COHESITY

Version 1.0

March 2024

Integrate Cisco XDR with Cohesity Data Cloud

ABSTRACT

Cohesity Data Cloud provides cyber resilience with AI-powered modern data management and protection capabilities. Integrating it with a SOC 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 Cisco XDR platform with Cohesity Data Cloud to enhance the security visibility, investigation, and rapid response of Cohesity incidents to protect customer-critical data with the Cohesity playbooks and automation capabilities to reduce the risk of data loss and minimize the business disruptions.

Table of Contents

Figures

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 lock up production systems, destroy backups, and steal sensitive data, which leaves your enterprise with no option but to pay a ransom.

When you are in a cyberattack, the speed of your response matters. Nowadays, the median ransomware variant can encrypt 100,000 files in just 43 minutes. Every second counts as you scramble to minimize the extent of data loss and disruption to business-critical applications.

Cyber resiliency is top-of-mind for Cohesity as we develop our product capabilities, and we're pleased to announce **new adaptive and automated data protection capabilities**—designed to help customers significantly reduce their risk of data loss in a cyberattack using real-time threat intelligence sharing and an accelerated threat response approach.

At the earliest signs of ransomware, Cohesity DataProtect will preserve potentially infected virtual machines for future forensic investigation while protecting data and workloads in the rest of the environment. As a result, InfoSec teams are intrinsically more proactive in data protection, ensuring they have a quick recovery point in case the threat proves to be real.

This integration between Cohesity DataProtect and Cohesity DataHawk with Cisco Extended Detection and Response (XDR) helps you detect and aggregate anomaly events before orchestrating a 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.

Cisco XDR Overview

Cisco XDR collects and correlates data across email, endpoints, servers, cloud workloads, and networks, enabling visibility and context into advanced threats. Threats can then be analyzed, prioritized, hunted, and remediated to prevent data loss and security breaches.

Cisco XDR's approach is designed around an integrated platform experience. As XDR is about organization and control, Cisco has broken down what it sees as the key components of any successful extended detection and response solution:

- **X: eXtended:** The platform should cover as many control points and data sources as possible. A security solution is only as good as the vulnerabilities it can cover.
- **D: Detection:** Machine learning-supported analysis decreases MTTD and lets security professionals make better decisions.
- **R: Response:** Automation and centralized security information means faster response times and streamlined security breach investigations.

To learn more about Cisco XDR, refer to Cisco.com.

Cohesity Data Cloud Overview

Cohesity Data Cloud is a unified platform for securing, managing, and extracting value from your data, that reduces your attack surface, lowers costs, and minimizes risk. Cohesity Data Cloud is available as self-managed software and SaaS with rich features, including:

- **Modern Backup and Recovery**—The most comprehensive, modern, web-scale data management and backup and recovery solution to protect cloud-native, SaaS, and on-prem data at scale. You get instant recovery at scale and with direct-metadata snapshots (so that each backup performs like a synthetic full), the ability to instantly put backed-up file shares online, and continuous data protection (CDP).
- **Traditional and Modern Workloads**—Support for VMs, databases, files, containers, cloud-native, SaaS, Storage, and traditional workloads.
- **Defend Against Ransomware Attacks**—Multilayered security architecture with Zero Trust Security, including granular RBAC, MFA, SSO, immutable snapshots, and ML-based ransomware attack detection. Protect and recover against ransomware with threat protection, cyber vaulting, and ML-powered data classification.
- **Threat Protection and Data Classification**—Highly curated and managed threat feeds, trained with ML, threat detection and response to your specific needs by augmenting the extensive library of over 117,000 behavioral patterns, create multiple YARA rules defining Indicators of Compromise (IOC), or import custom rules. Highly accurate NLP and ML-based engine to classify sensitive data, automatically or on-demand, including personally identifiable information (PII), PCI, and HIPAA.
- **Global Search and Unified Management**—Reduce recovery point objectives to minutes by eliminating slow-to-access, chain-based backups. A single management platform offering multilayered security architecture, unifying operations with integrated solutions for backup, CDP, DR, search, ransomware attack detection, and vulnerability scanning into a single scalable environment.
- **Cloud Vault**—Cohesity FortKnox is a SaaS cyber vaulting and recovery solution that gives your data additional layers of managed security and protection against cybersecurity threats. To learn more, refer to Cohesity product documentation.
- **Cloud Archive**—Policy-based data archival to meet long-term data retention, compliance, and regulatory requirements.
- **Cohesity Cloud Services**—Cohesity-managed data security and management with SaaS that runs multiple cloud data services, including backup, cyber vaulting, threat defense, data classification, DR, and more on a single multi-cloud platform.
- **Cohesity Gaia**—combines generative AI with your enterprise data. Unlock data insights by bringing retrieval augmented generation (RAG) AI and large language models (LLMs) to enterprise data within Cohesity. Ask natural language questions and get context-rich answers.
- **Business Continuity**—Simplify business continuity and disaster recovery with automated failover and failback orchestration for your mission-critical workloads. Get your critical applications online after a breach or outage through automated orchestration.
- **Security Integrations**—Cohesity integrates with leading perimeter and end-point security vendors, giving you greater visibility and actionable alerts in your Security Operations Center (SOC).

- **Deployment**—Software-defined solution for on-premises, public cloud, backup as a service, and edge sites.
- **API-first Extensibility**—Derive business insights with the Cohesity Marketplace partner ecosystem. Streamline operations and easily integrate on-prem and cloud environments with pre-built automated workflows and API integrations.

To learn more about how Cohesity provides **AI-powered data security and management**, refer to Cohesity.com.

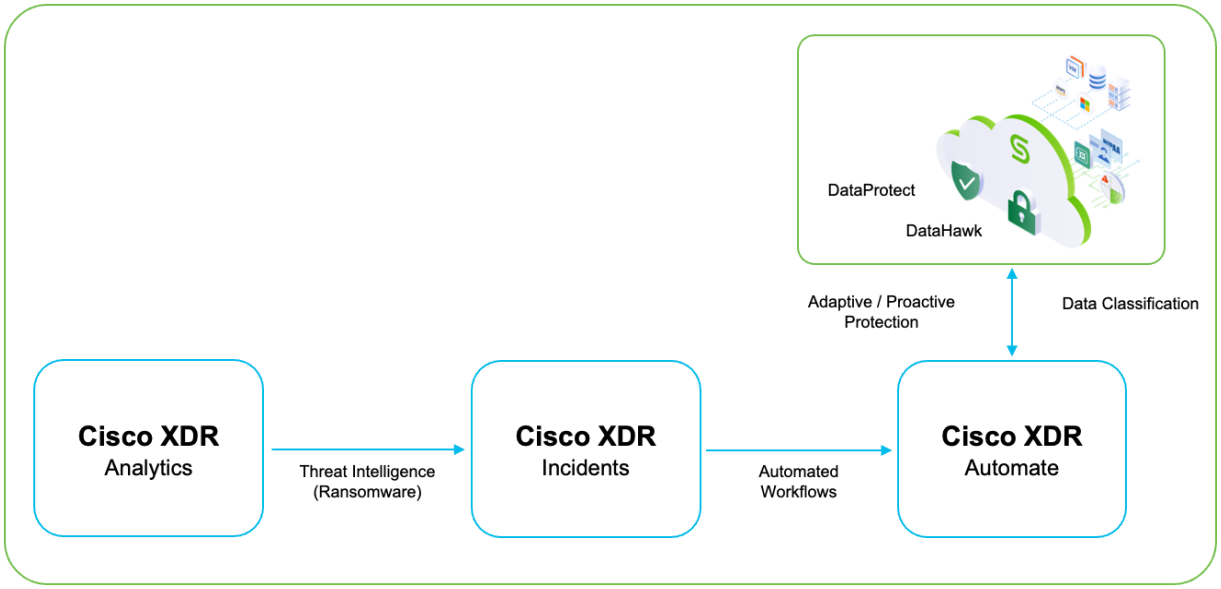
Cohesity Cisco XDR Integration Overview

Cohesity enables you to integrate **Cohesity DataProtect** and **Cohesity DataHawk** with **Cisco XDR,** which allows you to automatically add adaptive data protection to your cyber threat response process to achieve a near-zero recovery point objective (RPO). It automates critical data protection based on early warning signs of a malware infection detected by Cisco XDR to reduce your data loss significantly.

The integration provides the ability to:

- Automate threat response.
- Accelerate data recovery.

