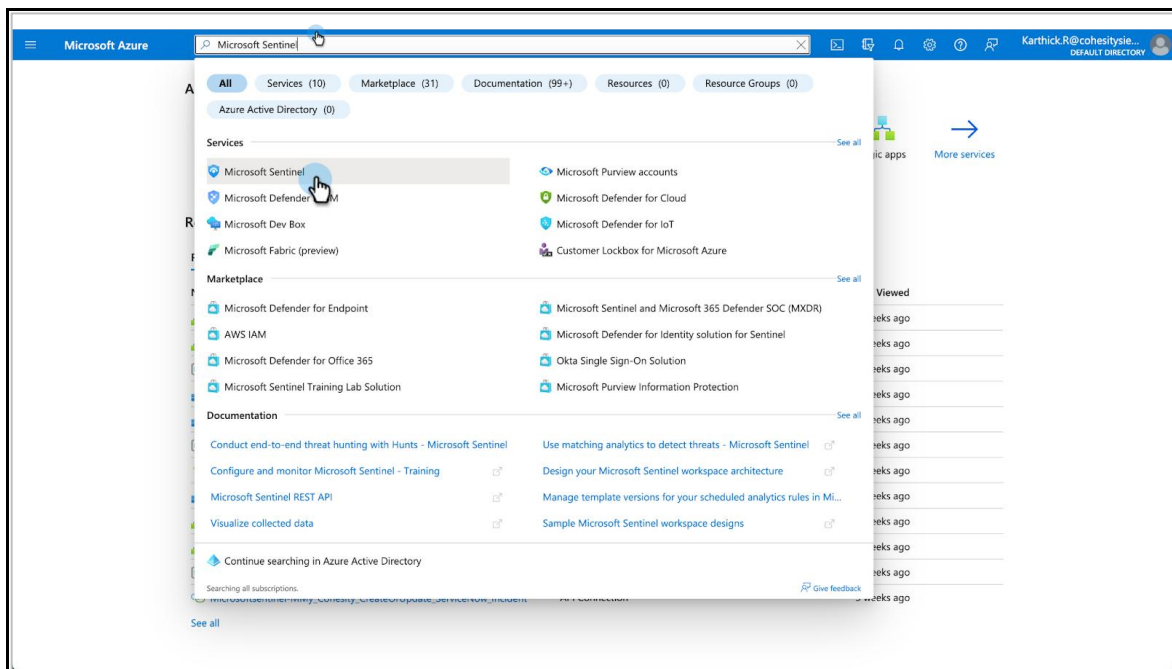
Configure Workspace and Resource Group

Microsoft uses a **Workspace and Resource group** to gather and store all logs-related information. A workspace is a unique environment for the log data from Microsoft Sentinel providing a centralized place to view and manage the artifacts and store events and other information. A workspace has a unique workspace ID and resource ID.

A **Resource group** includes all the resources for your Microsoft Sentinel solution and consists of multiple workspaces.

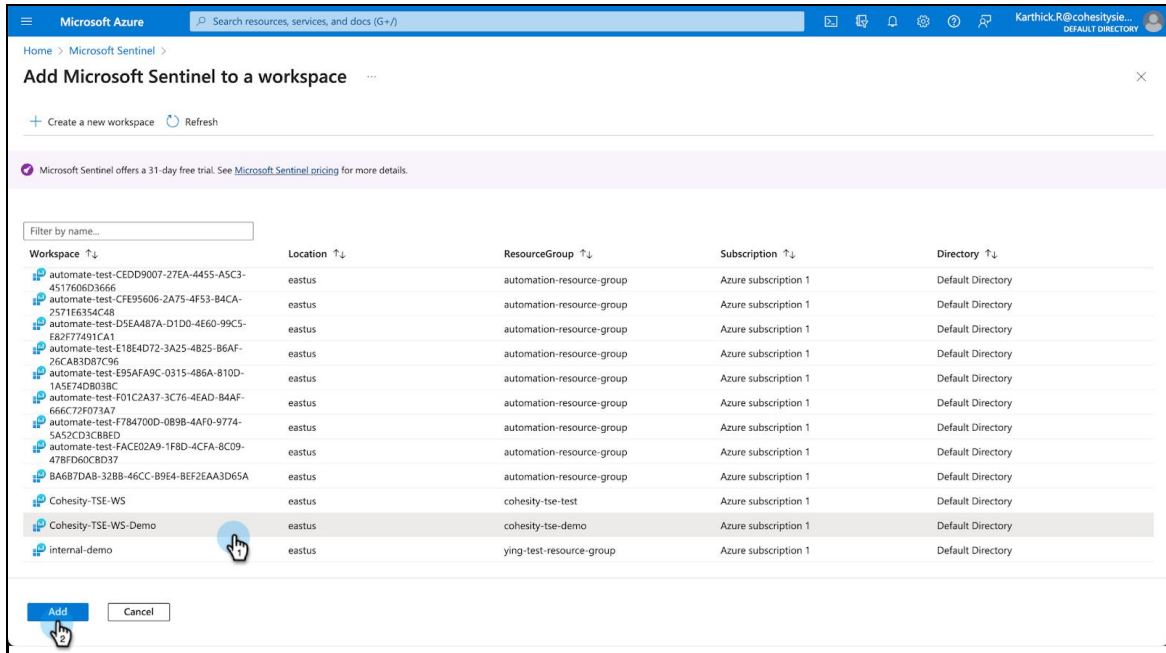
To create the Workspace and Resource group:

1. Sign in to the [Azure portal](#).
2. Search for and select **Microsoft Sentinel**.



3. Select the **Workspace and Resource group** you want to use or create a new one. Refer to [create the workspace and resource group](#).

4. Add new **Workspace** to Microsoft Sentinel.



Install Cohesity Security Integration Solution

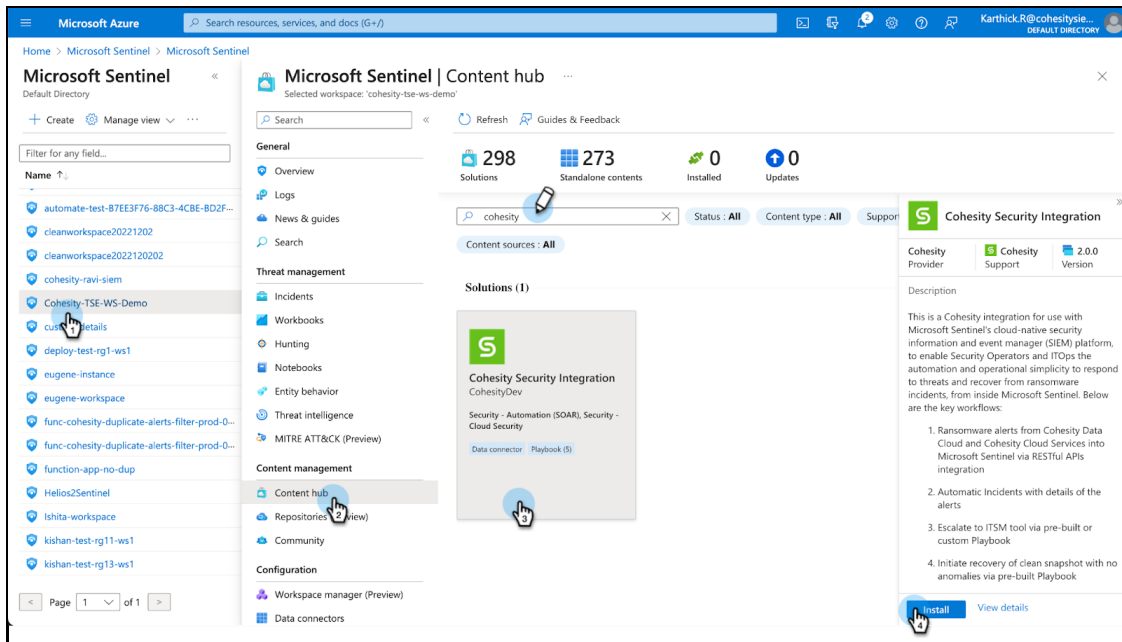
NOTE: Your MS Sentinel workspace and your app resources must be in the same resource group.

Microsoft Sentinel is a Cloud-native SIEM Solution that can be configured to integrate Cohesity Data Cloud with the built-in **Cohesity Security Integration** solution available on [Cohesity Marketplace](#). It contains a set of bundled content including a data connector and playbook templates configured specifically for Cohesity data.

To install the Cohesity Security Integration Solution:

1. From the Sentinel dashboard, select the created **Workspace**.
2. Under **Content management**, select **Content Hub** and then search for **Cohesity**.

- In the search results, select the “**Cohesity Security Integration**” solution, and on the right pane, click **Install**.



- You've now installed the required **Cohesity-developed playbook templates** configured specifically for Cohesity data in your Microsoft Sentinel environment.

Configure Cohesity Data Connectors

The next step is to configure **Cohesity Data Connectors** to start ingesting your data into Microsoft Sentinel. Cohesity Data Connector is a **Function App** that establishes the secure connection between Cohesity Helios and Microsoft Sentinel.

Before you configure data connectors, register the Azure application and grant permissions to fetch incidents on Microsoft Sentinel.

Register Azure Application for Cohesity

To create incidents in Microsoft Sentinel and store Cohesity alert-related data on Azure Storage, the Azure function applications need an Azure application identity. You can refer to [Register a Client Application in Azure Active Directory](#) to learn how to register an application, check the application ID, and create a New Client Secret.

Once you've registered the application, you should save the following information.

- Application (client) ID
- Directory (tenant) ID
- Secret Value

NOTE: You must grant Azure Storage (user_impersonation) permission to the Azure application.

The screenshot shows the 'Request API permissions' dialog in the Azure portal. The 'Azure Storage' API is selected. Under 'Select permissions', the 'user_impersonation' permission is chosen. The 'Admin consent required' column for this permission is set to 'No'. The 'Add permissions' button is highlighted at the bottom of the dialog.

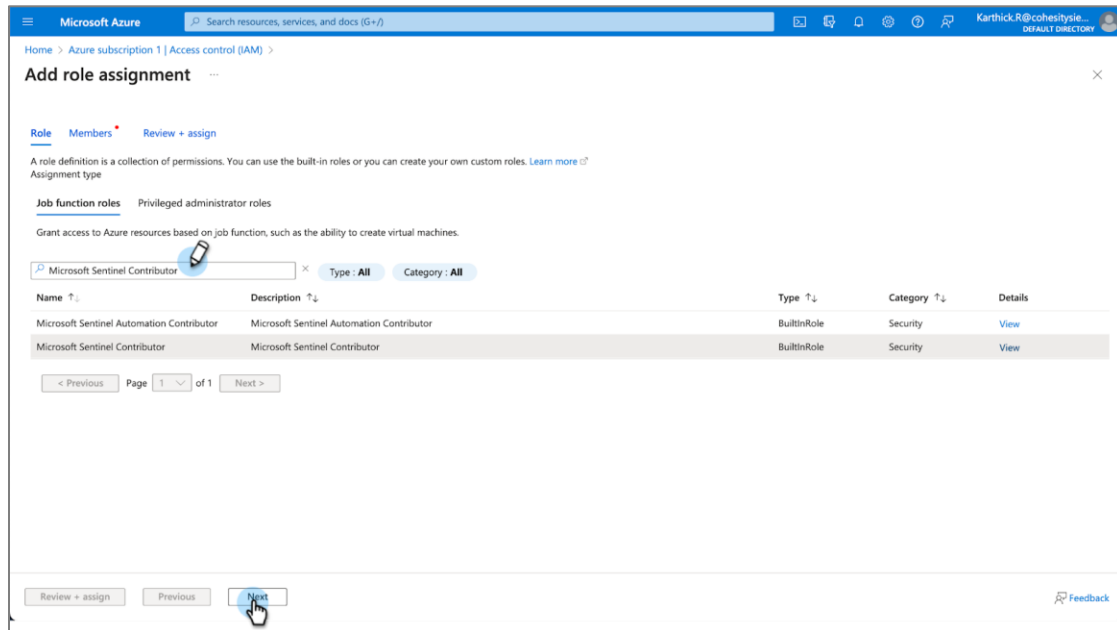
Set Required Permissions to Create Microsoft Sentinel Incidents

After Registering the Azure Application for Cohesity, assign the role of **Microsoft Sentinel Contributor** to allow Cohesity function apps to create incidents on Microsoft Sentinel. To assign the role:

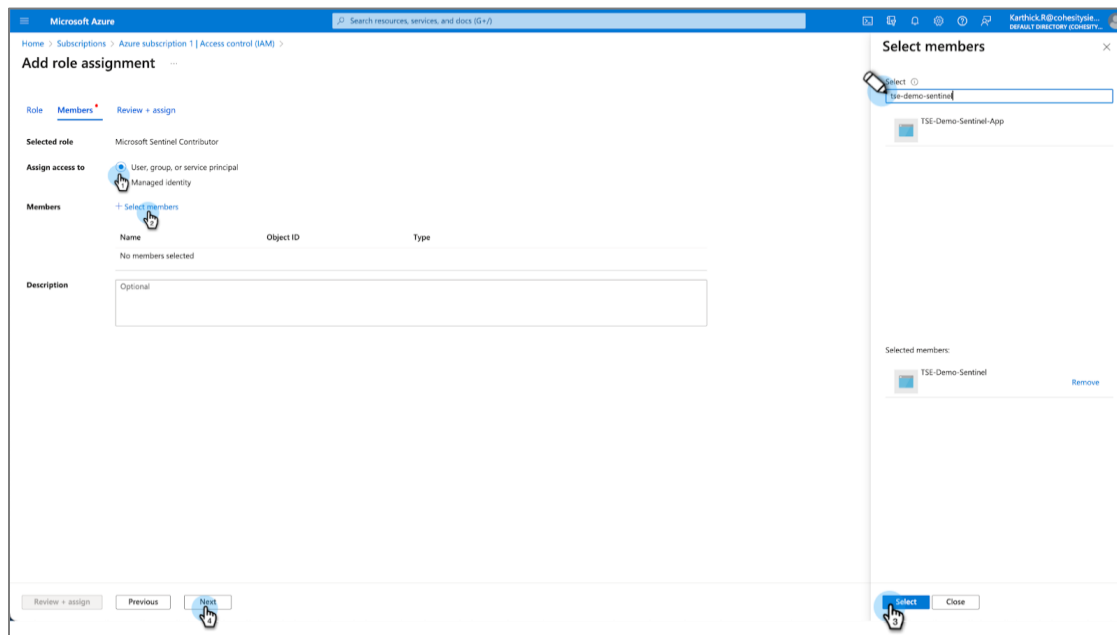
1. Under the **Subscriptions** tab from the **Home** page, choose your subscription name.
2. On the left pane, choose **Access Control (IAM)**.
3. Select **Add > Add Role Assignment**.

The screenshot shows the 'Access control (IAM)' page for 'Azure subscription 1'. The 'Add role assignment' button is highlighted in the top right area of the page. The left navigation pane shows 'Access control (IAM)' selected.

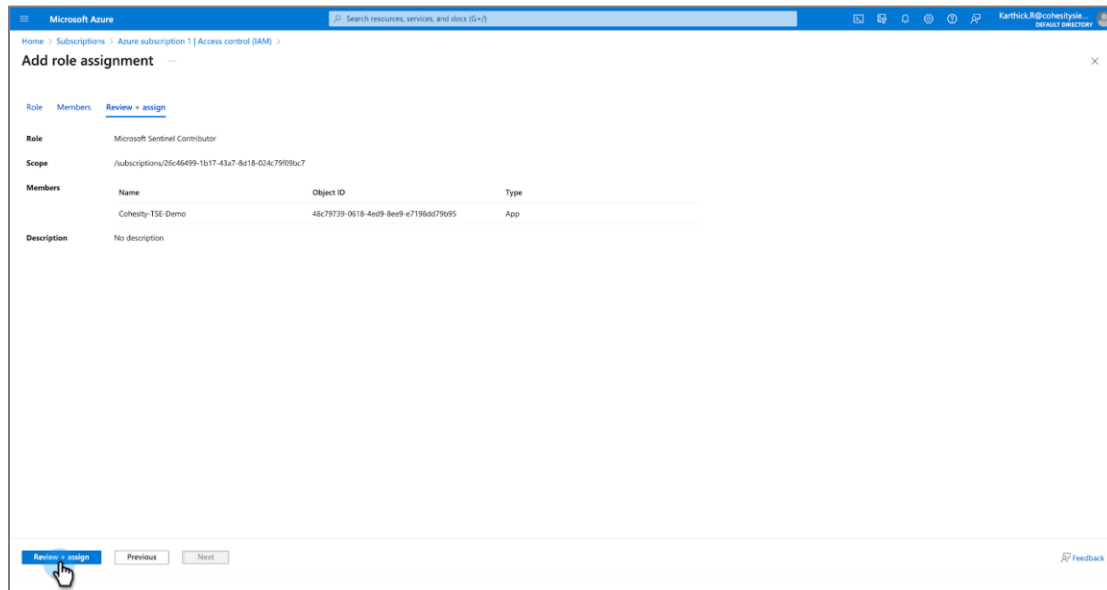
4. Search for the **Microsoft Sentinel Contributor** role and click **Next**.



5. Select **Assign Access to as users, group, or service principal**, and select the created App from the **Select members** right pane.



6. Select **Review + assign**. This will assign the **Microsoft Sentinel Contributor** permissions to the registered created app for Cohesity.



Deploy Cohesity Data Connector

Once you've registered the application (identity), follow the below steps to configure the Cohesity Data connector, which will establish the secure connection between Microsoft Sentinel and Cohesity Data Cloud to fetch the ransomware alerts from Cohesity Data Cloud to **Incidents tab** under Microsoft Sentinel

1. From the selected workspace, select **Configuration > Data Connectors**.
2. Search for Cohesity and select the data connector "**Cohesity (using Azure function)**". A right pane with connector details is displayed.