Figure 1: Cohesity – Cisco XDR Integration

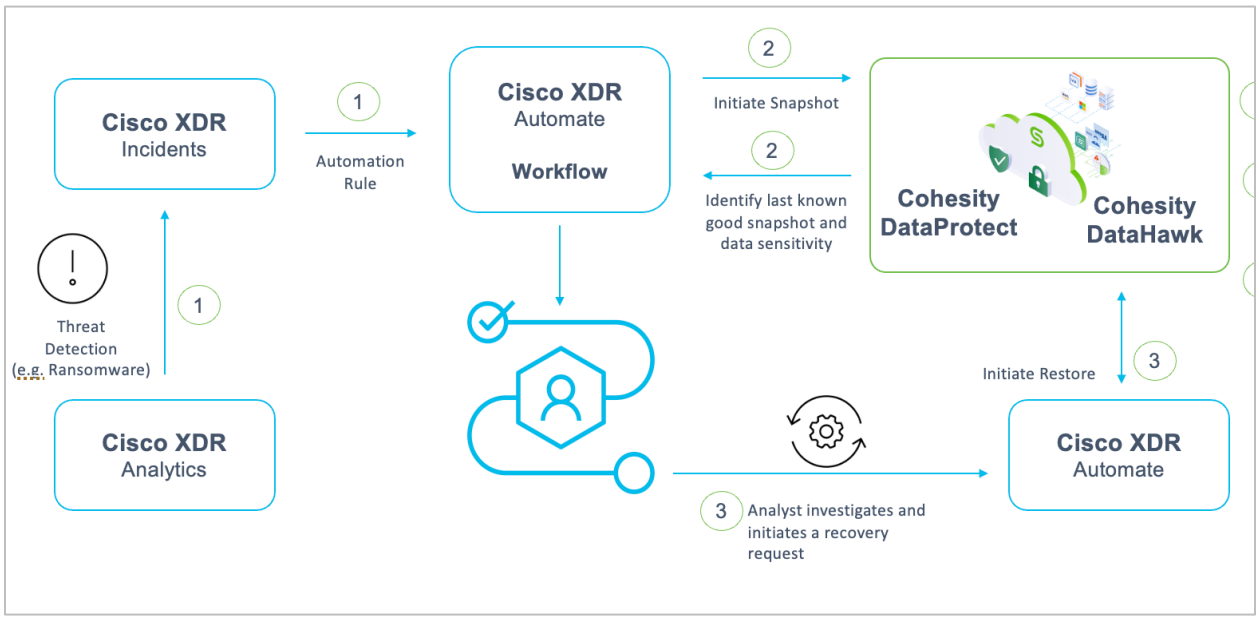


High-Level Integration Workflow

Cohesity's new integration complements Cisco XDR's robust detection, correlation, and integrated response capabilities, enabling customers to benefit from accelerated response for data protection and automated recovery from potential ransomware attacks as soon as the intrusions are detected.

Consider a typical multi-tier web application that is connected to multiple critical workloads. Each workload is backed up by Cohesity Data Protect within a protection group policy, monitored by Cisco XDR for threats and malicious activity, and tagged for sensitive data by the DataHawk Data Classification Engine.

Figure 2: Cohesity-Cisco XDR Workflow



Stage 1: During an attack / Potential Attack Detected

- Let's say that an attacker compromised the web server by exploiting a vulnerability or another vector. The attacker plants a malicious binary and begins reconnaissance to expand the attack. At this stage, Cisco XDR Analytics detects suspicious activity on the web server and assigns it a priority score based on potential risk with MITRE Tactics & Techniques mapping the attack chain.

Stage 2: Automate Data Protection and Classify Data

- Cisco XDR directs Cohesity DataProtect to initiate a backup run of the whole Protection Group using automatically triggered Cohesity workflows "**Cohesity - Take Protection Group Snapshot"** can help the organization reduce the risk of data loss and achieve a near-zero recovery point objective (RPO) This workflow takes a backup snapshot of the potentially infected VM and the rest of the VMs in the Protection Group, enabling adaptive and automated data protection. Cisco XDR also directs DataProtect to **identify viable restore points**, meaning data prior to encryption attacks, and **enriches the incidents in the Worklog notes**. Lastly, any data sensitivity information identified by **DataHawk's data classification capabilities** associated with the virtual machine will be added PII-related information to the XDR incident notes.

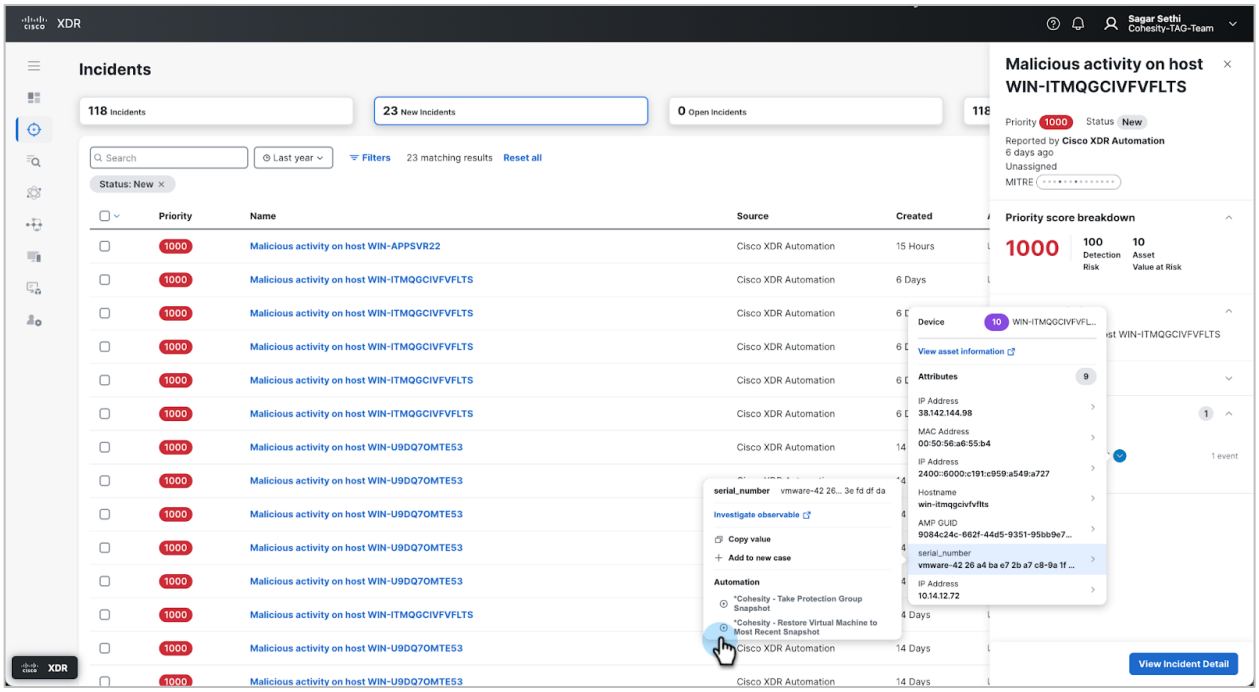
Stage 3: After an attack/ post-incident response

- Let's say the attacker was successful in laterally moving through the environment and detonating the ransomware, affecting large portions of the environment, and bringing down several critical applications. The organization's focus is now on the accelerated and safe recovery of critical workloads on priority, for which additional automatic backups are already taken during the early stages of the attack with **Cohesity Take Protection Group Snapshot Workflows**, which can help the organization reduce the risk of data loss and helps with the overall RTO.

Cohesity Supported Cisco XDR Workflows

The integration reduces the risk of data loss during an attack by ensuring that the most critical workloads are backed up more often when the ambient threat level is high. Below are the supported Workflows from Cohesity that you can use in Cisco XDR for proactive protection and restore operations within Cohesity Data Cloud:

1. **Pivot Menu Workflows**
   a. **Cohesity - Take Protection Group Snapshot:** The workflow enables you to capture snapshots of virtual machines into Cohesity cluster. Snapshots are taken for all virtual machines in the protection group to which the selected virtual machine belongs.
   When triggered from the pivot menu, the **"Take Protection group Snapshot"** workflow will:
      - **Search** Cohesity DataProtect for hosts that match the observable that was pivoted on.
      - **Find** the protection group for the host.
      - **Initiate** a protection policy run for the group and the specific host.



b. **Cohesity - Restore Virtual Machine To Most Recent Snapshot:** The workflow leverages Cohesity Data Cloud to restore the selected virtual machine to its most recent backup snapshot from prior to Cohesity detecting an anomaly indicative of an encryption attack. The user remains responsible for leveraging Cisco XDR, Cohesity DataHawk, or other tools to assess whether that backup contains malware or is otherwise compromised.

When triggered, the "**Restore Virtual Machine to Most Recent Snapshot**" workflow will:

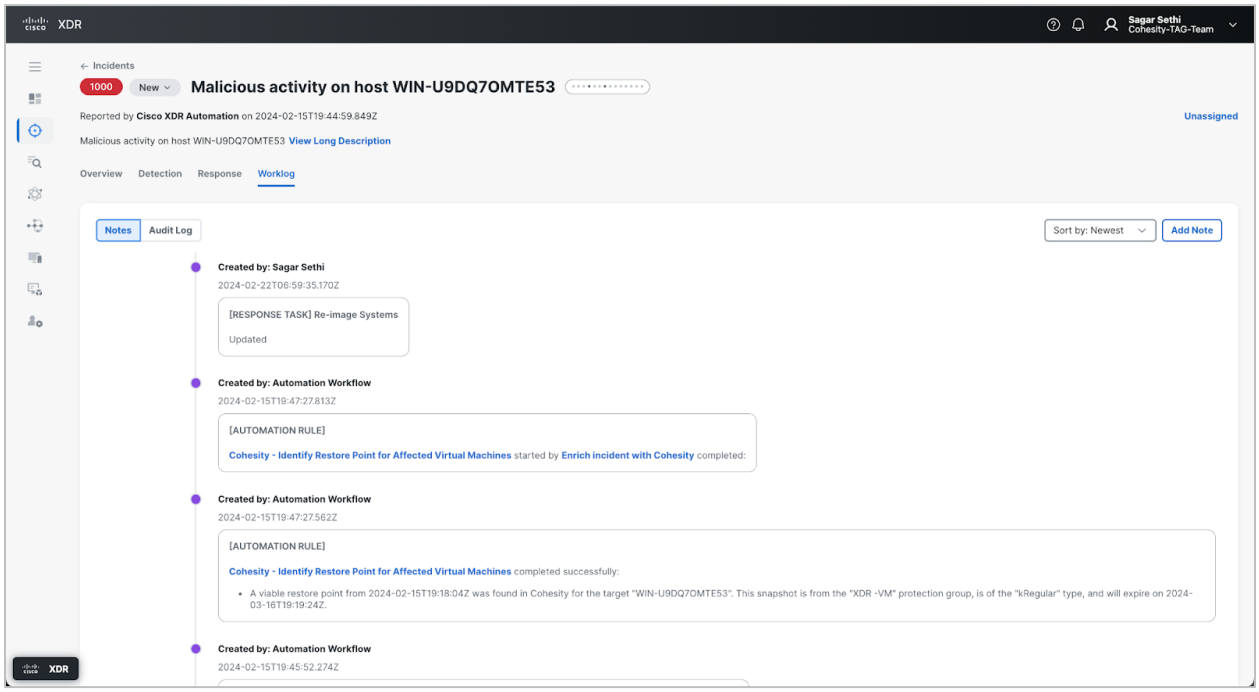
- Search Cohesity DataProtect for hosts that match the observable that was pivoted on.
  - Get the **host's snapshot summary** and extract the **cluster-ID**.
  - Get a **list of snapshots** for the host.
  - **Parse the snapshots** to find the Latest non-anomalous snapshot (before the workflow start time) and not expire.
- **Initiate** a recovery for the snapshot identified as the latest non-anomalous snapshot.

2. **Automation Workflows**

a. **Cohesity - Identify Restore Point For Affected Virtual Machines:** The workflow is triggered by an automation rule as soon as an incident is created in Cisco XDR. Once triggered, the workflow retrieves the list of virtual machine assets associated with the incident and then determines the most recent and viable restore point, meaning the latest backup made prior to detecting an anomaly indicative of encryption attacks, for each virtual machine in Cohesity Data Cloud. The user remains responsible for leveraging Cisco XDR or Cohesity DataHawk or other tools to assess whether that backup contains malware or is otherwise compromised. When triggered, the workflow will:

- **Search** Cohesity DataProtect for hosts that match the targets in the incident.
- For each host that's found:
  - Get the **host's snapshot summary** and extract the first **cluster-ID**.
  - Get a **list of snapshots** for the host.
  - **Parse the snapshots** to find the **most recent non-anomalous snapshot** (before the incident started time) and not expired.

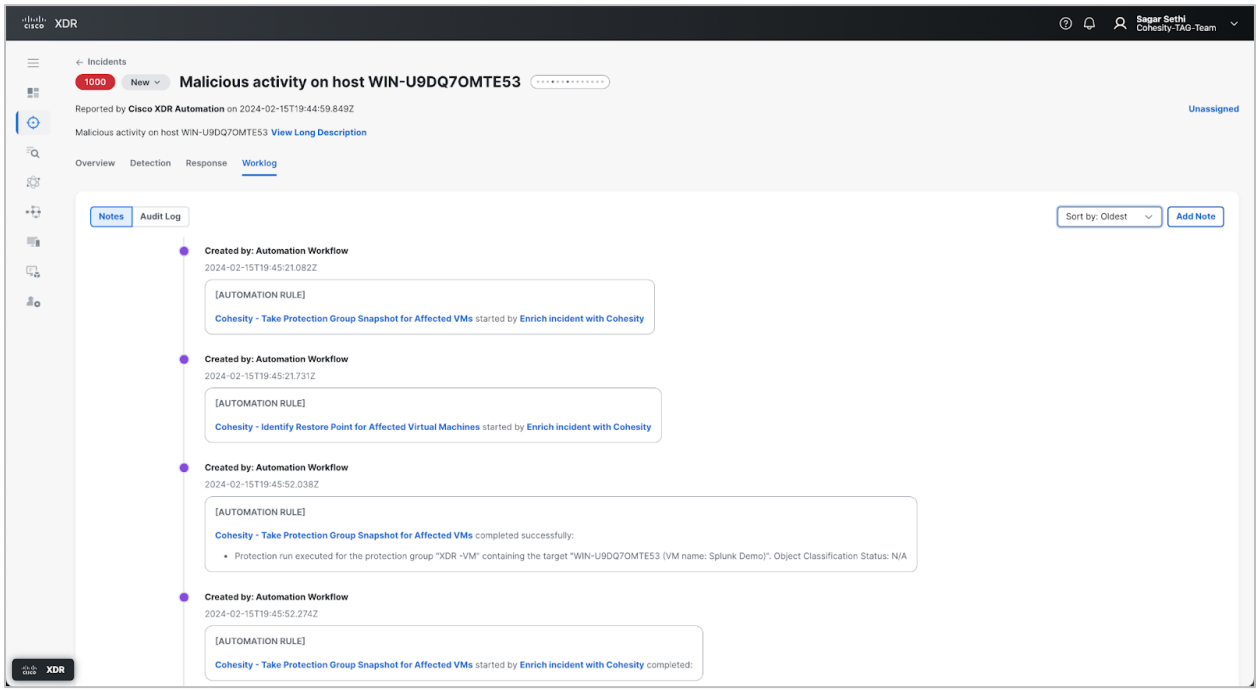
- Post a **Worklog note** to the incident with a summary.



b. **Cohesity - Take Protection Group Snapshot For Affected VMs:** The workflow is triggered by an automation rule immediately after an incident is created in Cisco XDR. Once triggered, the workflow identifies all virtual machine assets mentioned in the incident. It uses Cohesity Data Cloud to take a snapshot of the Protection Group to which each virtual machine mentioned in the incident belongs. Additionally, any data sensitivity information associated with the virtual machine is added to the incident notes. This workflow will:

- **Search** Cohesity DataProtect for hosts that match the targets in the incident.
- For each host that's found.
  - **Find** the best protection group for the host.
  - **Initiate** a protection policy run for the group and the specific host.

- Post a **work log note** about the incident with a summary.



Integration Benefits

Cisco XDR integration with Cohesity Data Cloud enables organizations to enhance their security and data protection capabilities and minimize the time from detection to action during a ransomware attack.

By integrating Cohesity with Cisco XDR, customers can achieve below benefits:

- **Adaptive and Automated Response**-Enhance the incident response and alert investigation with an 'intelligent' approach based on Cisco XDR threat detection. Cohesity proactively takes a snapshot of the group, including the detected threat to provide more information for a quick and precise response. Shortening the time to identify, isolate, and eradicate the threat before recovery helps with the overall RTO.
- **Classification of sensitive data**- Scan critical workloads backed up by Cohesity and monitored by Cisco XDR for threats using Cohesity DataHawk's highly accurate, NLP and ML-based engine to classify sensitive data, including PII, PCI, and HIPAA.
- **Multi-layered Protection for Snapshots-**Stop bad actors and unauthorized applications from modifying or deleting your data, thanks to Zero Trust Principles, including granular RBAC, MFA, SSO, immutable snapshots, ML-based ransomware attack detection, and more.
- **Instant Recovery**- Dramatically reduce recovery time with unlimited and fully hydrated snapshots without impacting performance. Leverage a built-in workflow in Cisco XDR to recover a snapshot for any asset protected by Cohesity automatically.