3. Select **Open Connector Page**. The **Instructions** tab is displayed.

The screenshot shows the Microsoft Sentinel interface. In the left-hand navigation pane, the 'Data connectors' option is highlighted. The main area displays a list of connectors, with 'Cohesity (using Azure Function)' selected. The details panel on the right shows the connector's status as 'Disconnected' and provides a description of its functionality. A blue button labeled 'Open connector page' is visible at the bottom of the details panel, with a hand cursor hovering over it.

4. Click **Deploy to Azure**.

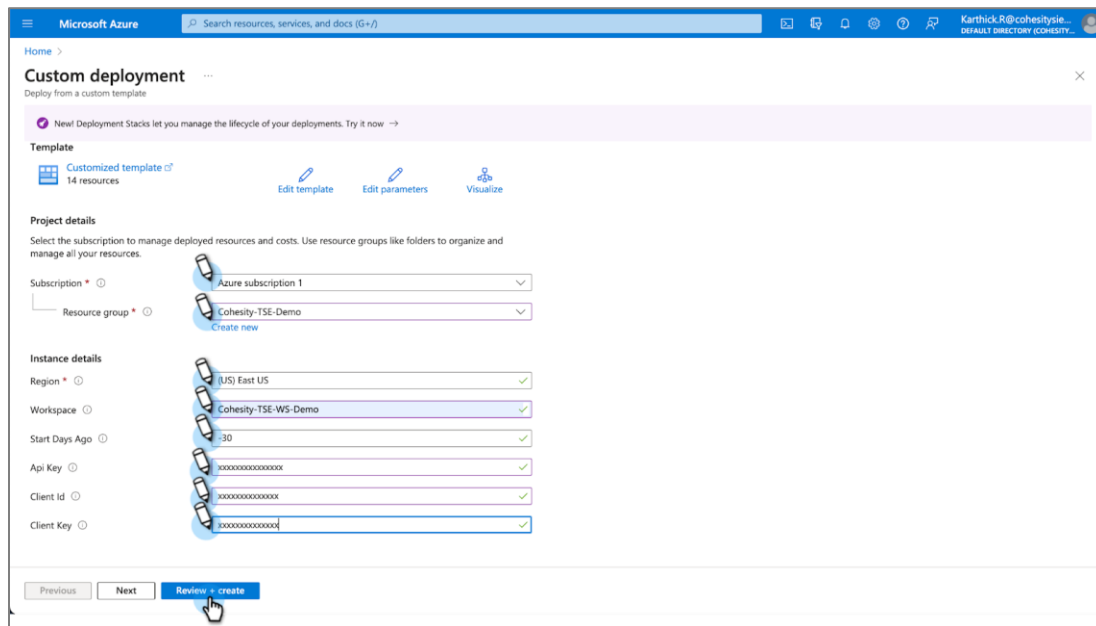
This screenshot shows the 'Cohesity (using Azure Function)' connector page. The 'Deploy to Azure' button is highlighted with a hand cursor. The page contains the following instructions:

- (Optional Step)** Securely store workspace and API authorization key(s) or token(s) in Azure Key Vault. Azure Key Vault provides a secure mechanism to store and retrieve key values. Follow [these instructions](#) to use Azure Key Vault with an Azure Function App.
- STEP 1 - Get a Cohesity DataHawk API key (see troubleshooting instruction 1)**
- STEP 2 - Register Azure app (link) and save Application (client) ID, Directory (tenant) ID, and Secret Value (instructions).** Grant it Azure Storage (user_impersonation) permission. Also, assign the 'Microsoft Sentinel Contributor' role to the application in the appropriate subscription.
- STEP 3 - Deploy the connector and the associated Azure Functions.**

Azure Resource Manager (ARM) Template
Use this method for automated deployment of the Cohesity data connector using an ARM Template.

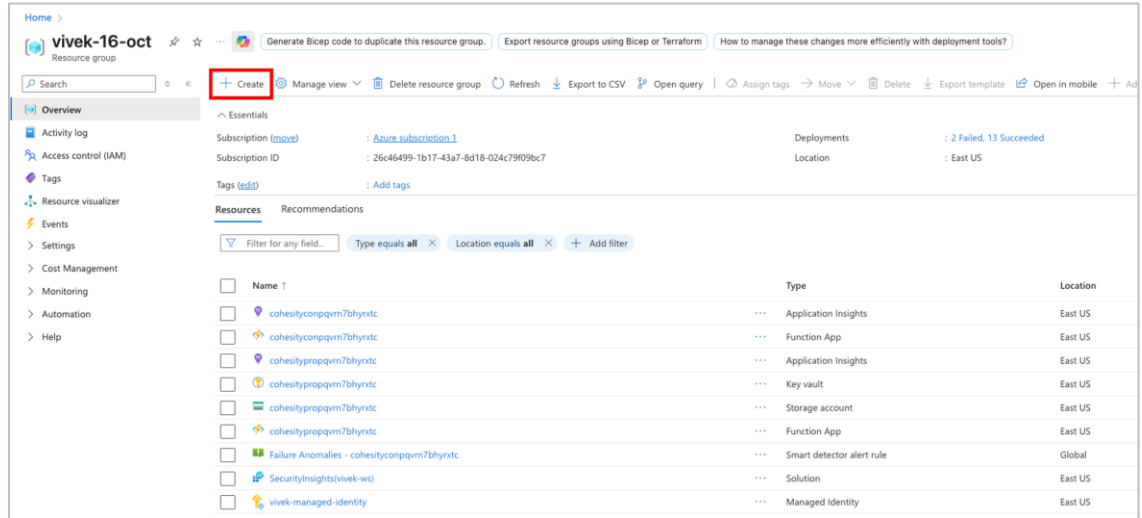
1. Click the **Deploy to Azure** button below.
2. Select your preferred **Subscription, Resource Group** and **Location**.
3. Enter the parameters that you created at the previous steps
4. Mark the checkbox labeled **I agree to the terms and conditions stated above**.
5. Click **Purchase** to deploy.

5. Add the below field names and click **Review + Create**.
 - a. **Subscription** - <Select the subscription name>.
 - b. **Resource Group** - <Select the resource group associated with workspace>.
 - c. **Region** - <Choose the Azure region>.
 - d. **Workspace** - <Enter the “name” of the workspace>.
 - e. **Start Day Ago** - <No. of days of historical data about security incidents>.
 - f. **API key** - <Enter your API key token from Cohesity data cloud>.
 - g. **Client Id** - <Enter your Client ID generated while registering the Azure function app>.
 - h. **Client Key** - <Enter your client Secret key generated while registering the Azure function app>.

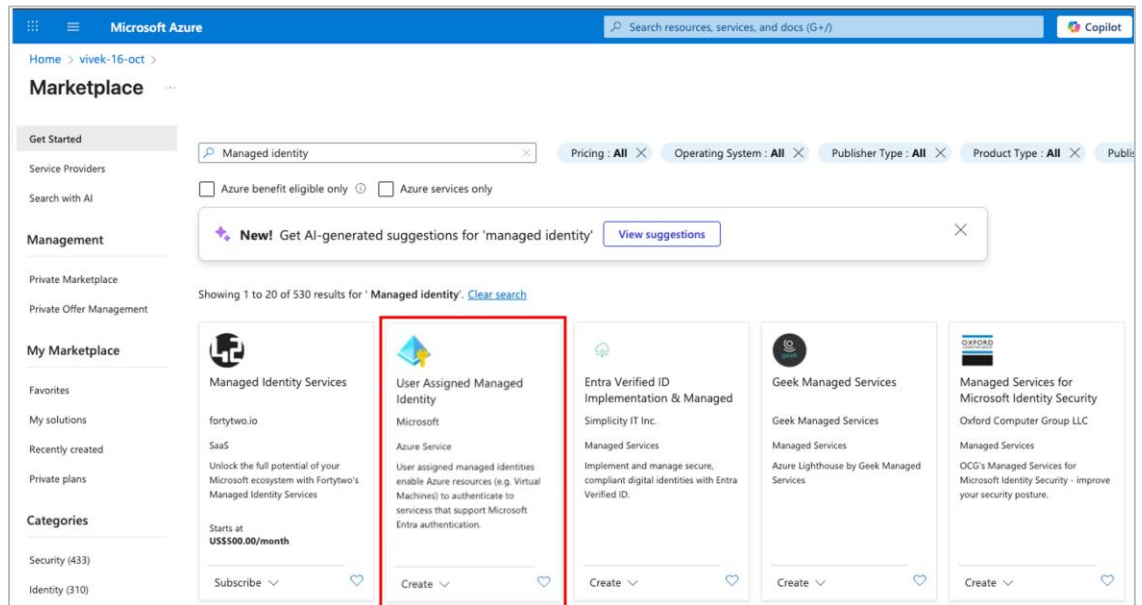


6. You've installed the **Cohesity Data Connector** successfully.
7. After installation, follow the below steps:
 - a. Your new workspace “Cohesity-TSE-WS-Demo” will be listed under MS Sentinel instance.
 - b. Create a Managed Identity App under the Resource Group and get the ‘Client ID’ from the app.

- i. Go to the Resource Group associated with the Microsoft Sentinel App and create a Managed Identity App from the marketplace by clicking 'Create'.



- ii. Search for 'Managed Identity' and create "User Assigned Managed Identity" app.



- iii. Provide the requested details and complete the creation of the app (*Provide the same resource group which was used for MS Sentinel App*).

Microsoft Azure

Home > vivek-16-oct > Marketplace >

Create User Assigned Managed Identity

Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group [Create new](#)

Instance details

Name *

Region

Isolation Scope

- iv. Click the newly created Managed Identity App.

Microsoft Azure

Home > vivek-16-oct Resource group

Essentials

Subscription (move) : Azure subscription 1

Subscription ID : 26c46499-1b17-43a7-8d18-024c79f09bc7

Deployments : 2 Failed, 13 Succeeded

Location : East US

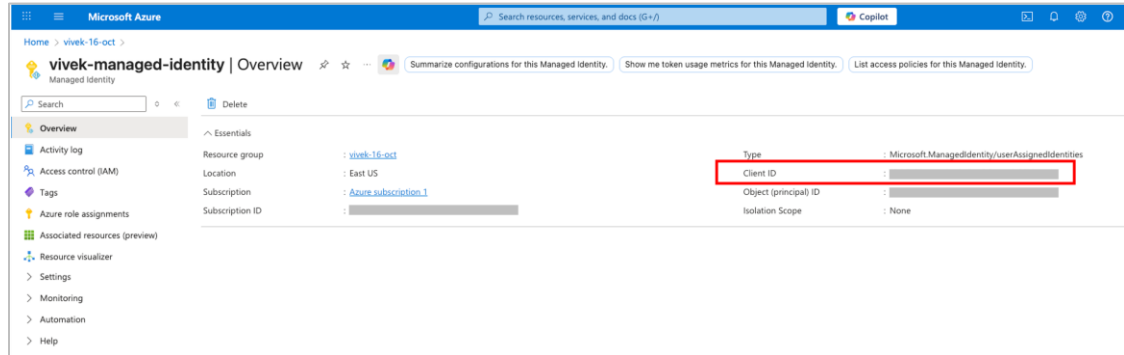
Tags (edit) : Add tags

Resources

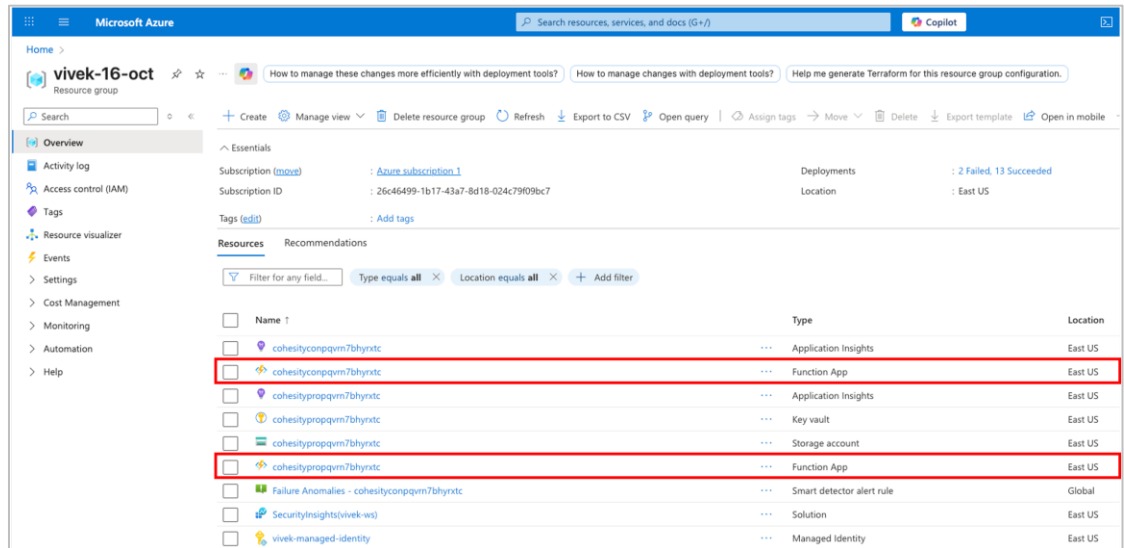
Filter for any field... Type equals all Location equals all + Add filter

Name	Type	Location
cohesityconpqvm7bhyrxc	Application Insights	East US
cohesityconpqvm7bhyrxc	Function App	East US
cohesitypropqvm7bhyrxc	Application Insights	East US
cohesitypropqvm7bhyrxc	Key vault	East US
cohesitypropqvm7bhyrxc	Storage account	East US
cohesitypropqvm7bhyrxc	Function App	East US
Failure Anomalies - cohesityconpqvm7bhyrxc	Smart detector alert rule	Global
SecurityInsights(vivek-ns)	Solution	East US
vivek-managed-identity	Managed Identity	East US

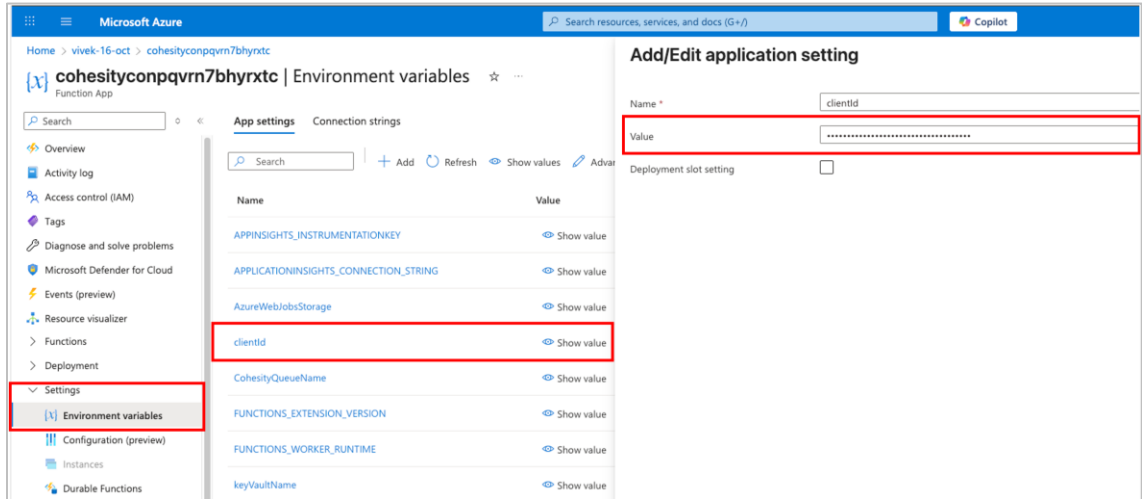
- v. Copy the “Client ID” from the app (*This needs to be copied to ‘Function Apps’ which is shown in step 7).*



- c. Copy the ‘Client Id’ to the ‘Function Apps’ under the Resource Group.
i. Go to both the “Function Apps” in the Resource Group.

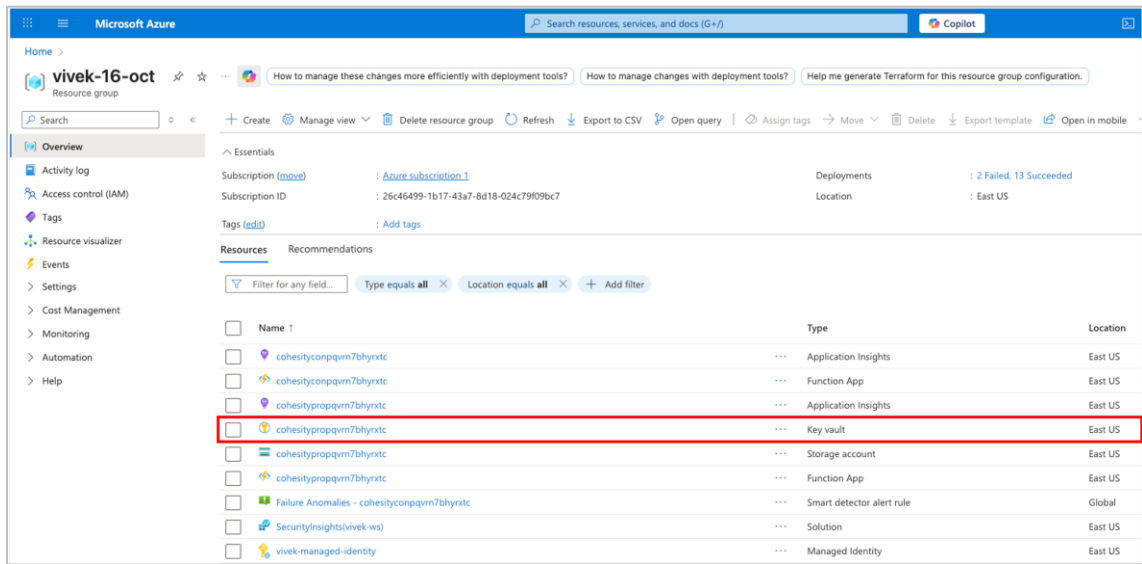


- ii. Copy the “Client ID” from step 6e to the Client ID Value under Settings > Environment variables > clientId and click “Apply” (This will restart the apps).

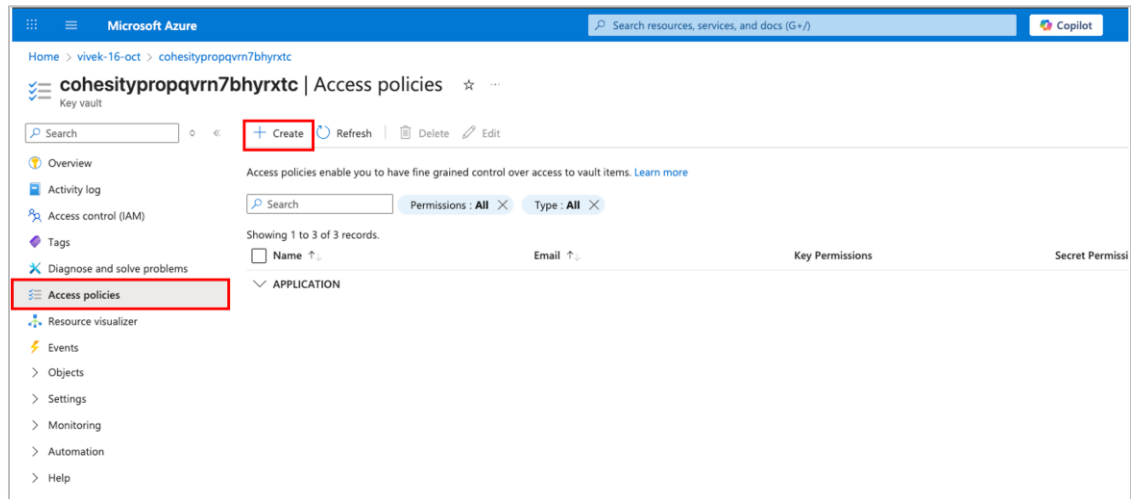


- d. Create ‘Access Policy’ in Key Vault App under the Resource Group.

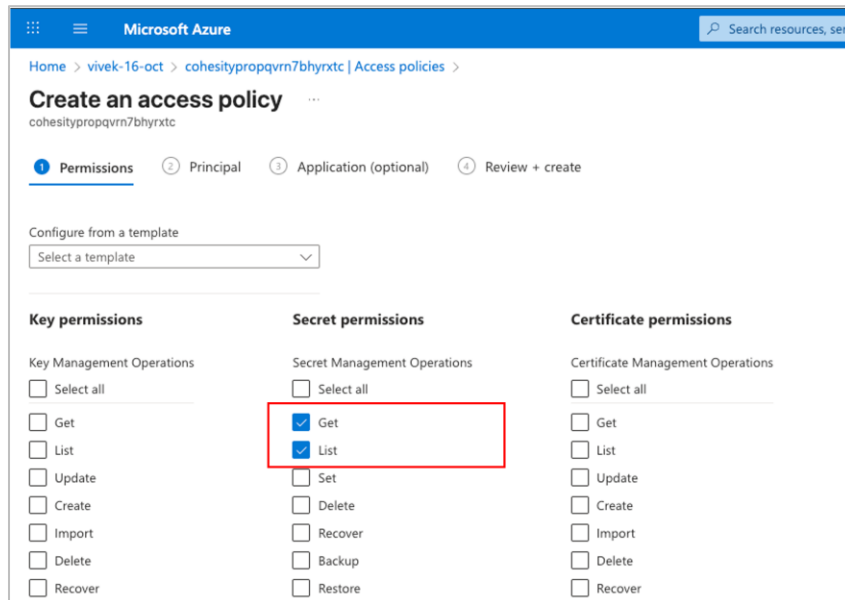
- i. Go to “Key Vault” app under the Resource Group.



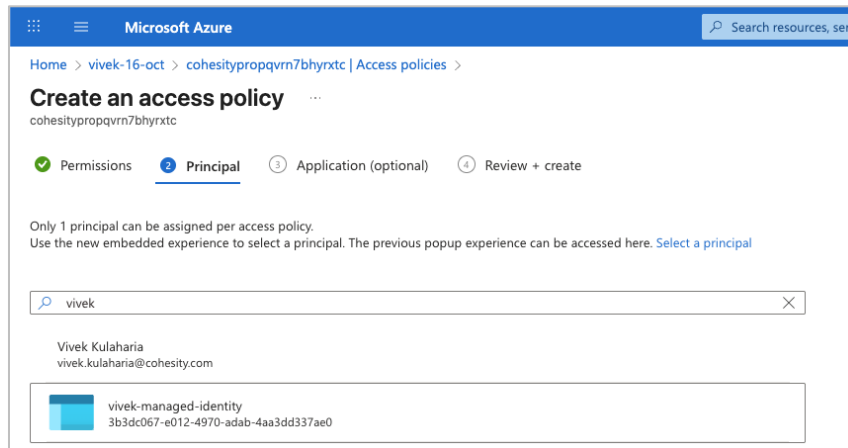
- ii. Click “Access Policies” and create an Access Policy by clicking “Create”.



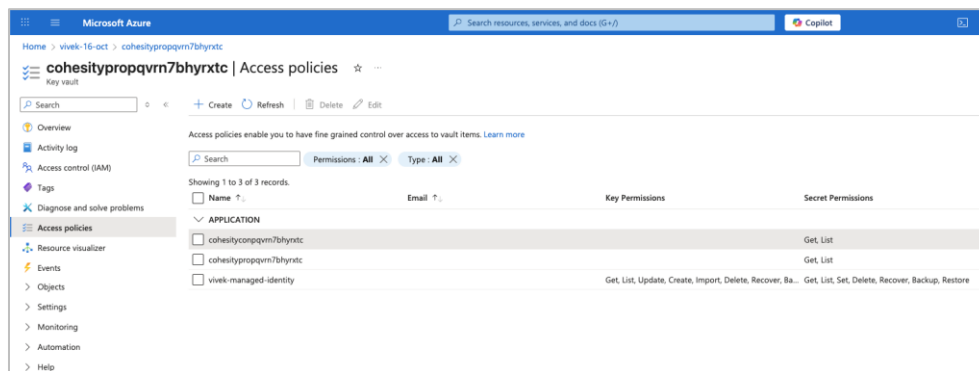
- iii. Select ‘Get’ and ‘List’ under ‘Secret Permissions’ and click ‘Next’.



- iv. Select the 'Managed Identity App' created in Step 8 for 'Principal'.

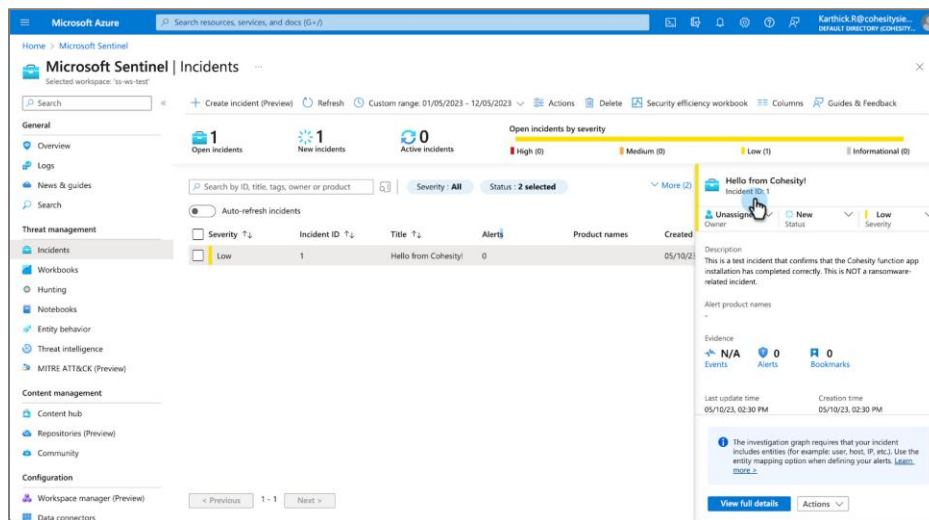


- v. Finish the creation of Access policies.



8. After installation, you should see a welcome incident with the title **Hello from Cohesity!**

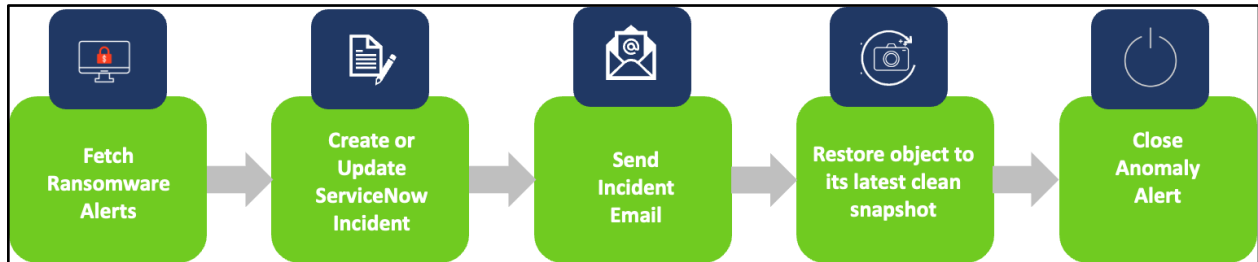
NOTE: The welcome incident may take a few minutes to appear after installation and all the existing anomaly alerts will also start appearing on the incident tab.



Configure the Cohesity Playbooks

Once you have installed the Cohesity solution, the Cohesity playbook templates are available in Microsoft Sentinel to unite security and IT teams for collaborative investigation and remediation. To check the playbook templates, go to **Automation -> Playbook templates** and search for Cohesity. Cohesity solution provides the following playbooks:

Figure 3: Cohesity Playbooks use cases



- **Cohesity Send Incident Email** – ends an email to the recipient with the details related to the incidents.
- **Cohesity CreateOrUpdate ServiceNow Incident** – Creates and updates the incident in the ServiceNow platform.
- **Cohesity Restore From Last Snapshot** – Allows you to restore your data from a clean snapshot.
- **Cohesity Close Helios Incident** – Allows you to resolve alerts on Cohesity Data Cloud.
- **Cohesity Delete Incident_Blobs** – Deletes the blobs on Azure storage created by an incident that is generated by the Cohesity function apps.

The screenshot displays the Microsoft Sentinel Automation interface. The left sidebar shows navigation options like Threat management, Content management, and Configuration. The main area shows a list of playbook templates under the 'Automation rules' tab. The filters are set to 'Trigger: All', 'Logic Apps Connectors: All', 'Entities: Malware', and 'Tags: All'. The source name is 'CohesitySecurity'.

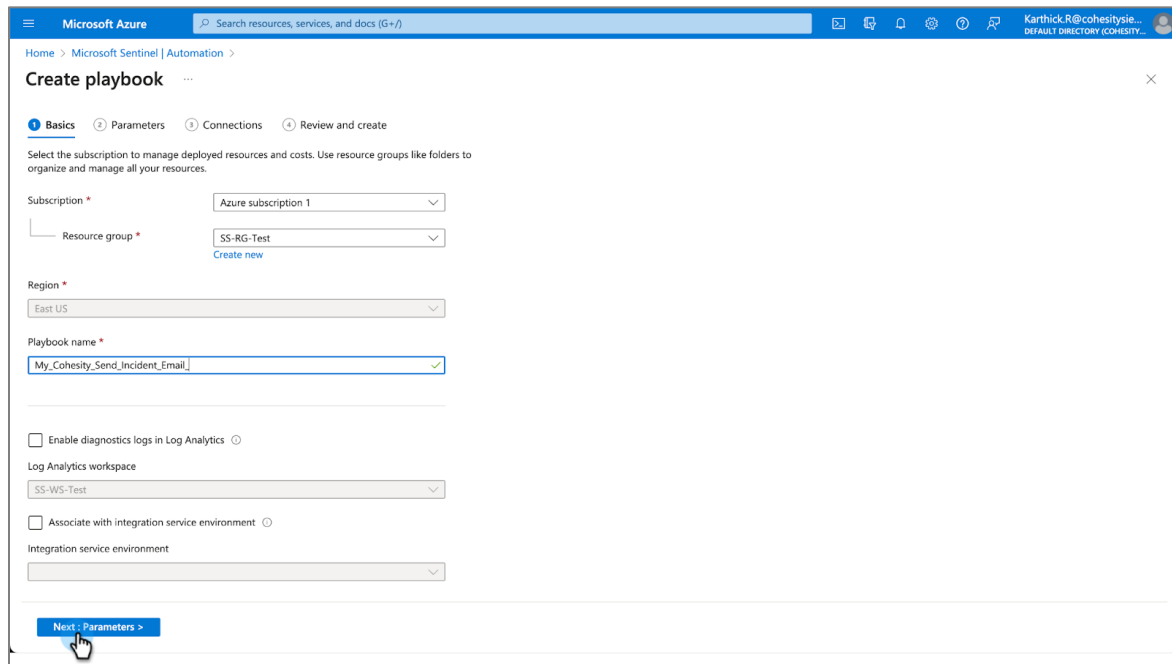
Name	Trigger	Logic Apps Connectors	Entities	Tags	Last modified	Source name
Cohesity Incident Email	Microsoft Sentinel...	Outlook.com +1	Malware	SOAR, Email Notificat...	12/23/22, 04:27 PM	CohesitySecurity
Restore From Last Cohesity Snapshot	Microsoft Sentinel...	Azure Blob Stor... +2	Malware	DataHawk, SOAR, C...	01/13/23, 03:32 PM	CohesitySecurity
Cohesity Create or Update ServiceNow incident	Microsoft Sentinel...	ServiceNow +1	Malware	ServiceNow, SOAR	12/23/22, 03:32 PM	CohesitySecurity
Delete Cohesity incident blobs	Microsoft Sentinel...	Azure Blob Stor... +1	Malware	Cleanup	01/27/23, 04:27 PM	CohesitySecurity
Close Cohesity Helios Incident	Microsoft Sentinel...	Azure Key Vault +1	Malware	DataHawk, SOAR, C...	01/13/23, 03:32 PM	CohesitySecurity

Now, Let's see how we can configure the different Cohesity-developed playbooks on the Microsoft Sentinel platform.

Cohesity Incident Email Playbook

This playbook sends an email to the recipient with the incident details. After you assign the [permissions to playbook](#), you need to perform the below configuration steps to enable this playbook:

1. From the Workspace, under the Configuration pane, navigate to **Automation** tab, and select **Cohesity Incident Email Playbook**.
2. Click **Create playbook**.



The screenshot displays the 'Create playbook' configuration page in the Microsoft Azure portal. The page is titled 'Create playbook' and is part of the 'Automation' section in Microsoft Sentinel. The configuration is organized into tabs: 'Basics' (selected), 'Parameters', 'Connections', and 'Review and create'. Below the tabs, there is a section for selecting the subscription to manage resources, with fields for 'Subscription' (set to 'Azure subscription 1'), 'Resource group' (set to 'SS-RG-Test'), and 'Region' (set to 'East US'). The 'Playbook name' field is set to 'My_Cohesity_Send_Incident_Email'. There are also checkboxes for 'Enable diagnostics logs in Log Analytics' and 'Associate with integration service environment', both of which are currently unchecked. The 'Log Analytics workspace' is set to 'SS-WIS-Test'. At the bottom of the page, there is a blue button labeled 'Next - Parameters >' which is being clicked by a mouse cursor.

3. Enter the **field details** and click **Next: Parameters**

- **Subscription**
- **Resource group**
- **Playbook Name**

The screenshot shows the 'Create playbook' wizard in the Microsoft Azure portal. The 'Basics' step is active, and the user has filled in the following details:

- Subscription:** Azure subscription 1
- Resource group:** SS-RG-Test
- Region:** East US
- Playbook name:** My_Cohesity_Send_Incident_Email

Additional options shown include:

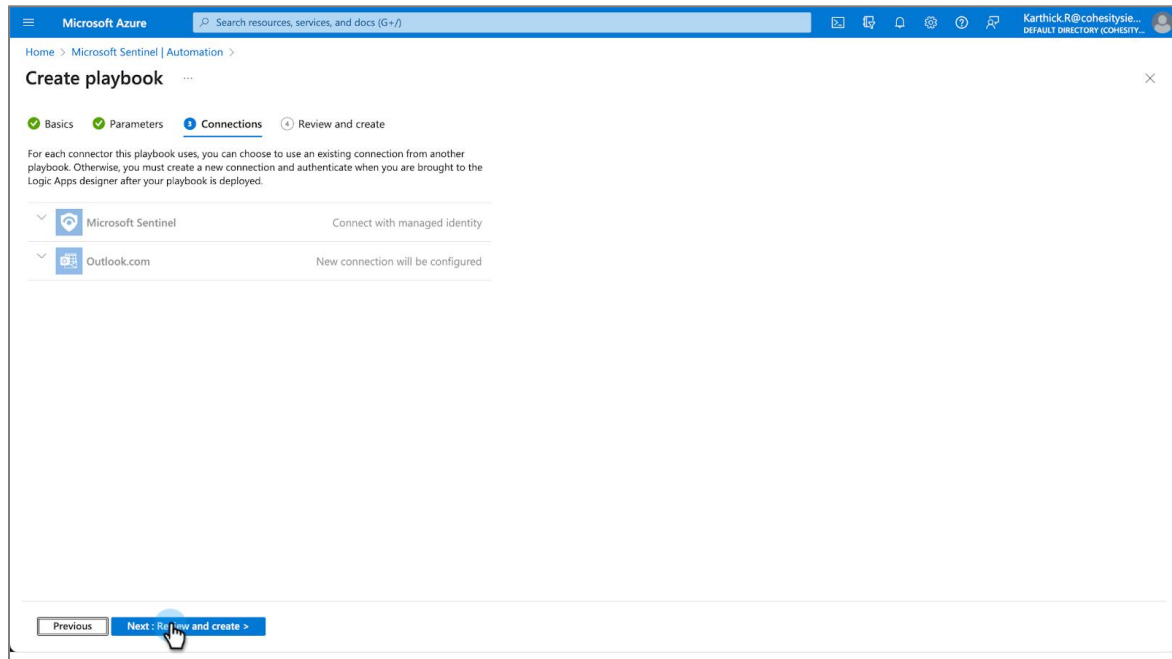
- Enable diagnostics logs in Log Analytics
- Log Analytics workspace:** SS-WS-Test
- Associate with integration service environment

The 'Next: Parameters >' button is highlighted with a mouse cursor.