Prerequisites

You must 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.
- Supported Cohesity cluster version is 6.8 and above and VMware.
- Be sure to add one or more workloads to protection groups with policies configured to take periodic snapshots.
- Access to a functional Cisco XDR instance.
- Deploy the Cisco Secure client and Cloud management agent on the backup workloads.
- Supported agents - Cisco Security Client, Security Endpoint, CrowdStrike, MS Defender, SentinelOne.
- License entitlement to DataProtect is required. License for Cohesity Data Hawk is optional and enables additional sensitive data visibility.
- All third-party integrations require Cisco XDR Advantage or Cisco XDR Premier licensing tier. For more information on the licensing tiers, see Cisco XDR Licenses.

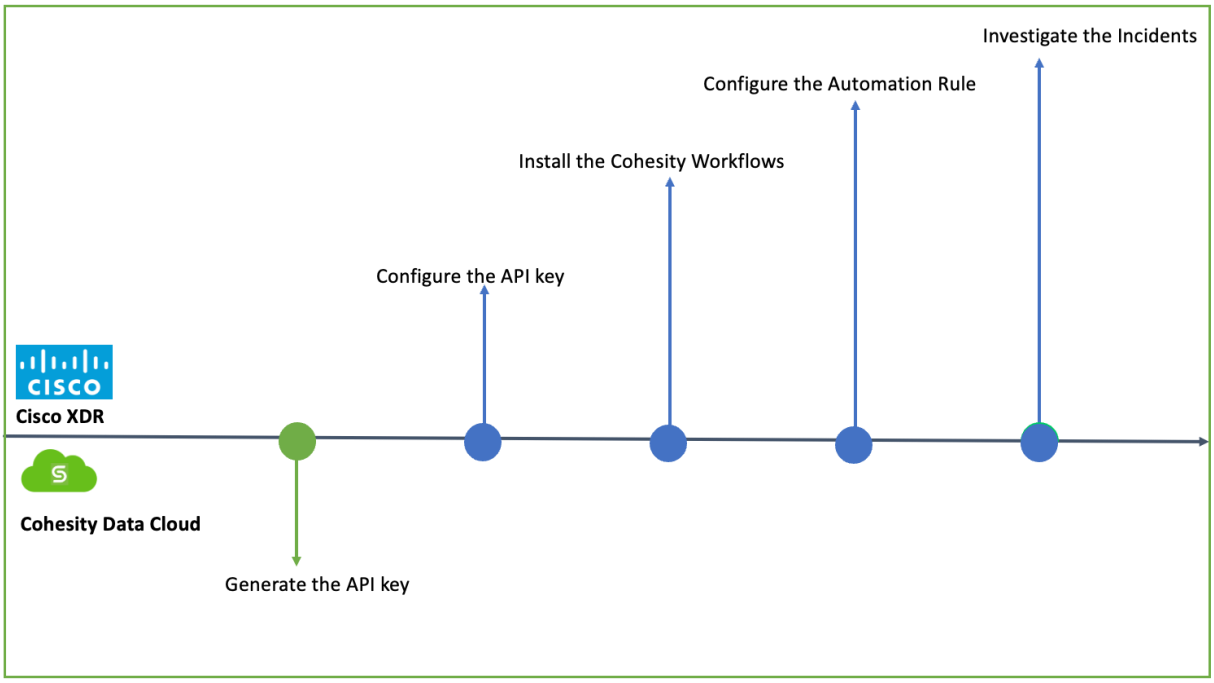
Configure Cohesity Cisco XDR

This solution empowers customers to respond at the onset of a ransomware attack by automatically capturing backup snapshots of critical data. This approach significantly reduces the recovery point objective (RPO) and minimizes business disruption.

You can integrate Cohesity Data Cloud with Cisco XDR to stay updated with the security alerts from your Cohesity Marketplace and immediately respond to a ransomware attack or an incident.

To integrate with **Cohesity Data Cloud with Cisco XDR**, perform the following steps:

Figure 3: Configuration Workflow



NOTE: Refer to the Prerequisites before you start configuration

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.

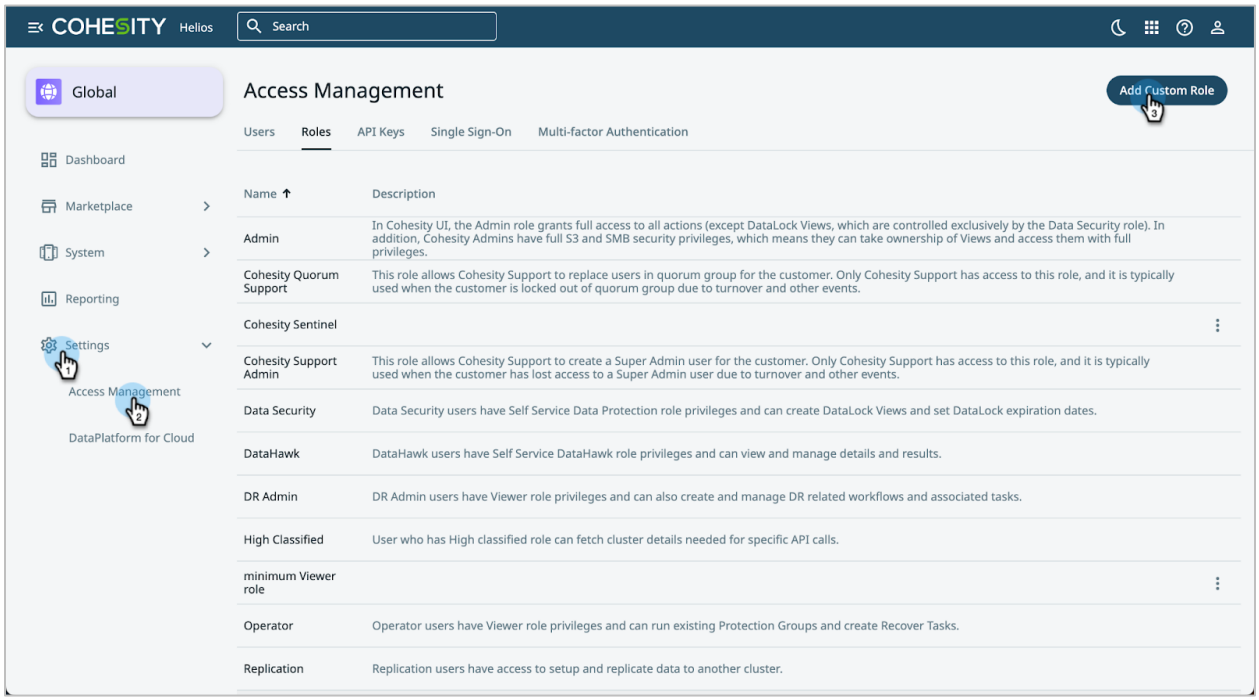
You must create a role with minimum permissions in Cohesity Data Cloud.

Create a Custom Role with Minimum Permissions

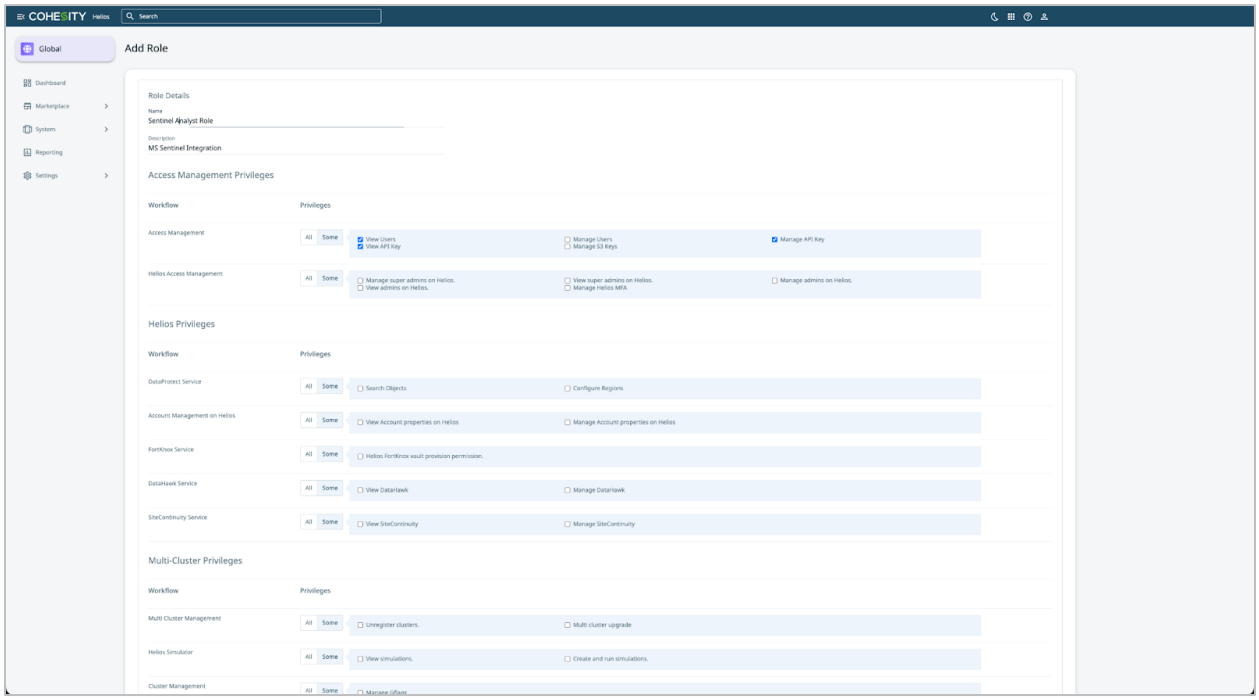
Cohesity Data Cloud allows you to create a role and choose its permissions. However, Cohesity recommends creating a role with the minimum required permissions for data connection purposes.