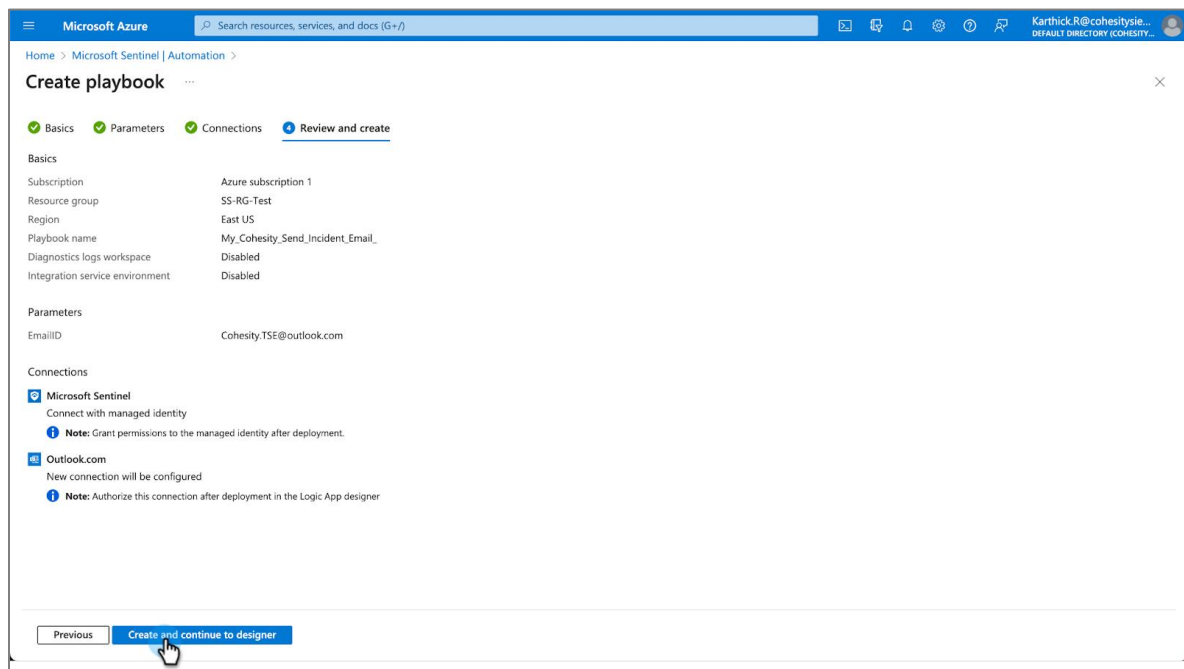
4. Enter the **recipient's email address** and click **Next: Connections**.

The screenshot shows the 'Create playbook' wizard in the Microsoft Azure portal, now at the 'Parameters' step. The 'EmailID' field is filled with an email address ending in @outlook.com. The 'Next: Connections >' button is highlighted with a mouse cursor.

5. Click **Next: Review and create**. This will review and validate the parameter details.



6. Click **Create and continue to designer**. This will redirect to the Logic apps window to authorize the API connections.

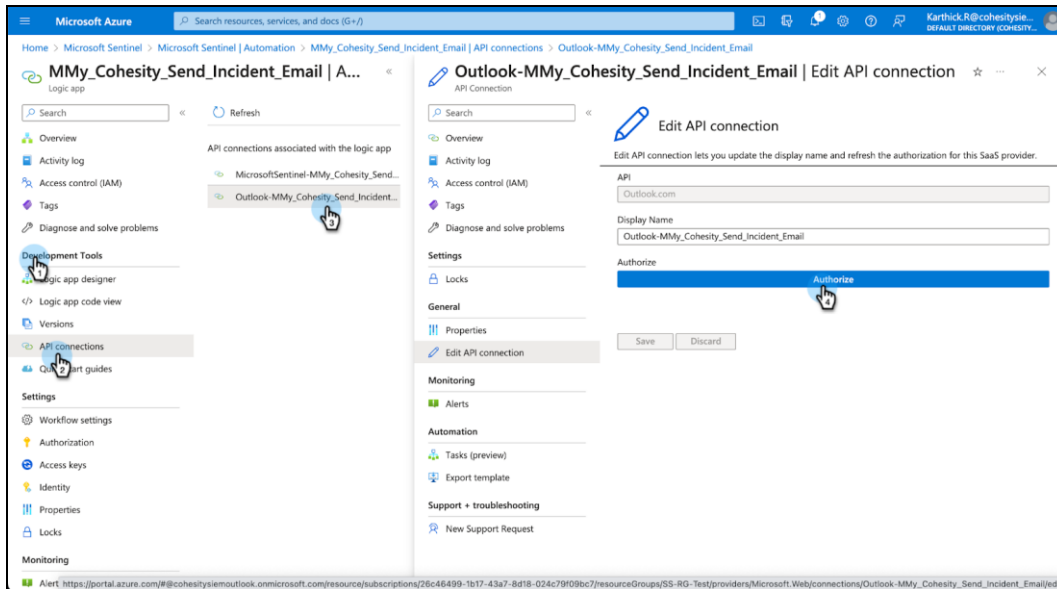


Authorize Microsoft Sentinel to Access Outlook

After creating the playbook, you should authorize a connection from the Logic Apps to access Outlook.

To authorize the connections:

1. In Microsoft Sentinel, go to **Logic Apps**, and choose your playbook.
2. Choose **Development Tools > API Connections**.
3. Select an Outlook **connection** to authorize.
4. Select **General > Edit API Connection**.



5. Select **Authorize** and you will be redirected to an email account configured to authorize the connections.
6. After authorizing the connection to Outlook, Go to the **Incidents tab** under the selected workspace, and select **Run** to trigger the playbook.

NOTE: Make sure the user that runs the playbook has the role **Microsoft Sentinel Playbook Operator** assigned. To assign the role, refer [set required permissions to access playbook](#).

The screenshot shows the Microsoft Azure portal interface for running a playbook on an incident. The main heading is "Run playbook on incident". Below this, there's a table of playbooks with columns for Name, Subscription, Resource group, and Plan. The "MMy_Cohesity_Send_Inc..." playbook is selected, and its "Run" button is highlighted. A notification at the top right indicates "Playbook was triggered successfully".

Name	Subscription	Resource group	Plan	Run
Cohesity_Incident_RAG...	Azure subscription 1	SS-RG-Test	Consumption	Run
Dev_clone	Azure subscription 1	SS-RG-Test	Consumption	Run
GS_Post_Comment_Azu...	Azure subscription 1	SS-RG-Test	Consumption	Run
MMy_Cohesity_Close_H...	Azure subscription 1	SS-RG-Test	Consumption	Run
MMy_Cohesity_CreateO...	Azure subscription 1	SS-RG-Test	Consumption	Run
Mmy_Cohesity_Restore...	Azure subscription 1	SS-RG-Test	Consumption	Run
MMy_Cohesity_Send_In...	Azure subscription 1	SS-RG-Test	Consumption	Run
My_Cohesity_CreateOrU...	Azure subscription 1	SS-RG-Test	Consumption	Run
My_Cohesity_Restore_Fr...	Azure subscription 1	SS-RG-Test	Consumption	Run
My_Cohesity_Send_Inc...	Azure subscription 1	SS-RG-Test	Consumption	Run
Recover_from_clean_sn...	Azure subscription 1	SS-RG-Test	Consumption	Run
Punit-Devclone/Clone-P...	Azure subscription 1	SS-RG-Test	Standard	Run

7. You will get an auto-notification email with **Incident details** from the configured email ID.

The screenshot shows an Outlook email titled "Cohesity Alert - Inbox". The email is from "Cohesity" and is dated "Thursday, 13 July 2023 at 2:54 AM". The body of the email contains the following information:

Hello SecurityTeam,

You have a Cohesity incident from Microsoft Sentinel. Below is information:

- Incident ARM Name: 1507c467-a573-4a92-b0c4-dbc61e6d44fd
- Description: Anomalous change in file system detected on Ransomware/vm-file-ext-prod-canary, a symptom of potential ransomware attack on your primary environment. Alert cause: The recent protection run of Protection Group anti-ransomware-fastsim-prod-4-588C with job id 34773 has dramatic changes in the composition of files, which is a significant deviation from the previously observed protection runs. Anomaly Strength: 90. Additional Info: Use the latest clean snapshot taken at 12, Jul 2023 04:25 PM to perform Instant Recovery. Helios ID: [REDACTED]
- Severity: High
- Incident ID: 287
- Incident Create Time Utc: 2023-07-12T16:40:07.5438692Z
- Incident URL: https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/Incident/subscriptions/26c46499-1b17-43a7-8d18-024c79f09bc7/resourceGroups/kishan-test-rg11/providers/Microsoft.Operationallnsights/workspaces/kishan-test-rg11-ws1/providers/Microsoft.SecurityInsights/incidents/1507c467-a573-4a92-b0c4-dbc61e6d44fd

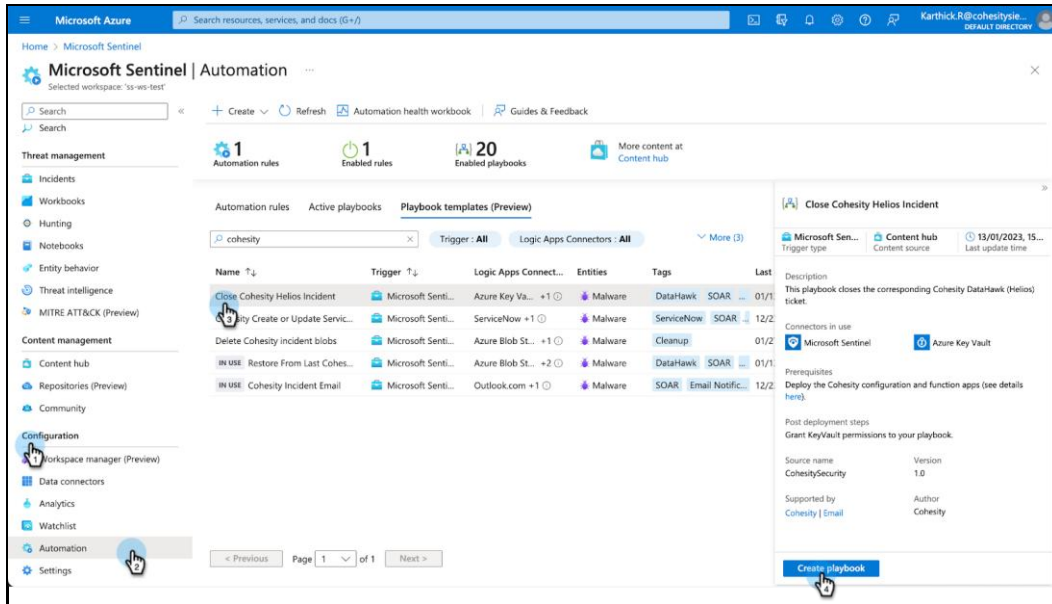
Please review and update incident accordingly.

Cohesity Team

Cohesity Close Helios Incident

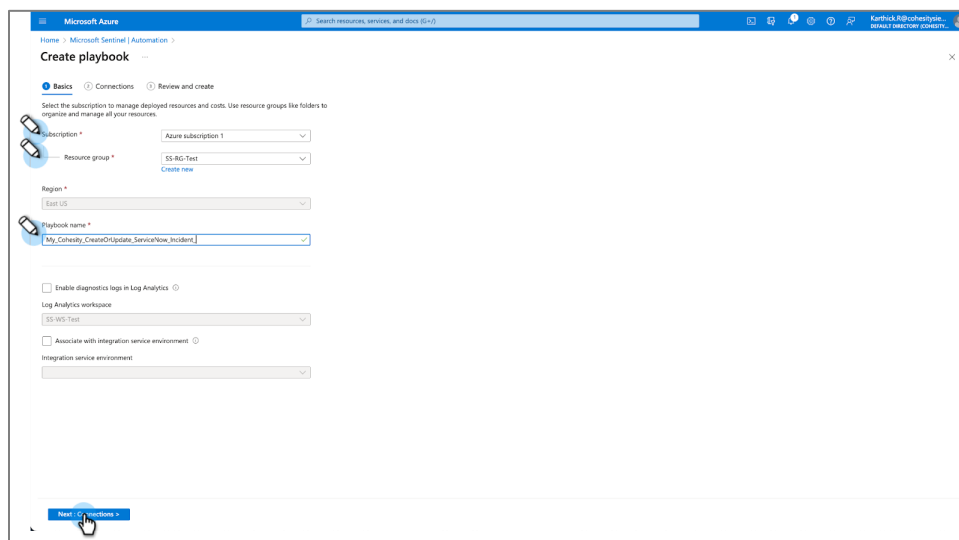
This playbook allows you to resolve alerts on Cohesity Data Cloud. Once you assign the [permissions to playbook](#), you have to perform the below configuration steps to enable this playbook:

1. From the workspace, under the **Configuration** pane, navigate to the **Automation** tab, and select the **Cohesity Close Helios Incident Playbook**.
2. Click **Create playbook**.

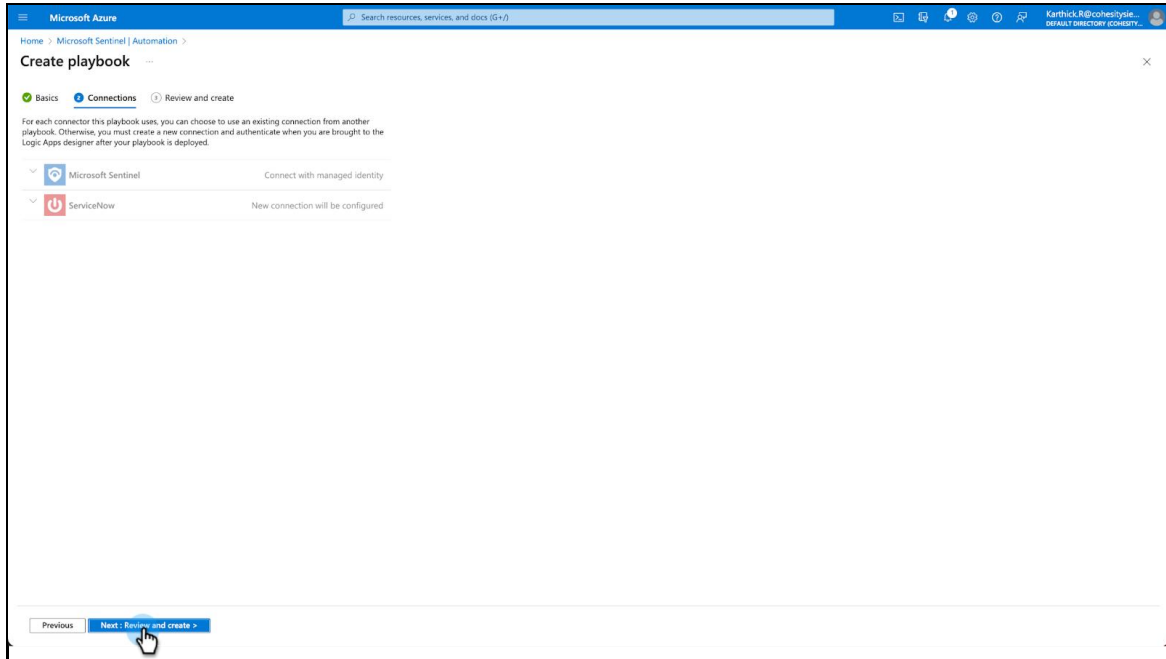


3. Enter the **field details** and select **Next: Connections**:

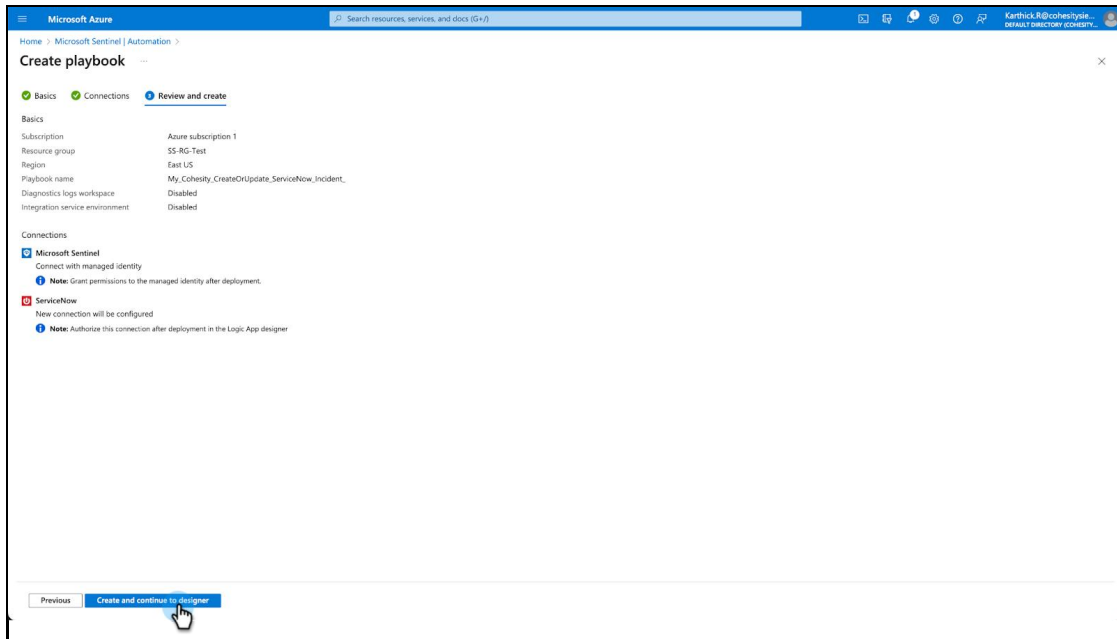
- **Subscription**
- **Resource group**
- **Playbook Name**



4. Click **Next: Review and create**. This will review and validate the parameter details.



5. Select **Create and continue to designer**.



6. After creating the playbook, [Grant KeyVault Permissions](#) for the playbook to access the objects.

Create Automation Rule to Resolve Cohesity Data Cloud Alerts

You can create an automation rule to resolve alerts on Cohesity Data Cloud. To create an automation rule follow the below steps:

1. In your Microsoft Sentinel workspace instance, go to the **Automation** tab under the **Configuration** pane.
2. Select **Create > Automation Rule**.
3. From the automation rule panel, Enter the **Field details** and select **Apply**
 - **Automation rule name** - <Enter a name for your rule>.
 - **Trigger** - <From the Trigger drop-down, select the appropriate trigger according to the circumstance for which you're creating the automation rule - **"When incident is updated"**>.
 - **Conditions** - <Define the conditions>.
 - **Actions** - <Add a run playbook action, you will be prompted to choose from the drop-down list of Cohesity playbooks>.
 - **Rule Expiration** - <Set an expiration date for your automation rule if you want it to have one>.
 - **Order** - <Enter a number under Order to determine where in the sequence of automation rules this rule will run>.

NOTE: You should create this automation rule only if you're using Microsoft Sentinel as the only SIEM/SOAR solution. If you're also using another SIEM/SOAR solution, then resolving the alerts through Microsoft Sentinel may remove it from the other SIEM/SOAR solutions.

The screenshot shows the Microsoft Sentinel interface with the 'Create new automation rule' dialog box open. The dialog is configured as follows:

- Automation rule name:** Close_Cohesity_Helios_Incident
- Trigger:** When incident is updated
- Conditions:**
 - If Incident provider Equals All
 - Analytic rule name Contains All
 - Status Changed To Closed
- Actions:** Run playbook (Cohesity_Close_Helios_Incident)
- Rule expiration:** Indefinite
- Order:** 2

The 'Apply' button is highlighted at the bottom right of the dialog.

Cohesity Create or Update ServiceNow Incident

This playbook creates a ticket on ServiceNow's platform. It can also be used for updating the ticket or closing it on ServiceNow. Once you assign the [permissions to access the playbook](#), you have to perform the below configuration steps to enable this playbook:

1. From the workspace, under the Configuration pane, navigate to the **Automation** tab, and select **Cohesity Create or Update ServiceNow Incident**.
2. Click **Create playbook**.

The screenshot displays the Microsoft Sentinel Automation interface. The left sidebar shows the navigation menu with 'Automation' selected. The main area shows a list of automation rules and playbooks. The 'Cohesity Create or Update ServiceNow Incident' playbook is highlighted, and its configuration details are shown on the right.

Name	Trigger	Logic Apps Connect...	Entities	Tags	Last modified	Source name
IN USE Close Cohesity Helios Incident	Microsoft Senti...	Azure Key Va... +1	Malware	Datahawk SOAR	01/13/21, 03:32 PM	CohesitySecurity
Cohesity Create or Update ServiceNow in...	Microsoft Senti...	ServiceNow +1	Malware	ServiceNow SOAR	12/23/22, 03:32 PM	CohesitySecurity
DELETE Delete Cohesity incident blobs	Microsoft Senti...	Azure Blob St... +1	Malware	Cleanup	01/27/21, 04:27 PM	CohesitySecurity
IN USE Restore From Last Cohesity Snaps...	Microsoft Senti...	Azure Blob St... +2	Malware	Datahawk SOAR	01/13/21, 03:32 PM	CohesitySecurity
IN USE Cohesity Incident Email	Microsoft Senti...	Outlook.com +1	Malware	SOAR Email Notific...	12/23/22, 04:27 PM	CohesitySecurity

The configuration details for the 'Cohesity Create or Update ServiceNow Incident' playbook are as follows:

- Description:** This playbook creates and updates the incident in the ServiceNow platform.
- Connectors in use:** Microsoft Sentinel, ServiceNow
- Prerequisites:** Create an account for ServiceNow.
- Post deployment steps:**
 1. Update ServiceNow credentials in the playbook.
 2. For the playbook to run, there is a need to assign the Microsoft Sentinel Responder role to the playbook's managed identity.
 3. (Recommendation) You can create an automation rule to close the corresponding ServiceNow ticket when the corresponding Sentinel ticket is closed.
- Source name:** CohesitySecurity
- Version:** 1.0
- Supported by:** Cohesity | Email
- Author:** Cohesity

The 'Create playbook' button is visible at the bottom right of the configuration panel.

3. Enter the **field details** and click **Next: Connections**:

- **Subscription**
- **Resource group**
- **Playbook Name**

The screenshot shows the 'Create playbook' wizard in the Microsoft Azure portal. The 'Basics' tab is selected. The form includes the following fields:

- Subscription:** Azure subscription 1
- Resource group:** SS-RG-Test
- Region:** East US
- Playbook name:** My_Cohesity_CreatesOrUpdate_ServiceNow_Incident_

There are also checkboxes for 'Enable diagnostics logs in Log Analytics' and 'Associate with integration service environment'. A 'Next: Connections >' button is highlighted at the bottom.

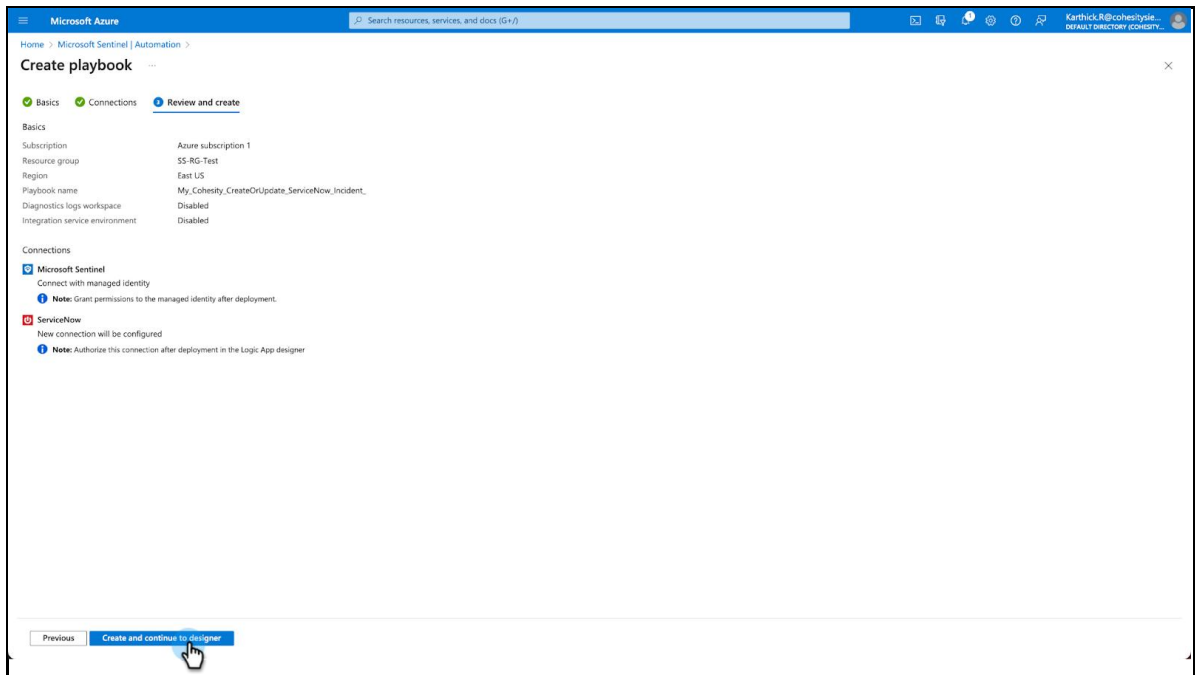
4. Click **Next: Review and create**. This will review and validate the parameter details.

The screenshot shows the 'Create playbook' wizard in the Microsoft Azure portal, now on the 'Connections' tab. The 'Basics' tab is marked as complete with a green checkmark. The 'Connections' tab shows the following configuration:

- Microsoft Sentinel:** Connect with managed identity
- ServiceNow:** New connection will be configured

A 'Next: Review and create >' button is highlighted at the bottom.

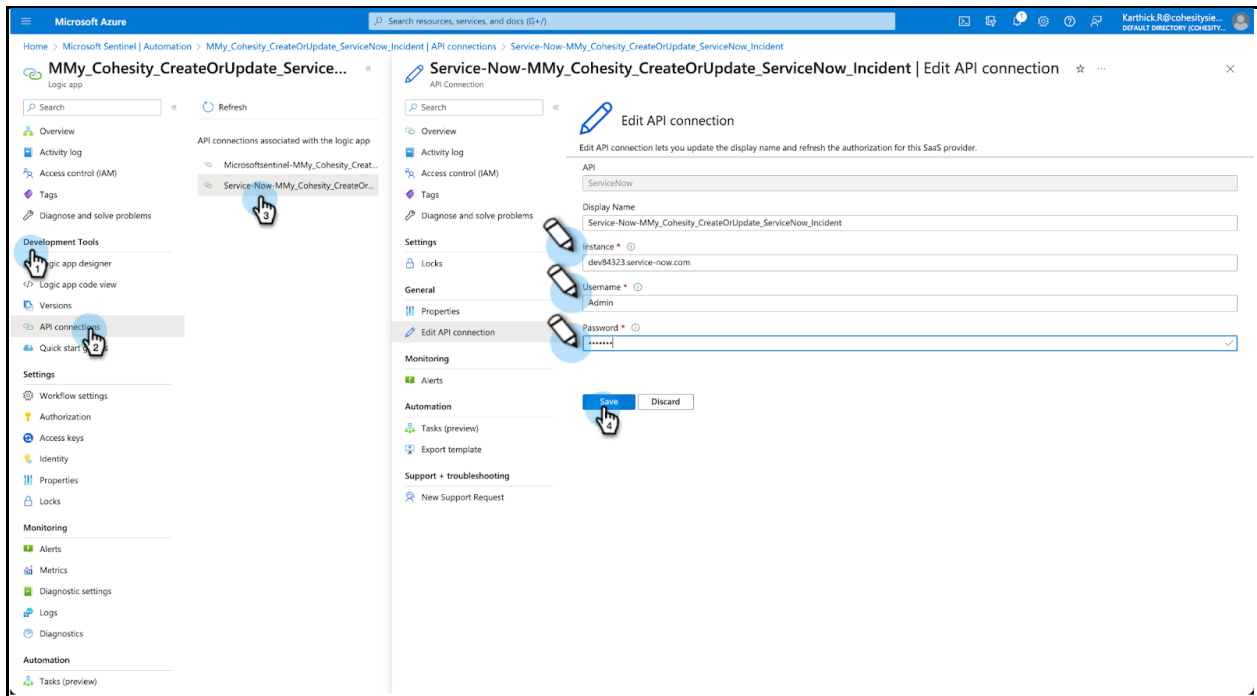
5. Click **Create and Continue to designer**. This will redirect to the Logic apps window to authorize the API connections.



Authorize Microsoft Sentinel to Access ServiceNow Account

After creating the playbook, the next step is to authorize Microsoft Sentinel to access your ServiceNow account. Follow the below steps to enable the ServiceNow API connections:

1. Go to **Logic Apps** and choose your playbook "**Cohesity Create or Update ServiceNow Incident**".
2. Select **Development Tools > API Connections**.
3. Select a **ServiceNow** connection to authorize.
4. Select **General > Edit API Connection**.
5. Enter the domain of your **ServiceNow instance** and credentials.
6. Click **Save**.



Assign the Microsoft Sentinel Responder permissions to the created playbook

The created playbook must have responder permission to respond to the alert and take automated actions.

To assign the role:

1. Under the **Subscriptions** tab from the **Home** page, choose your subscription name.
2. On the left pane, select **Access Control (IAM)**.

3. Select **Add > Add Role Assignment**.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'Karthick.R@cohesity...'. The main content area is titled 'Azure subscription 1 | Access control (IAM)'. On the left, there is a sidebar with 'Subscriptions' and 'Azure subscription 1' selected. The main area shows the 'Add role assignment' button highlighted with a blue circle and a mouse cursor. Below it, the 'Add role assignment' dropdown menu is open, showing 'co-administrator' selected. The main content area also shows 'Check access' and 'Grant access to this resource' sections.

4. Add **Microsoft Sentinel Responder** to the created playbook name.

The screenshot shows the 'Add role assignment' page in the Microsoft Azure portal. The search bar contains 'Microsoft Sentinel Responder'. Below the search bar, there is a table with the following data:

Name	Description	Type	Category	Details
Microsoft Sentinel Responder	Microsoft Sentinel Responder	BuiltInRole	Security	View

The page also shows 'Showing 1 - 1 of 1 results.' and a 'Next' button at the bottom.

The screenshot shows the 'Add role assignment' page in the Microsoft Azure portal. The 'Role' is 'Microsoft Sentinel Responder'. The 'Assign access to' is set to 'Managed identity'. The 'Members' section shows 'No members selected'. A 'Select managed identities' dialog is open on the right, displaying a list of managed identities. The 'Next' button at the bottom is highlighted with a mouse cursor.

5. Click **Next** and select **Review + Assign**. This will assign the **Microsoft Sentinel Responder** permissions to the playbook.

The screenshot shows the 'Add role assignment' page in the Microsoft Azure portal, now on the 'Review + assign' tab. The 'Role' is 'Microsoft Sentinel Responder'. The 'Scope' is '/subscriptions/26c46499-1b17-43a7-8d18-024c79f09bc7'. The 'Members' section shows a table with one member:

Name	Object ID	Type
My_Cohesity_CreateOrUpdate_ServiceNow_Incident	e39641b4-b5f9-4193-9594-384-05c3a79	Logic app

The 'Description' is 'No description'. The 'Review + assign' button at the bottom is highlighted with a mouse cursor.

Create Automation Rule to Close ServiceNow Incidents

To automate the ServiceNow actions from Microsoft Sentinel, you can create an automation rule for SNOW_Record_Create_Update_Playbook. This means that if an incident in Microsoft Sentinel is closed and the corresponding incident in ServiceNow is open, then this automation rule will ensure to run the playbook and close the incidents in the ServiceNow platform.

To create an automation rule:

1. In Microsoft Sentinel, go to the **Automation** tab under the **Configuration** pane.
2. Click **Create > Automation Rule**.
3. From the automation rule panel, enter the **Field details**, and click **Apply**.
 - **Automation rule name** - <Enter a name for your rule>.
 - **Trigger** - <From the Trigger drop-down, select the appropriate trigger according to the circumstance for which you're creating the automation rule such as when the incident is updated>.
 - **Conditions** - <Define the conditions to match>.
 - **Actions** - <Add a run playbook action, you will be prompted to choose from the drop-down list of Cohesity playbooks>.
 - **Rule Expiration** - <Set an expiration date for your automation rule if you want it to have one>.
 - **Order** - <Enter a number under Order to determine where in the sequence of automation rules this rule will run>.

NOTE: You can create the incident on ServiceNow using playbook **SNOW-CreateAndUpdateIncident**.

The screenshot shows the Microsoft Sentinel 'Edit automation rule' configuration page. The rule name is 'CloseServiceNowTickettoSentinel ticket update'. The trigger is 'When incident is updated'. The conditions are: Incident provider (Equals, All), Analytic rule name (Contains, All), and Status (Changed To, Closed). The action is 'Run playbook' with the selected playbook 'MMMy_Cohesity_CreateOrUpdate_ServiceN...'. The rule expiration is 'Indefinite' and the order is '1'. The 'Apply' button is highlighted.

Delete Cohesity Incident Blobs

The data on Azure storage created by a Microsoft Sentinel incident is not required once the ransomware alert on Cohesity Helios is resolved. This playbook allows you to delete those blobs. Once you assign the [permissions to access the playbook](#), you need to perform the below configuration steps to enable this playbook:

NOTE: Cohesity recommends running this playbook as per organizational policy to clean up storage.

1. From the workspace, under the Configuration pane, navigate to the **Automation** tab and select **Delete Cohesity Incident Blobs**.
2. Click **Create playbook**.

The screenshot shows the Microsoft Sentinel Automation console. The left sidebar contains navigation options: General, Threat management, Content management, and Configuration. The 'Automation' tab is selected. The main area displays a list of automation rules and playbooks. The 'Delete Cohesity incident blobs' playbook is highlighted. The right pane shows the details for this playbook, including its description, connectors, prerequisites, and post-deployment steps.

Name	Trigger	Logic Apps Connect...	Entities	Tags	Last modified	Source name
IN USE Close Cohesity Helios Incident	Microsoft Senti...	Azure Key Va... +1	Malware	Datahawk SOAR	01/13/23, 03:32 PM	CohesitySecurity
Cohesity Create or Update ServiceNow in...	Microsoft Senti...	ServiceNow +1	Malware	ServiceNow SOAR	12/23/22, 03:32 PM	CohesitySecurity
Delete Cohesity incident blobs	Microsoft Senti...	Azure Blob St... +1	Malware	Cleanup	01/27/23, 04:27 PM	CohesitySecurity
Restore From Last Cohesity Snaps...	Microsoft Senti...	Azure Blob St... +2	Malware	Datahawk SOAR	01/13/23, 03:32 PM	CohesitySecurity
IN USE Cohesity Incident Email	Microsoft Senti...	Outlook.com +1	Malware	SOAR Email Notif...	12/23/22, 04:27 PM	CohesitySecurity

Delete Cohesity incident blobs

Description
This playbook deletes the blobs on Azure storage created by an incident that is generated by Cohesity function apps.