To create a role:

1. Login to Cohesity Data Cloud.
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 the snapshot tagging feature
   - Restore from tagged snapshots



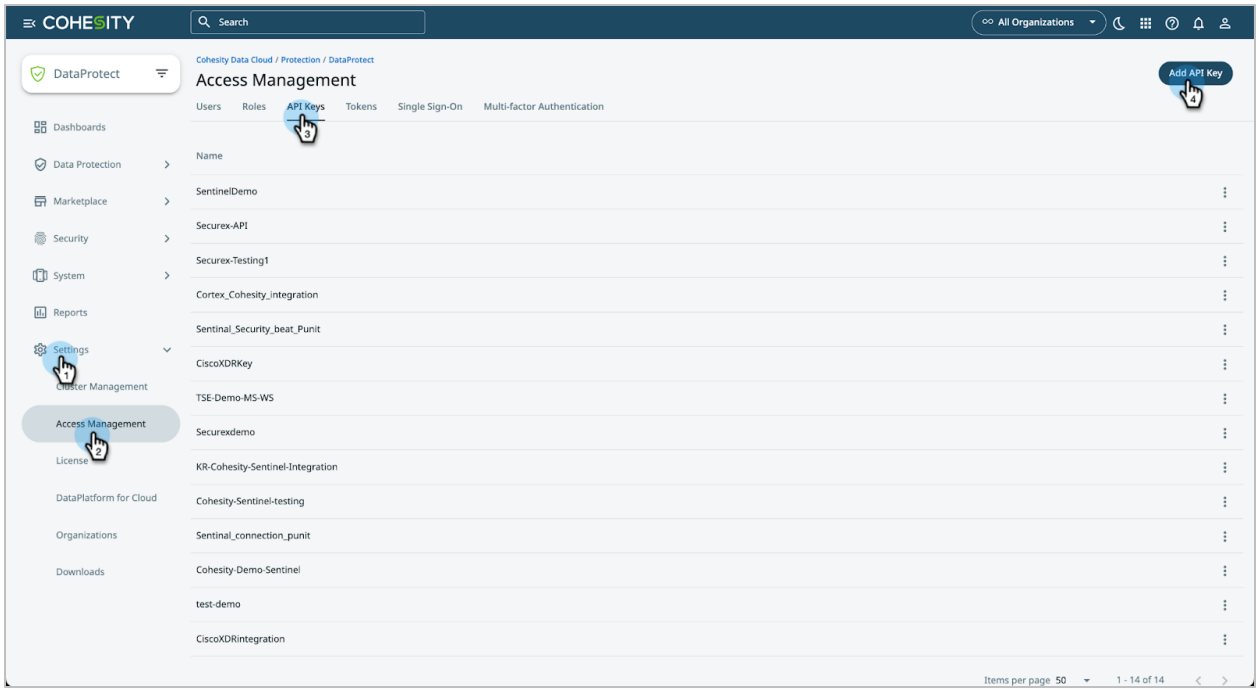
6. Click **Save**. A new role is created successfully.
7. Once the new role is created, you have to assign the created role to a user.
8. You have to log back into Cohesity Data Cloud as this user and then create an API key to authenticate an application.

NOTE: This API key has the minimum permissions because the user role who created this API key has minimum assigned permissions. Changing the user's role in the future will change the privileges associated with the API keys created in the past.

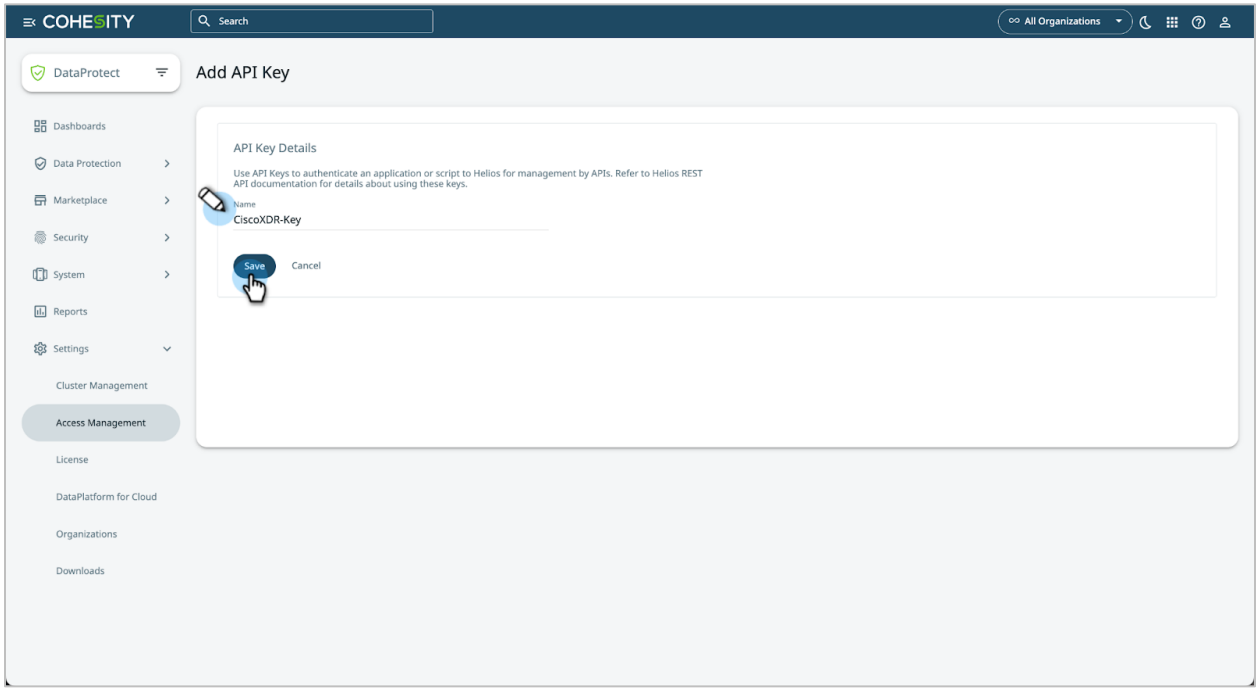
Create and Copy the API Keys

To create and copy the API keys:

1. Log in to Cohesity Data Cloud.
2. From the **Global Dashboard**, navigate to **Settings** > **Access Management**>**API Keys** >**Add API Key**.

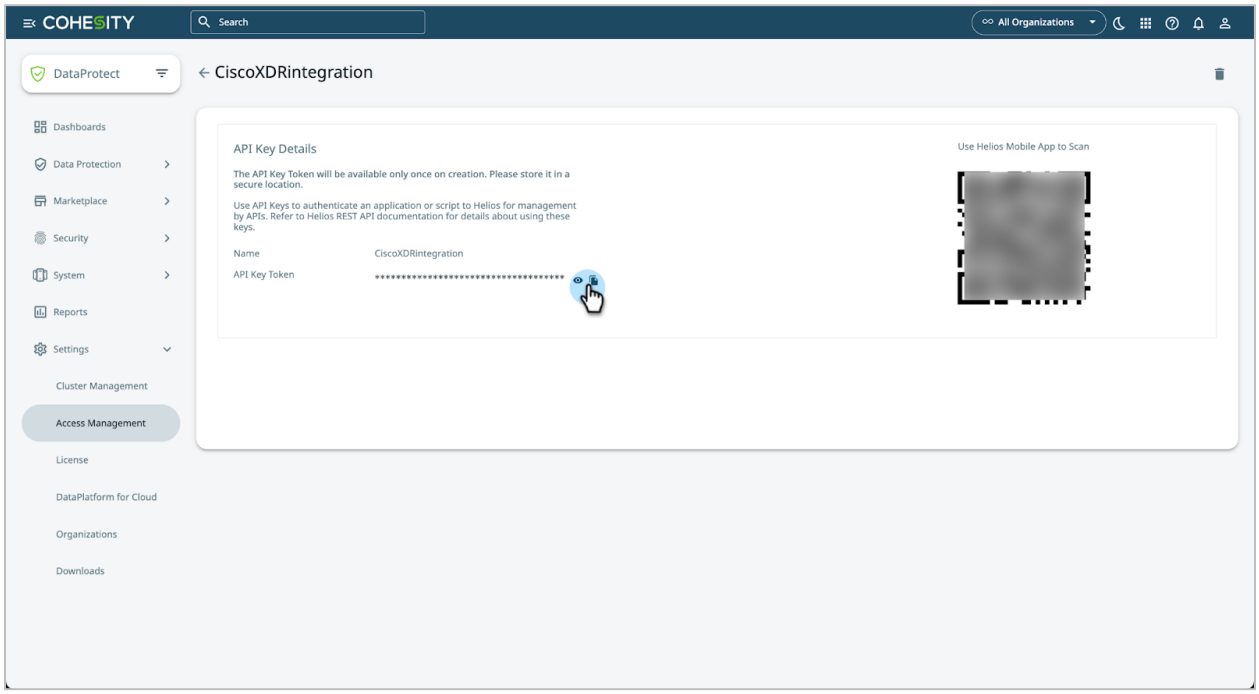


3. Enter a name for the API key and click **Save**.



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

NOTE: Be sure to copy and save the API Key token to add it later while configuring the Cohesity Data Cloud plugin in Cisco XDR.



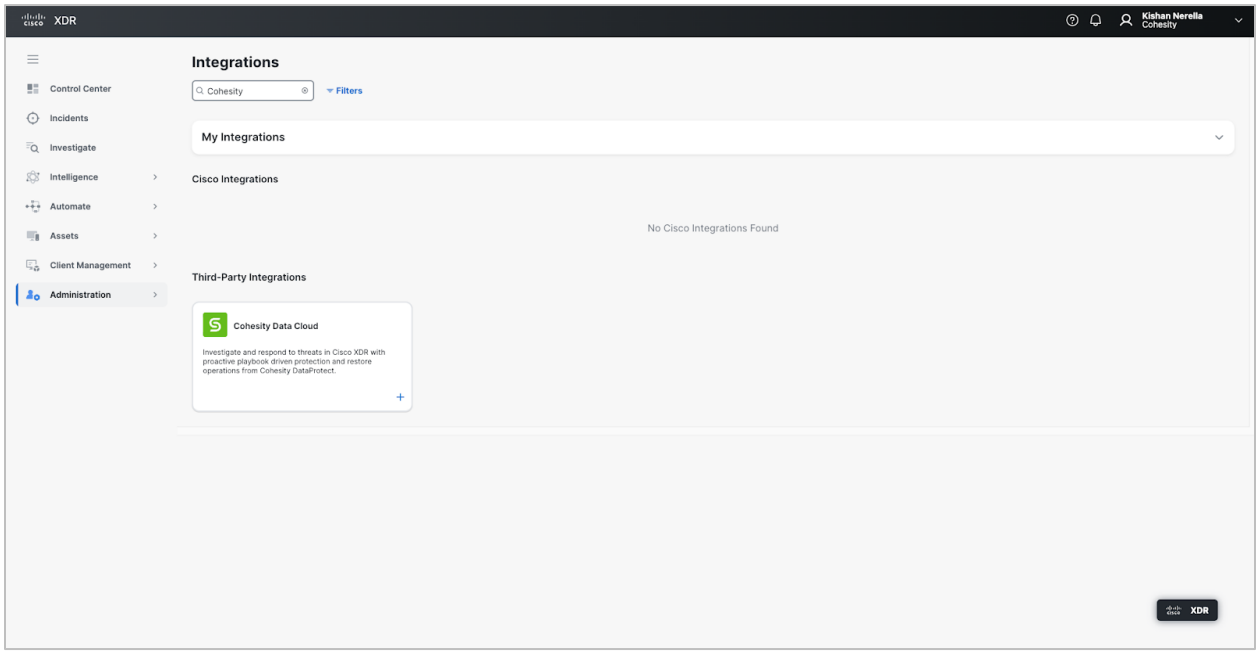
Configure the Cohesity Data Cloud Connector

The next step is configuring the Cohesity Data Cloud connector on the Cisco XDR platform.

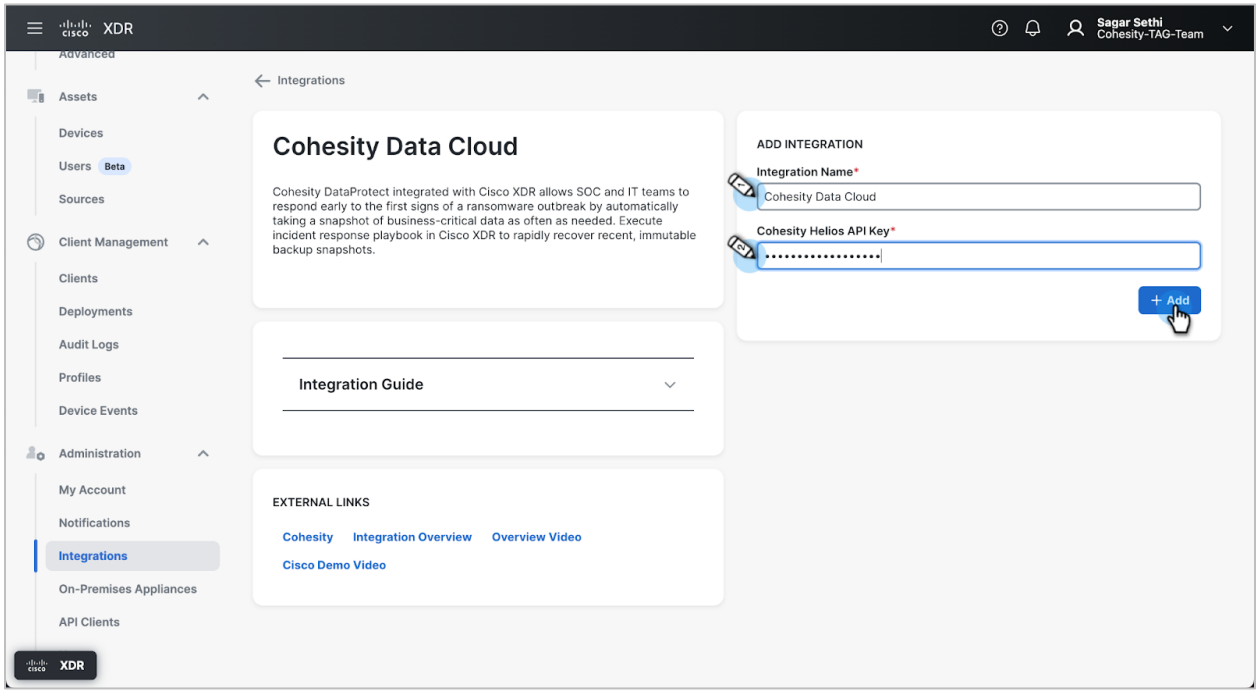
Cisco XDR has a built-in Cohesity cloud app that contains Cohesity-supported workflows and atomics in a bundled solution.

To integrate Cohesity Data Cloud with Cisco XDR:

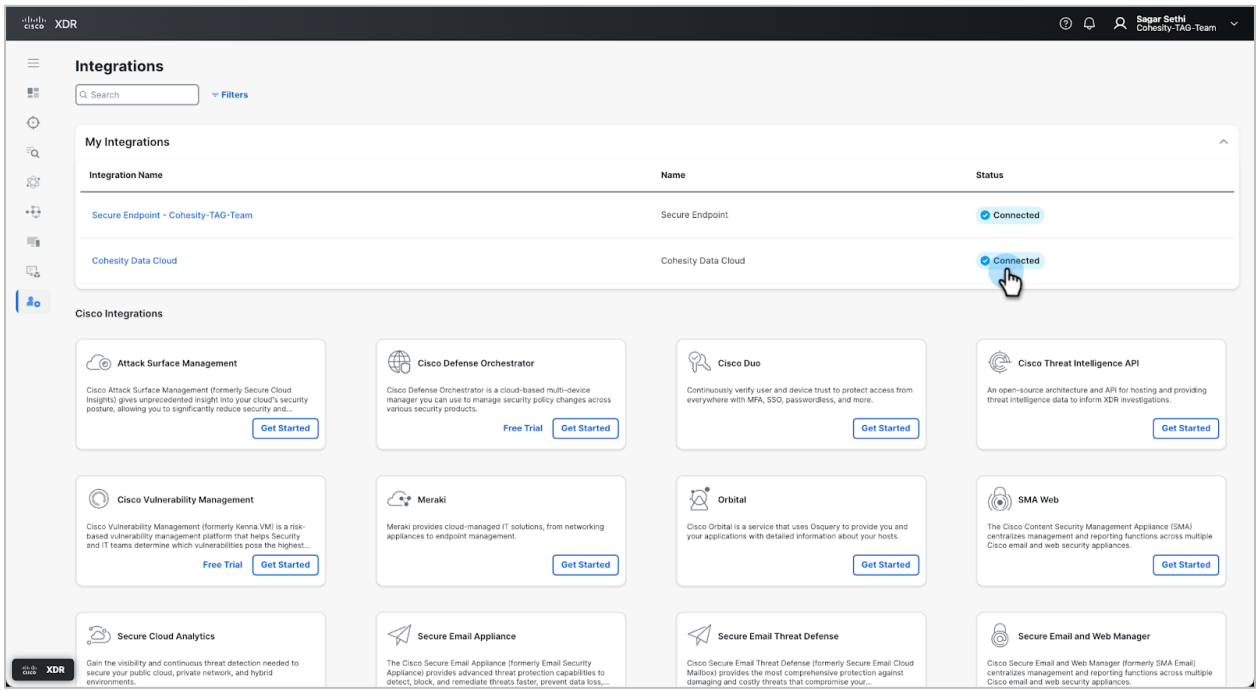
1. Log in to the Cisco XDR Control Center.
2. Navigate to **Administration** > **Integrations** and search for **Cohesity**.



3. On the **Cohesity Data Cloud** tile, click **+**.
4. On the **Cohesity Data Cloud Integration** page, add the **Cohesity Data Cloud API Key** you have generated and copied from Cohesity Data Cloud and click **Add**.



5. After the integration is completed, Cohesity Data Cloud is displayed under **My Integration panel** on the **Integrations** page. The **Status** column indicates whether the module is **Connected** (successfully configured) or if it has an **Error** with the configuration.



Configure the Cohesity-supported XDR Workflow

Automation workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks, using activities, logic, and even other workflows to communicate with other systems and resources.

The Cohesity Data Cloud integration provides the following workflows from Cohesity that you can use in Cisco XDR for proactive protection and restore operations from Cohesity DataProtect:

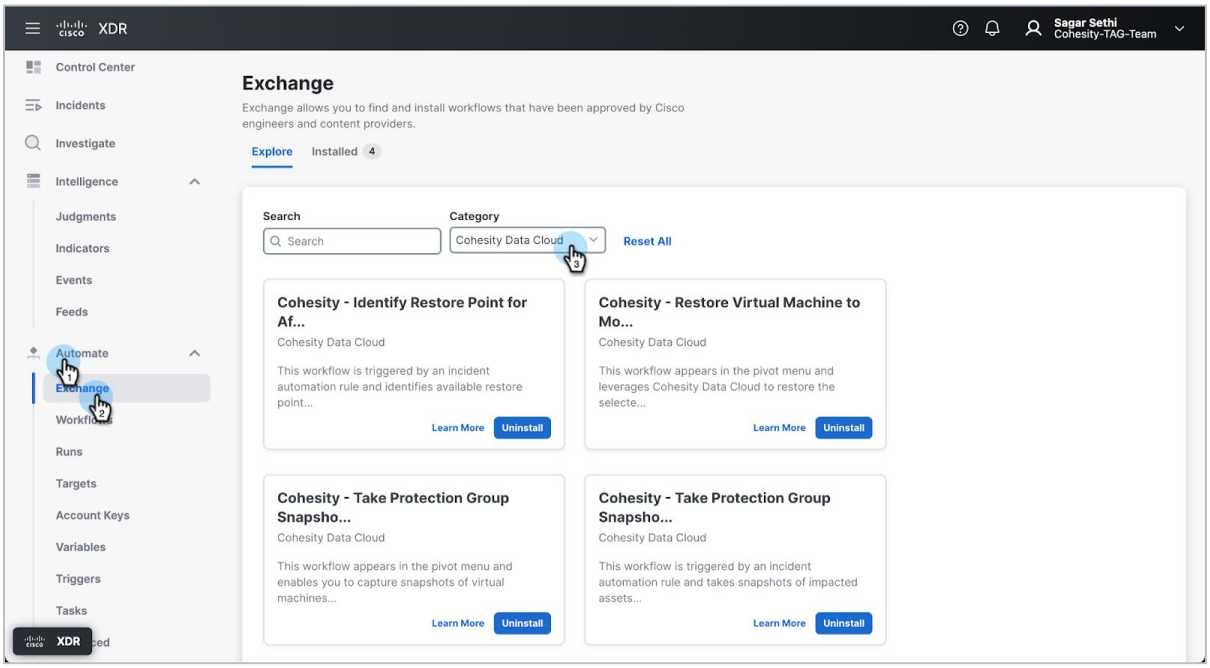
1. Navigate to **Automate** > **Exchange**, search for the Cohesity Data Cloud under Category. You will see the following Cohesity-supported workflows:

   a. **Cohesity - Take Protection Group Snapshot***
   b. **Cohesity - Restore Virtual Machine To Most Recent Snapshot**
   c. **Cohesity - Take Protection Group Snapshot For Affected VMs***
   d. **Cohesity - Identify Restore Point For Affected Virtual Machines**

2. Select **Install** on all supported workflows and follow the installation wizard.

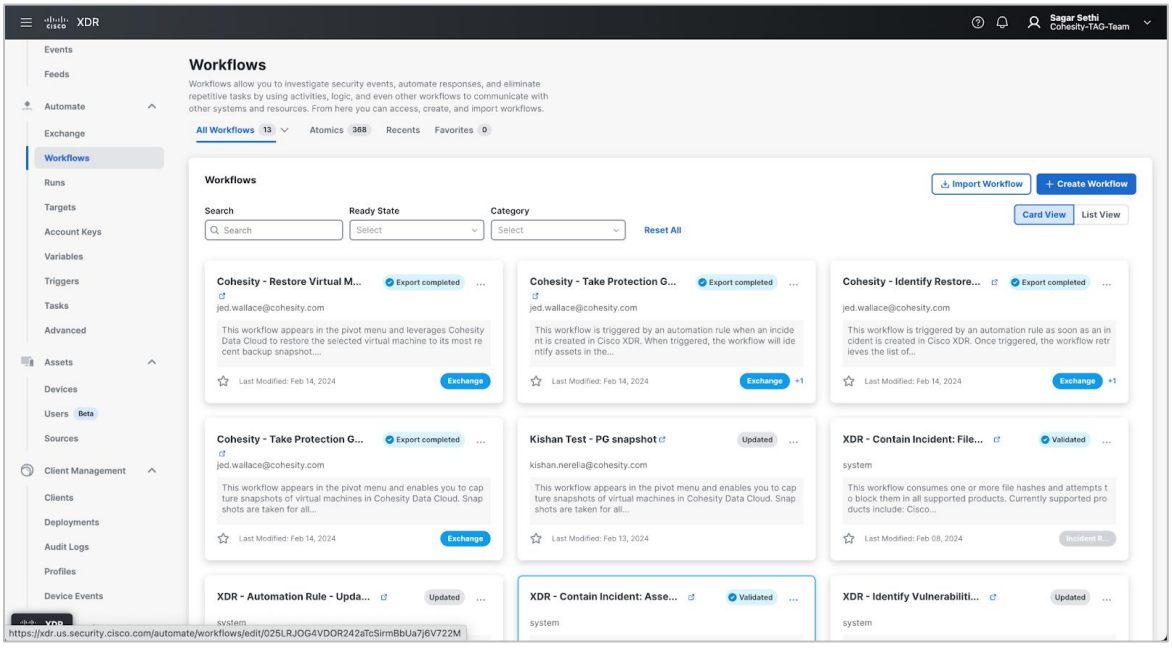
   For a detailed function of each workflow, refer to Cohesity Supported Workflows .

NOTE: *For installing Cohesity workflows, Buffer value is required, which is the last time the snapshot is taken for Backup hosts. The default value is 60 mins.



3. Navigate to **Automate>Workflows**. You will see that all the Cohesity workflows are installed and validated.

4. Click **View in Workflows** to go to the **All-Workflows** tab. The status of the new workflow will be either **Import in Progress** or **Import Completed**.