Connectors in use
Microsoft Sentinel Azure Blob Storage

Prerequisites
Deploy the Cohesity configuration and function apps (see details [here](#)).

Post deployment steps
Authorize all connections.

Source name
CohesitySecurity

Version
1.0

Supported by
Cohesity | Email

Author
Cohesity

Buttons: < Previous, Page 1 of 1, Next >, Create Playbook

3. Enter the field **details** and click **Next: Connections**:

- **Subscription**
- **Resource group**
- **Playbook Name**

The screenshot shows the 'Create playbook' wizard in the Microsoft Azure portal. The 'Basics' step is active, and the 'Connections' step is highlighted in blue. The form contains the following fields and options:

- Subscription ***: Azure subscription 1
- Resource group ***: SS-RG-Test (with a 'Create new' link)
- Region ***: East US
- Playbook name ***: My_Cohesity_Delete_Incident_Blobs
- Enable diagnostics logs in Log Analytics**
- Log Analytics workspace**: SS-WS-Test
- Associate with integration service environment**
- Integration service environment**: (empty dropdown)

A blue button labeled 'Next: Connections >' is located at the bottom of the form, with a mouse cursor hovering over it.

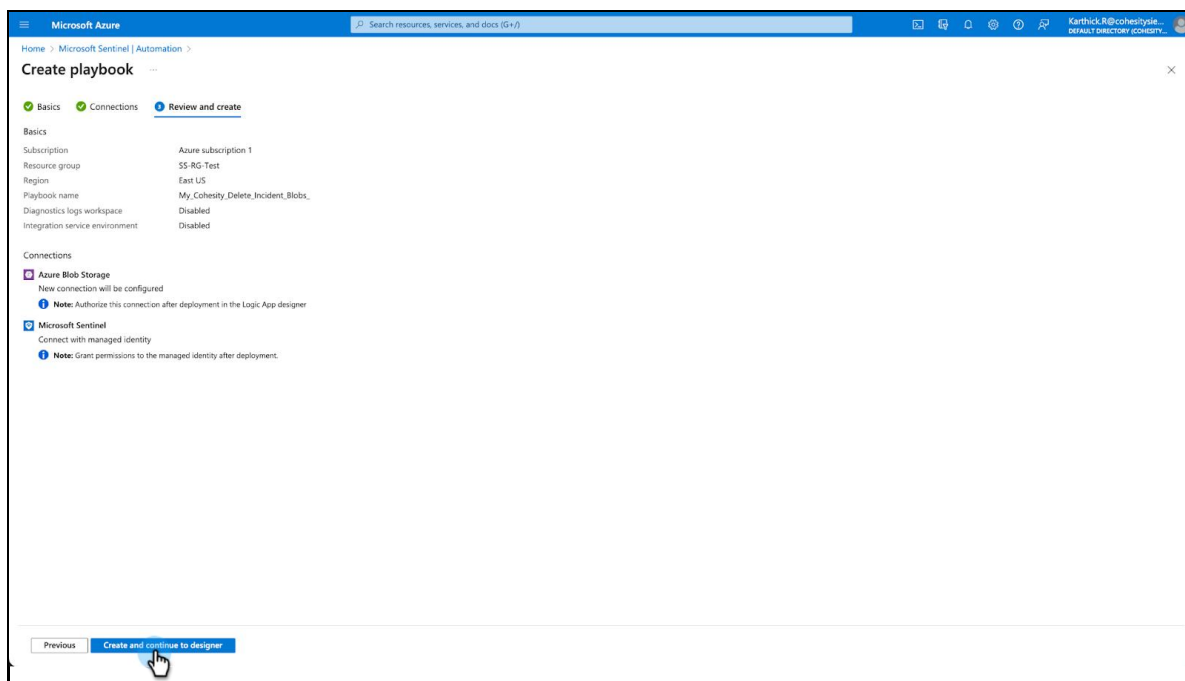
4. Click **Next: Review and create**. This will review and validate the parameter details.

The screenshot shows the 'Create playbook' wizard in the Microsoft Azure portal, now at the 'Connections' step. The 'Basics' step is marked as complete with a green checkmark. The 'Connections' step is active, and the 'Review and create' step is highlighted in blue. The form contains the following information:

- For each connector this playbook uses, you can choose to use an existing connection from another playbook. Otherwise, you must create a new connection and authenticate when you are brought to the Logic Apps designer after your playbook is deployed.
- Azure Blob Storage**: New connection will be configured
- Microsoft Sentinel**: Connect with managed identity

At the bottom of the form, there are two buttons: 'Previous' and 'Next: Review and create >'. A mouse cursor is hovering over the 'Next: Review and create >' button.

5. Click **Create and Continue to designer**. This will redirect to the Logic apps window to authorize the API connections.



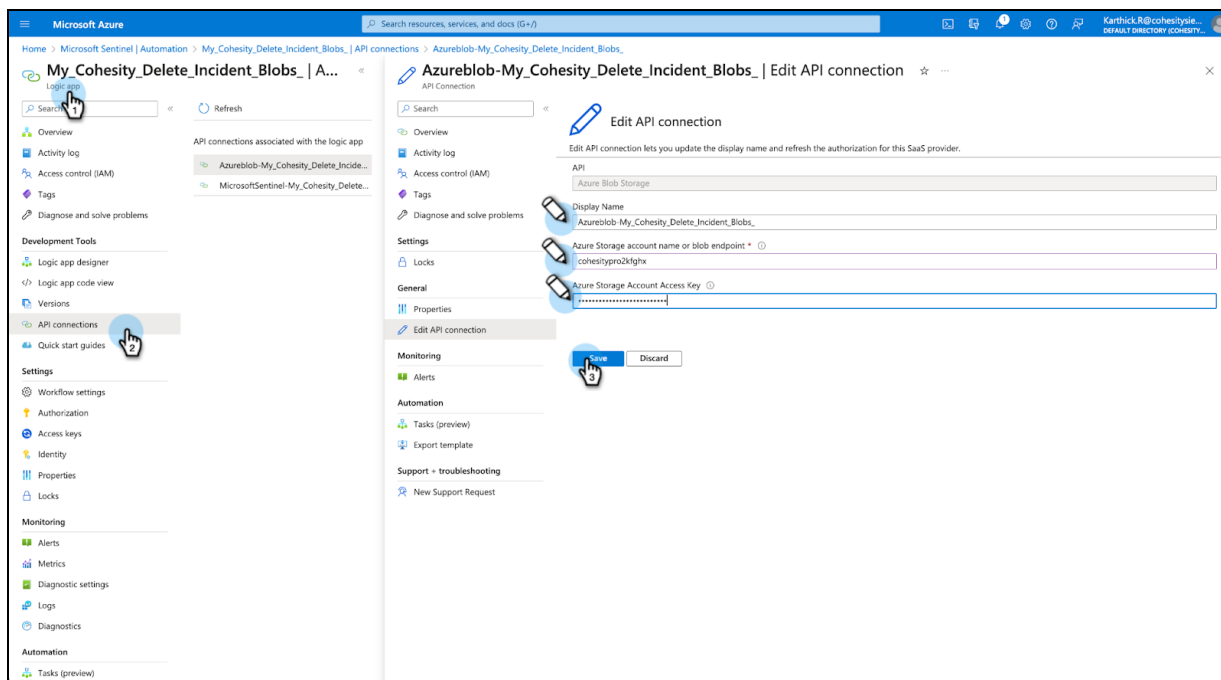
Authorize Connections to Microsoft Azure Blob Storage

After creating the playbook, you should authorize a connection from the Logic Apps to access Blob storage. Follow the below steps to authorize the connections:

1. Go to **Logic Apps** and choose your playbook.
2. In the **Development Tools** section, select **API Connections**. In the left pane, the list of connections is displayed that require authorization.
3. Authorize the Azure blob storage connection by selecting it and clicking **General > Edit API Connection**.

4. Enter your **connection name**, **storage account name (starts with Cohesitypro****)**, and **access key**.

NOTE: You can find your storage account name and access keys under **storage account tab** and then go to **Security + Networking > Access Keys**.



Create Automation Rule to Delete Azure Blobs

You can create an automation rule to delete the blobs used for an incident by running this playbook when the corresponding Sentinel ticket is closed. You need to perform the following configuration steps to create an automated rule for this playbook:

1. In Microsoft Sentinel, go to the **Automation** tab under the **Configuration** pane.
2. Click **Create > Automation Rule**.
3. From the automation rule panel, enter the **Field details**, and click **Apply**.
 - **Automation rule name** - <Enter a name for your rule>.
 - **Trigger** - <From the Trigger drop-down, select the appropriate trigger according to the circumstance for which you're creating the automation rule such as when the incident is updated>.
 - **Conditions** - <Define the conditions to match>.
 - **Actions** - <Add a run playbook action, you will be prompted to choose from the drop-down list of Cohesity playbooks>.
 - **Rule Expiration** - <Set an expiration date for your automation rule if you want it to have one>.
 - **Order** - <Enter a number under Order to determine where in the sequence of automation rules this rule will run>.

The screenshot shows the 'Create new automation rule' dialog in the Microsoft Sentinel Automation console. The dialog is configured with the following details:

- Automation rule name:** Delete-Cohesity-Incident-blobs
- Trigger:** When incident is updated
- Conditions:**
 - If Incident provider: Equals, All
 - Analytic rule name: Contains, All
 - Status: Changed To, Closed
 - Description: Contains, Helios ID
- Actions:** Run playbook (My_Cohesity_Delete_Incident_Blobs)
- Rule expiration:** Indefinite
- Order:** 3

Restore From Last Cohesity Snapshot Playbook

This playbook allows you to restore your data from a clean snapshot. After you assign the [permissions to the playbook](#), you need to perform the following configuration steps to enable this playbook:

1. From the workspace, under the **Configuration** pane, navigate to the **Automation** tab and select **“Restore from last Cohesity Snapshot”**.
2. Click **Create playbook**.

The screenshot shows the 'Restore From Last Cohesity Snapshot' playbook template in the Microsoft Sentinel Automation console. The template is highlighted in the 'Playbook templates (Preview)' section. The details pane on the right shows the following information:

- Name:** Restore From Last Cohesity Snapshot
- Trigger:** All
- Logic Apps Connectors:** All
- Entities:** Malware
- Tags:** DataH
- Description:** This playbook restores the latest good Data Hawk (Helios) snapshot.
- Connectors in use:** Microsoft Sentinel, Azure Blob Storage, Azure Key Vault
- Prerequisites:** Deploy the Cohesity configuration and function apps (see details here).
- Post deployment steps:** Authorize all connections.
- Source name:** CohesitySecurity, **Version:** 1.0
- Supported by:** Cohesity | Email, **Author:** Cohesity

3. Enter the **field details** and click **Next: Connections**:

- **Subscription**
- **Resource group**
- **Playbook Name**

Microsoft Azure | Search resources, services, and docs (G+)

Home > Microsoft Sentinel | Automation >

Create playbook

1 Basics 2 Connections 3 Review and create

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure subscription 1

Resource group * SS-RG-Test

Region * East US

Playbook name * My_Cohesity_Delete_Incident_Blobs

Enable diagnostics logs in Log Analytics

Log Analytics workspace SS-WS-Test

Associate with integration service environment

Integration service environment

Next: Connections >

4. Click **Next: Review and create**. This reviews and validates the parameter details.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Microsoft Sentinel | Automation >

Create playbook

1 Basics 2 Connections 3 Review and create

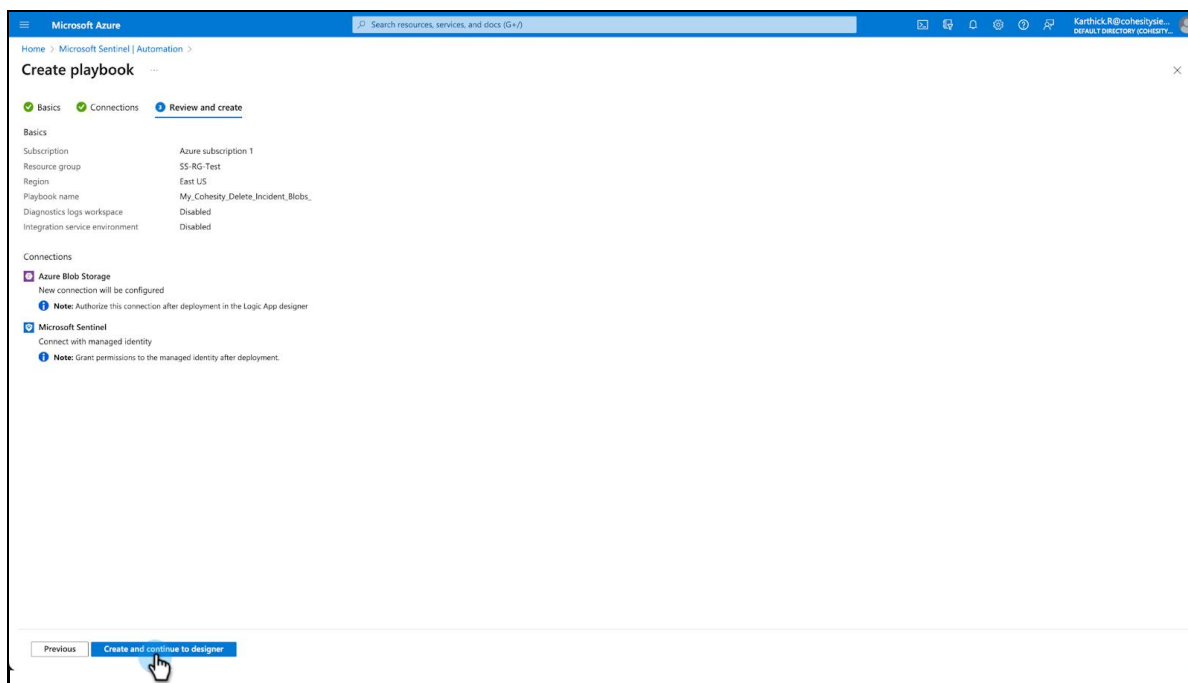
For each connector this playbook uses, you can choose to use an existing connection from another playbook. Otherwise, you must create a new connection and authenticate when you are brought to the Logic Apps designer after your playbook is deployed.

Azure Blob Storage New connection will be configured

Microsoft Sentinel Connect with managed identity

Previous Next: Review and create >

5. Click **Create and continue to designer**. This will redirect to the Logic apps window to authorize the API connections.

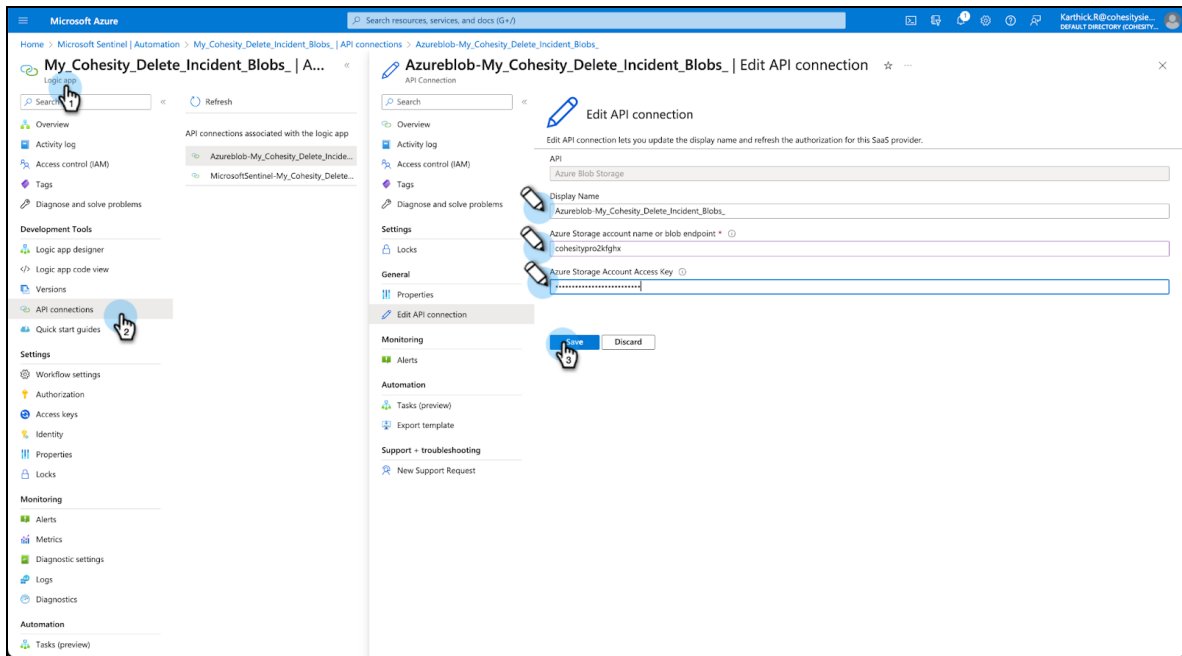


Authorize Connections to Microsoft Azure Blob Storage

After creating the playbook, You should authorize a connection from the Logic Apps to access Blob storage. Follow the below steps to authorize the connections:

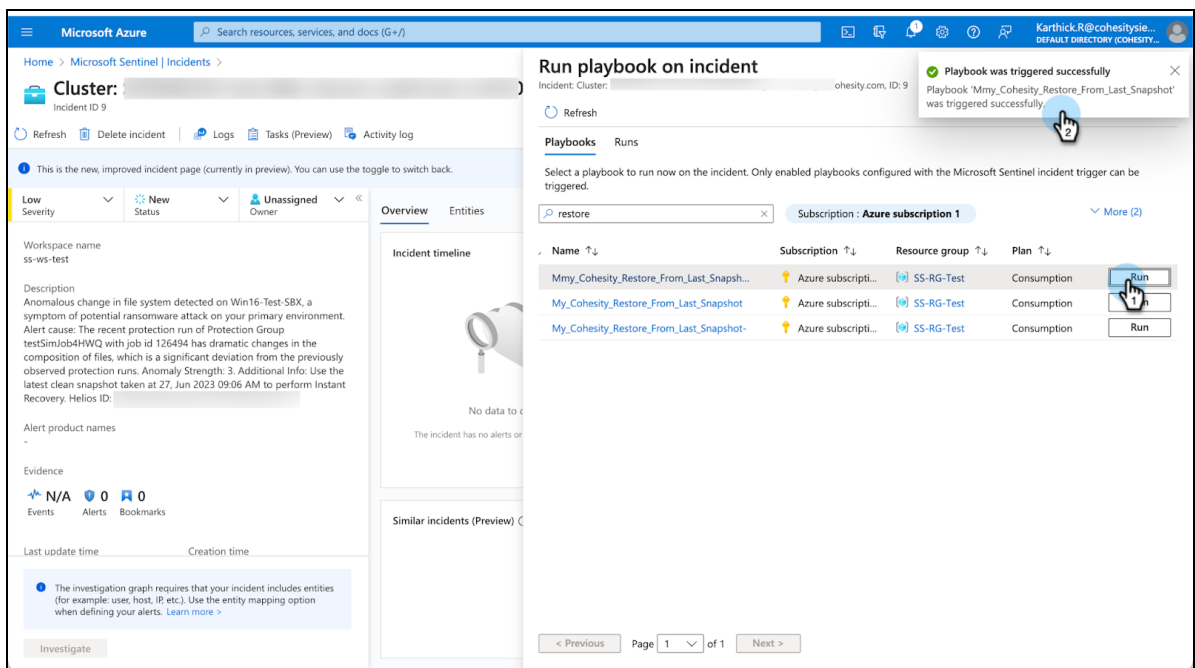
1. Go to **Logic Apps** and choose your playbook.
2. In the **Development Tools** section, select **API Connections**. In the left pane, the list of connections is displayed that require authorization.
3. Authorize the Azure blob storage connection by selecting it and clicking **General > Edit API Connection**.
4. Enter your connection name, storage account name (starts with Cohesitypro****), and access key.

NOTE: You can find your storage account name and access keys under **storage account tab** and then go to **Security + Networking > Access Keys**.

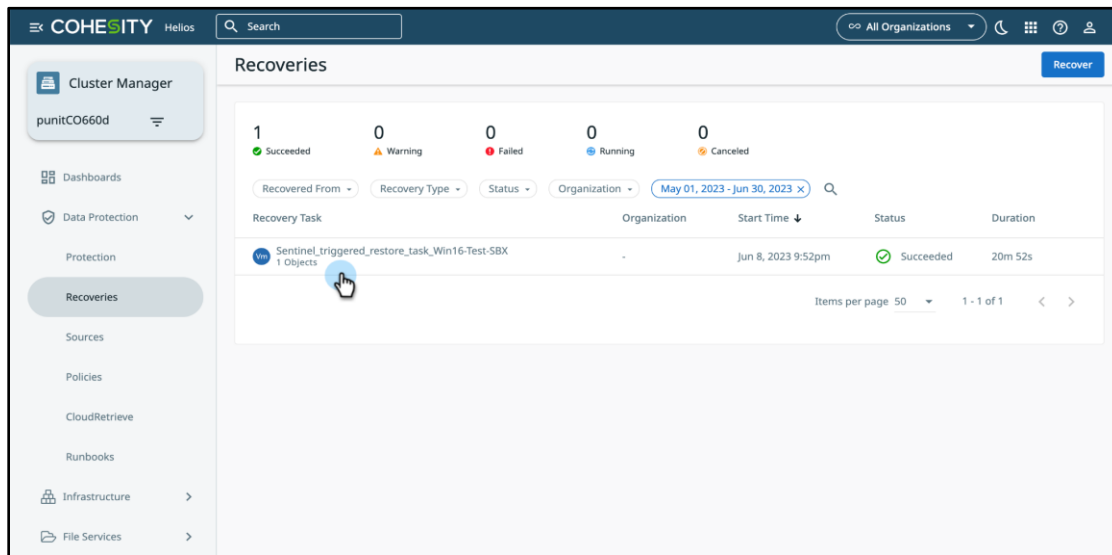


- After adding connections to **Microsoft Azure Blob Storage**, the next step is to [Grant KeyVault Permissions](#) for the playbook to access the objects.
- Once the permissions are granted, go to the **Incidents** tab under the selected workspace, and select **Run** to trigger the playbook after investigating the incident.

NOTE: Cohesity recommends that only a backup administrator should have the necessary permissions to run **Restore from Last Snapshot** as it involves handling sensitive user data.



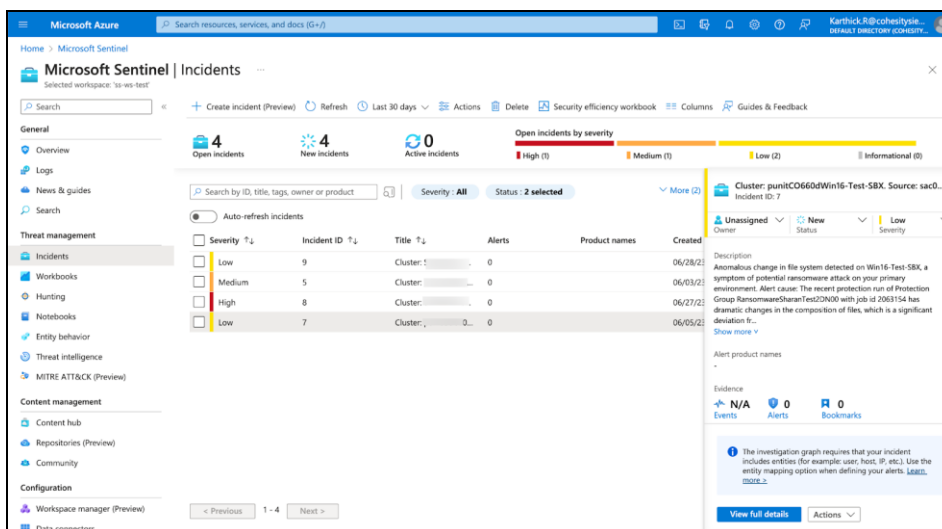
- This will trigger the **Restore** action from the last clean snapshot on Cohesity Helios from the Microsoft Sentinel platform.



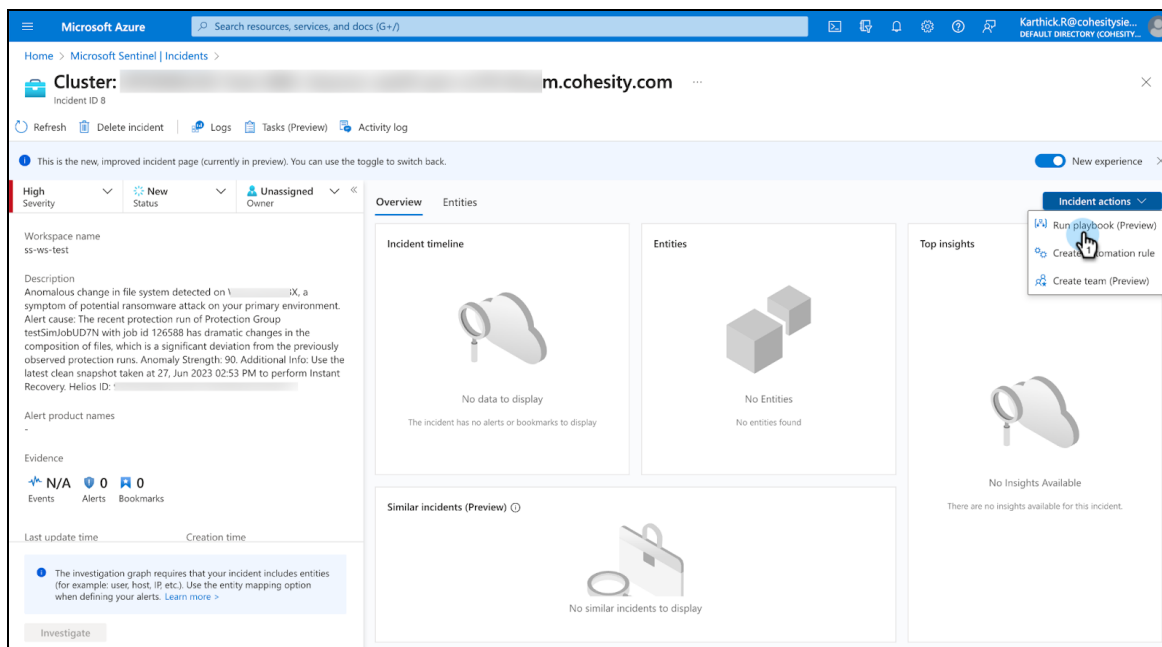
Investigate an Incident

After you successfully configure the playbook on Microsoft Sentinel, you can investigate your Anomaly alert triggers from Cohesity Data cloud more quickly, effectively, and efficiently, thereby reducing your mean time to resolve (MTTR).

- From the Microsoft Sentinel navigation menu, under **Threat management**, select Incidents. The Incidents page gives you basic information about all of your open incidents whether they are new, active, or 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.



- 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 (Such as **Helios Id, Object Id, Description**, and the **cause of alert**).



- Once you check the incident, depending on the investigation, you can take multiple actions on it.
- From the incident pane, click **Actions > Run Playbook**.

The **Run Playbook** pane is displayed with the following playbooks.

- **Cohesity_Send_Incident_Email** - Sends an email to the recipient with the details related to the incidents.
- **Cohesity_CreateOrUpdate_ServiceNow_Incident** - Creates and updates the incident in the ServiceNow platform.
- **Cohesity_Close_Helios_Incident** - Allows you to resolve alerts on Cohesity Data Cloud.
- **Cohesity_Restore_From_Last_Snapshot** - Allows you to restore your data from a clean snapshot.
- **Cohesity_Delete_Incident_Blobs** - Deletes the blobs on Azure storage created by an incident that is generated by Cohesity function apps.

- You can choose to run any playbook after an alert Investigation to trigger the actions.

NOTE: Cohesity recommends that only a backup administrator should have the necessary permissions to run **Restore from Last Snapshot** and **Close Cohesity Helios Incident**.

Prerequisites

You have to meet the following prerequisites before starting the integration.

- A Cohesity Data Cloud user account with permissions to create and manage API keys and create a custom role. For more information, see [Access Management](#) in Cohesity Data Cloud documentation.
- Create new API keys on Cohesity Data Cloud to authenticate an application or script for management through APIs.
- If your organization uses ServiceNow Now Platform to track incidents, then you can integrate it with Cohesity Helios. You would need a ServiceNow user account with the required permissions to create and update any incident in the ServiceNow Now platform.[Optional]
- You should have an account on ServiceNow's Now Platform to add the instance details for configuring the ServiceNow playbook.
- Create an email address that you can use for sending out incident email notifications.
- Ensure you have assigned the relevant permissions to the playbook to operate and respond from MS Sentinel for automatic action.

Customer Benefits

Microsoft Sentinel integration with Cohesity Data Cloud enables organizations to enhance their security and data protection capabilities.

By integrating Cohesity with Microsoft Sentinel, customers can benefit from the following:

- **Unified threat visibility**—Allows organizations to have a unified view of anomaly events and data protection activities. Security and data protection teams can access a centralized dashboard within Microsoft Sentinel to monitor and analyze the Cohesity-generated anomaly events in real-time.
- **Intelligent threat detection and response**—Combined capabilities of Cohesity and Microsoft Sentinel enable advanced threat detection and response. The integration empowers security teams to quickly identify and respond to security incidents.
- **Streamlined incident management**—Anomalous events detected in Microsoft Sentinel can trigger automated responses within Cohesity, such as initiating data restores to a clean snapshot or creating the ServiceNow ITSM Incident, etc. This automation accelerates incident response and minimizes the impact of security incidents.
- **Compliance Adherence**—Cohesity's integration with Microsoft Sentinel supports compliance and auditing requirements. Organizations can adhere to regulatory standards by leveraging the combined capabilities.

Conclusion

In conclusion, the integration of Microsoft Sentinel with Cohesity brings together security and data protection functionalities, allowing organizations to streamline their security operations, enhance threat detection and response, and ensure the availability and integrity of their data. This integration provides a holistic approach to managing security incidents and protecting critical data assets.

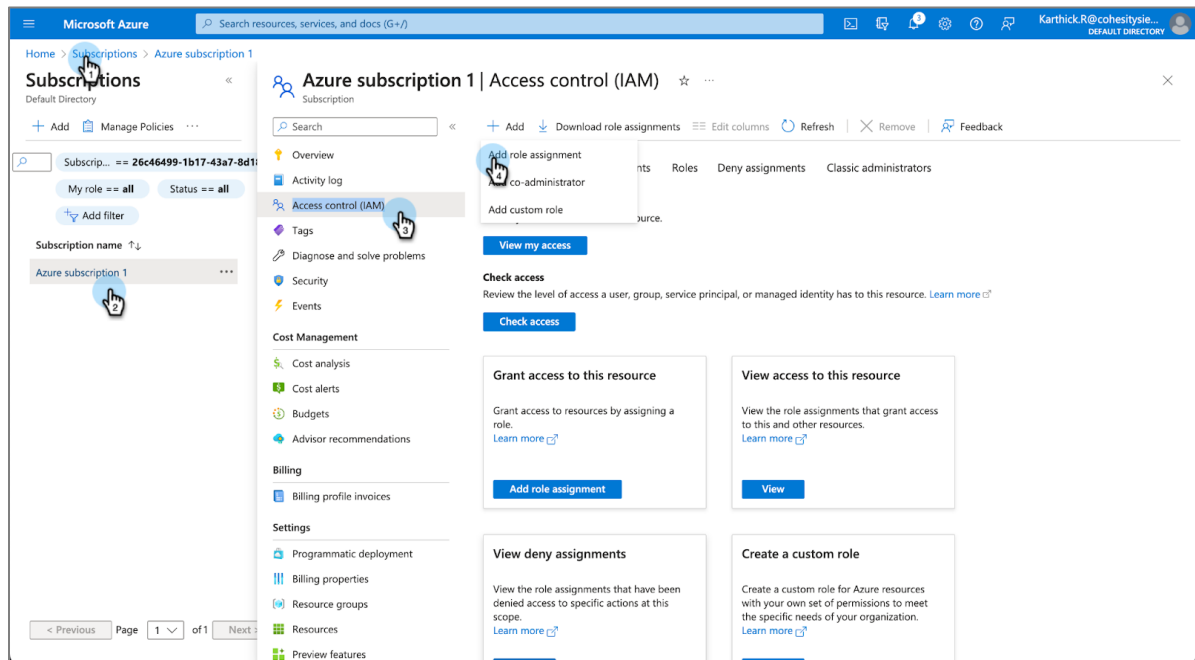
Appendix A

Set Required Permissions to Access Playbook

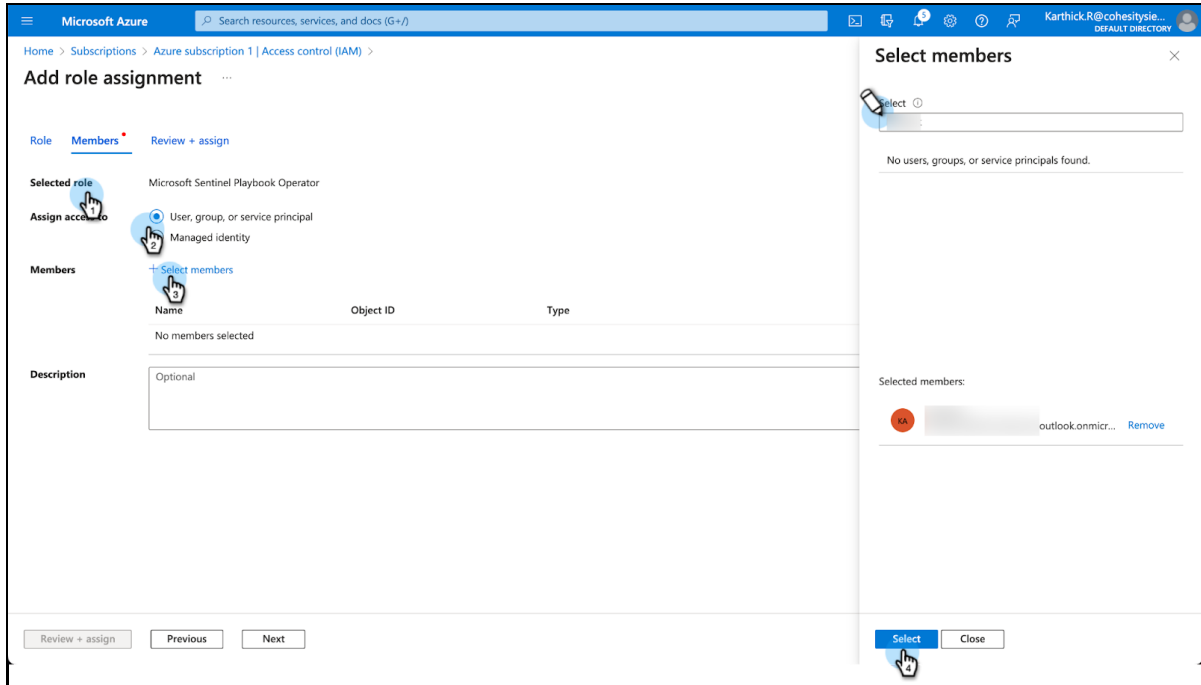
The SOC analyst must have the role of **Microsoft Sentinel Playbook Operator** to run the playbook.

To assign the role:

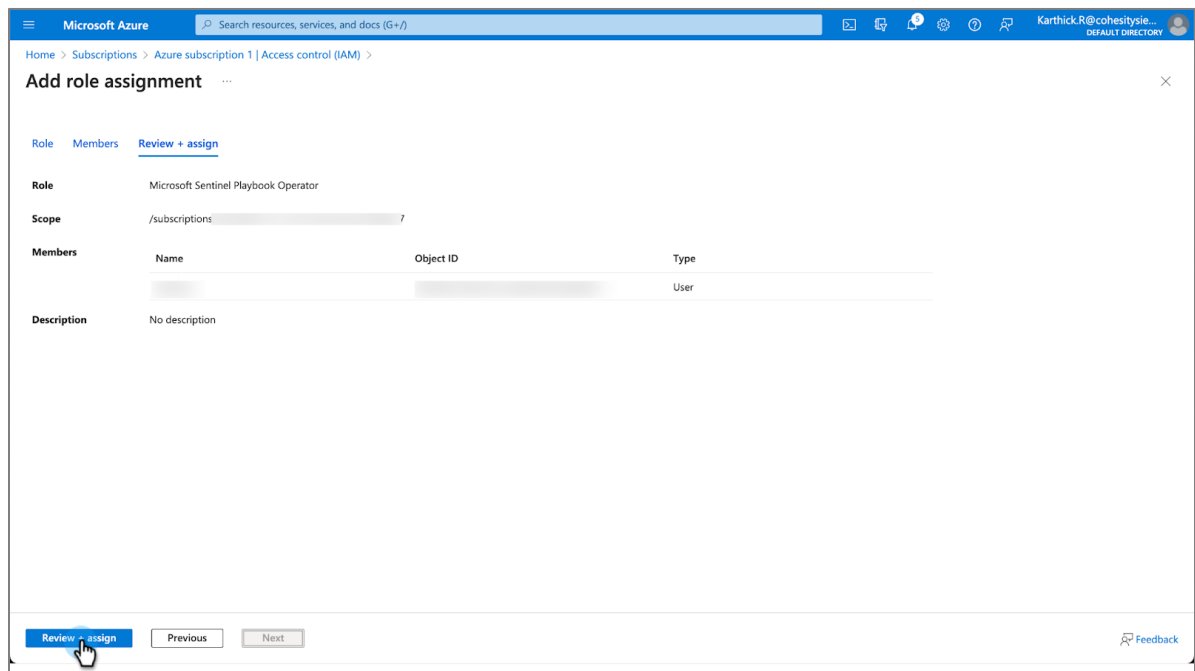
1. Under the **Subscriptions** tab from the **Home** page, choose your subscription name.
2. On the left pane, select **Access Control (IAM)**.
3. Select **Add > Add Role Assignment**.



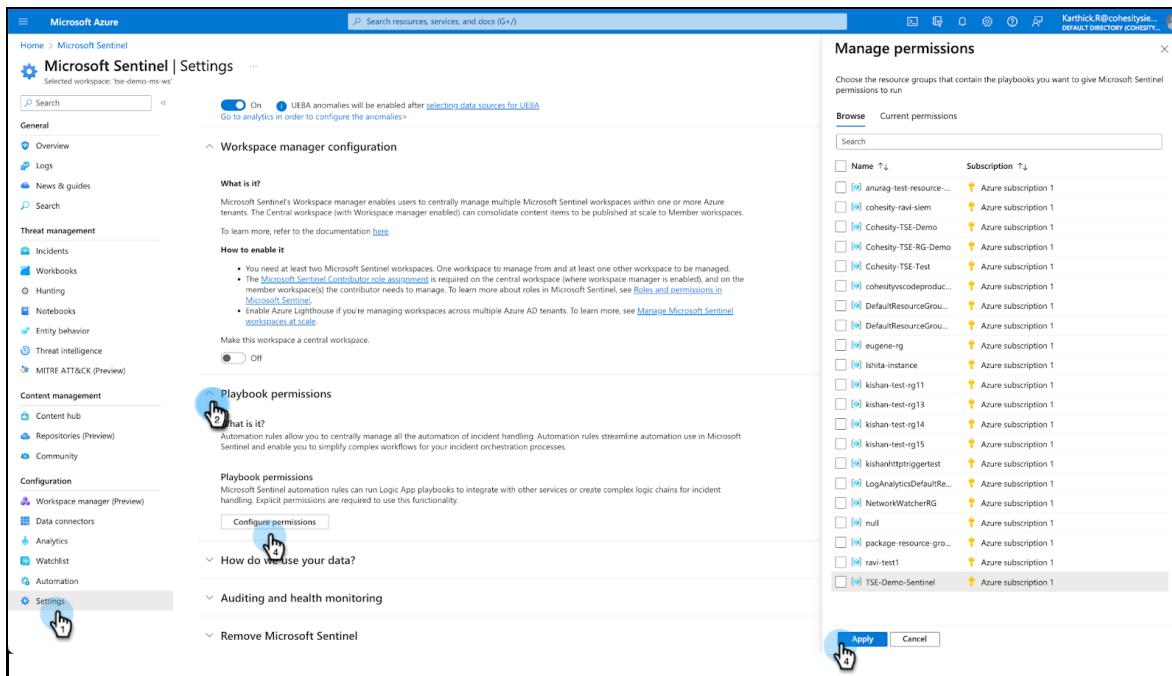
4. Add **Microsoft Sentinel Playbook Operator** to the user.



5. Click **Next** and select **Review + Assign**. This will assign the **Microsoft Sentinel Playbook Operator permissions** to an analyst.



6. After assigning the user permissions you can configure the playbook permission for **Resource group** which allows you to centrally manage all the automation of incident handling. From the Workspace, select **Configuration> Settings> Settings> Playbook permissions**.
7. Select **configure permissions** and select the **resource group name** that contains the playbooks you want to give Microsoft Sentinel permissions to run.



Grant KeyVault Permissions

Azure KeyVault protects cryptographic keys, certificates, and secrets on the Azure cloud.

Once you create the playbooks, then you need to assign the key vault permissions to specific playbook templates to access the objects after deploying the playbooks template.

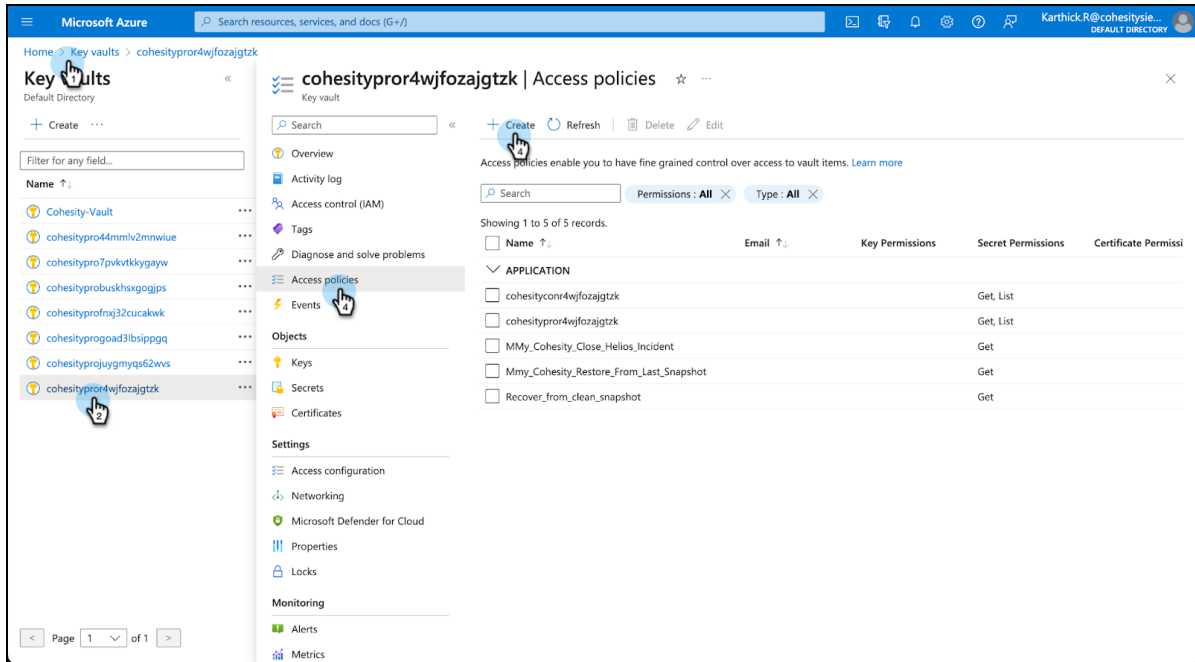
The playbooks templates which require Keyvault permissions are:

- Cohesity Close Helios Incident
- Delete Cohesity Incident Blobs
- Restore From Last Cohesity Snapshot Playbook

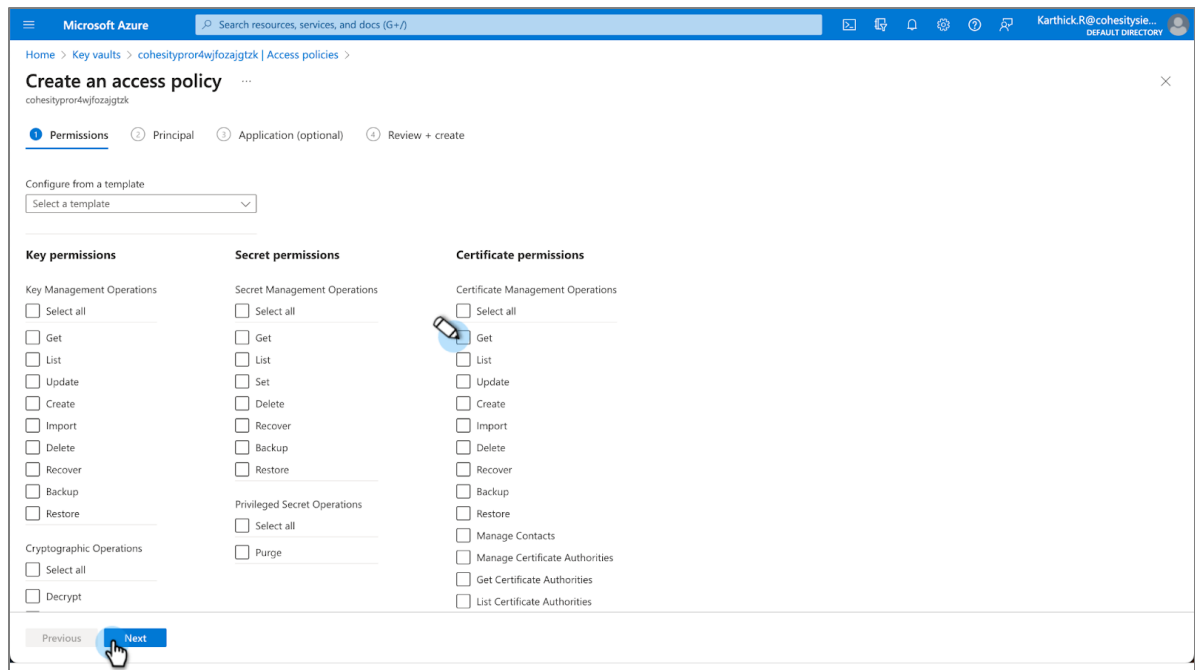
NOTE: Once you create the playbooks, then you need to assign the key vault permissions to specific playbooks mentioned.

To grant the permissions:

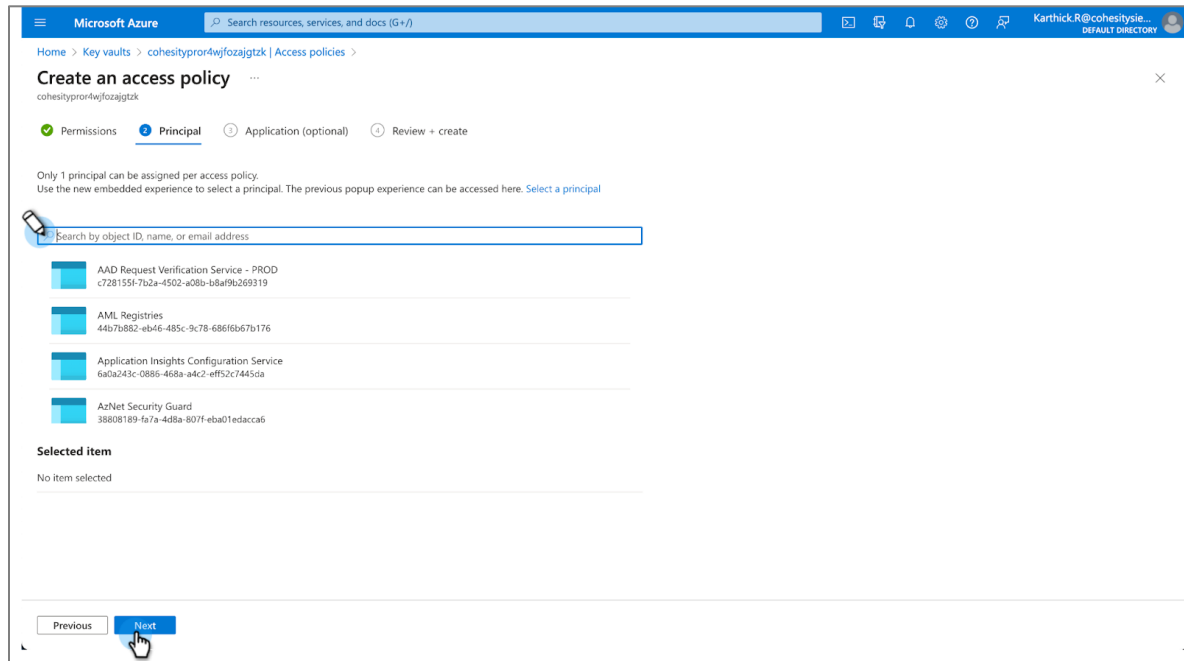
1. Go to [Key vaults](#) and choose your **keyvault** that starts from cohesitypro and is followed by a sequence of letters and numbers. For example, cohesityprofnxj32cucakwk.
2. On the right pane, select **Access Policies** and click **Create**.



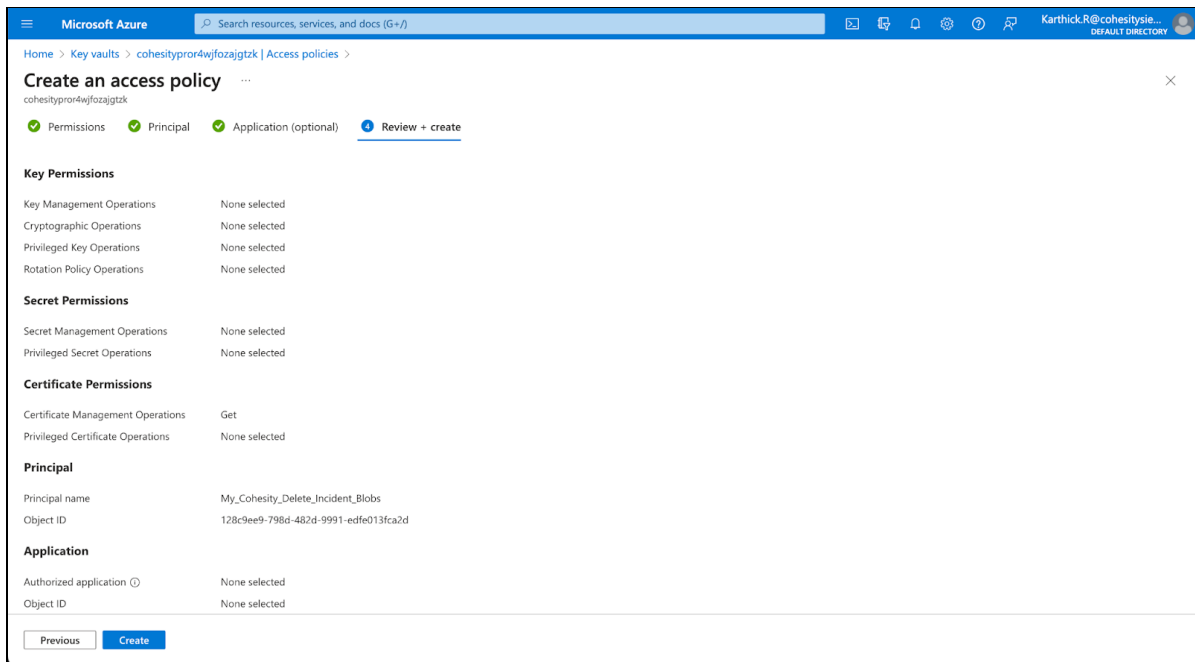
3. Choose **Get** permission in the **Secret Permissions** section and click **Next**.



4. Enter your playbook name and click **Next**.



5. Select **Next** and **Create** to finish granting permissions.



Terminology

Terms	Description
Workspace	The workspace is the top-level resource for all your activities under Azure instance, providing a centralized place to view and manage the artifacts and store events and other information.
Resource group	A container that contains related resources for a particular workspace.
Playbook	A playbook is a collection of these remediation actions that you run from Microsoft Sentinel as a routine, to help automate and orchestrate your threat response.
SIEM	Security Incident and Event Management (SIEM) aggregates and correlates logs from infrastructure such as Cohesity Data Cloud to generate incidents to manage in a centralized location.
SOAR	Security Orchestration, Automation, and Response (SOAR) technology helps coordinate, execute, and automate tasks between various people and tools—all within a single platform to reduce the MTTD and MTTR metrics.

Your Feedback

Was this document helpful? [Send us your feedback!](#)

About the Authors

Shashanka SR, Sr. Solutions Architect - Focuses on Security, Cohesity Gaia and GSI.

Other essential contributors included:

- Karthick Radhakrishnan, Director, Solutions Architecture
- Rob Young, Product Manager, Competitive Intelligence
- Robert Shields, Director, Product Marketing
- Mary Juliya, Technical Editor
- Kishan Nerella, Engineering
- Luke Walker, Product management

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.3	Feb 2026	Minor Updates
1.2	Aug 2025	Republished with latest template
1.1	July 2024	Republishing
1.0	Aug 2023	First full release

ABOUT COHESITY

[Cohesity](#) is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

Visit our [website](#) and [blog](#), follow us on [Twitter](#) and [LinkedIn](#) and like us on [Facebook](#).

© 2026 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, DataHawk, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.