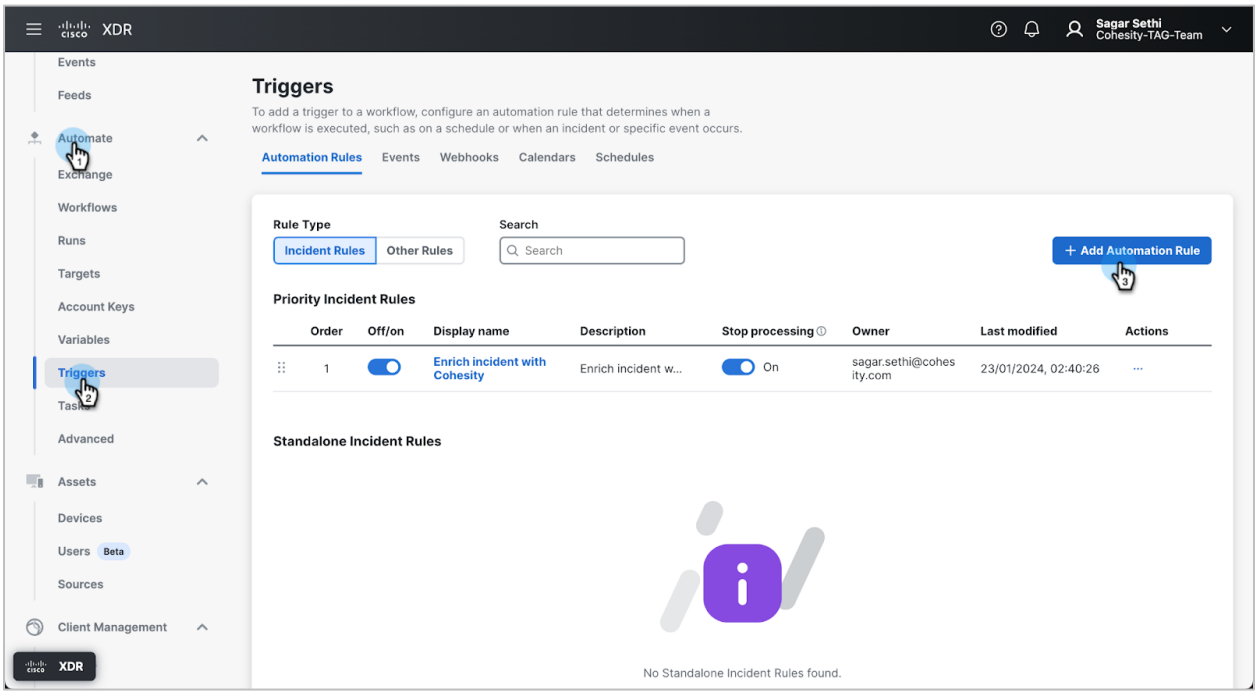
5. To validate, open the workflow in the Workflow Editor. Complete any remaining workflow and click **Validate** to ensure the workflow has the required data to run successfully.

NOTE: Each workflow 'must' be opened once for validation for execution, as Cisco does not support auto-validation today.

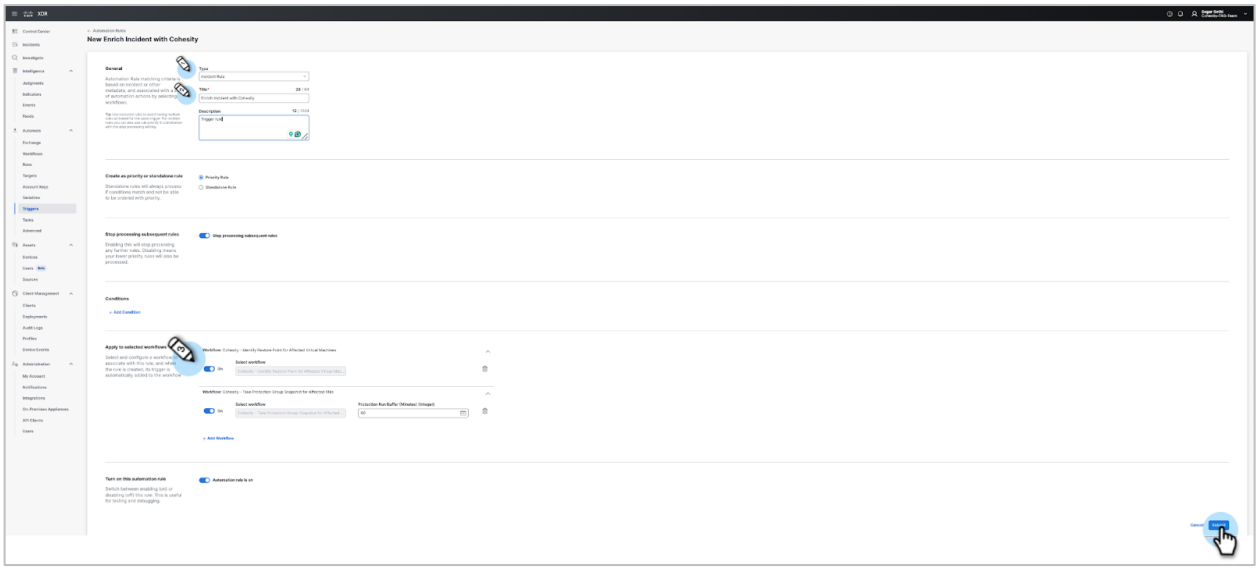
Create the Cohesity Automation Rule

Automation rule workflows are triggered when conditions for the rule are matched in Cisco XDR. To add a trigger to a workflow, configure an automation rule that determines when a workflow is executed, such as on a schedule or when an incident or specific event occurs.

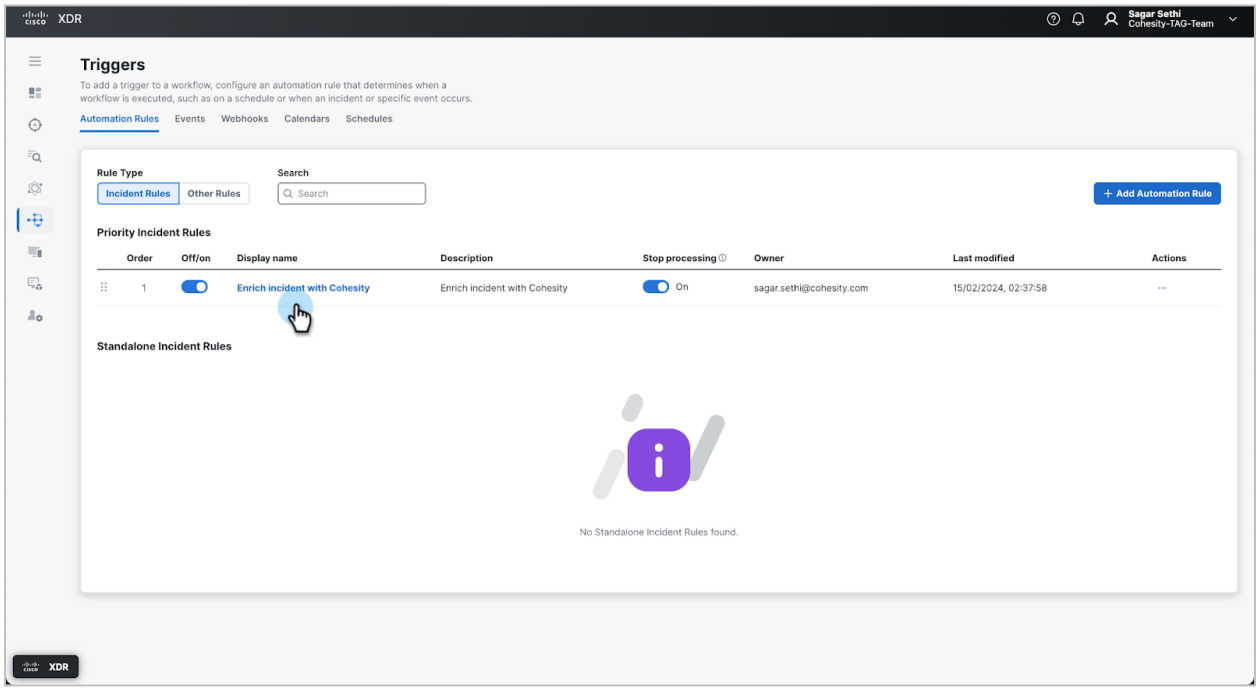
1. Navigate to **Automate** > **Triggers** and click on **Add Automation Rule**.



2. Enter the following details and click **Submit**.
   a. **Type:** < Select the rule type>
   b. **Title:** < Enter the title >
   c. **Description:** < Enter the description>
   d. **Create as priority or standalone rule:**< Select as Priority>
   e. **Condition**: <Add a 'condition' for the workflows to trigger. E.g. 'Confidence' 'Equals' 'High'>
   f. **Apply to selected workflows:**< Add the associated workflow >
   g. **Protection Run Buffer (Minutes) (Integer):** < This is the value time from the last snapshot taken for the protection group. The default value is 60 mins>
   h. **Automation rule is on :**< Toggle to on>



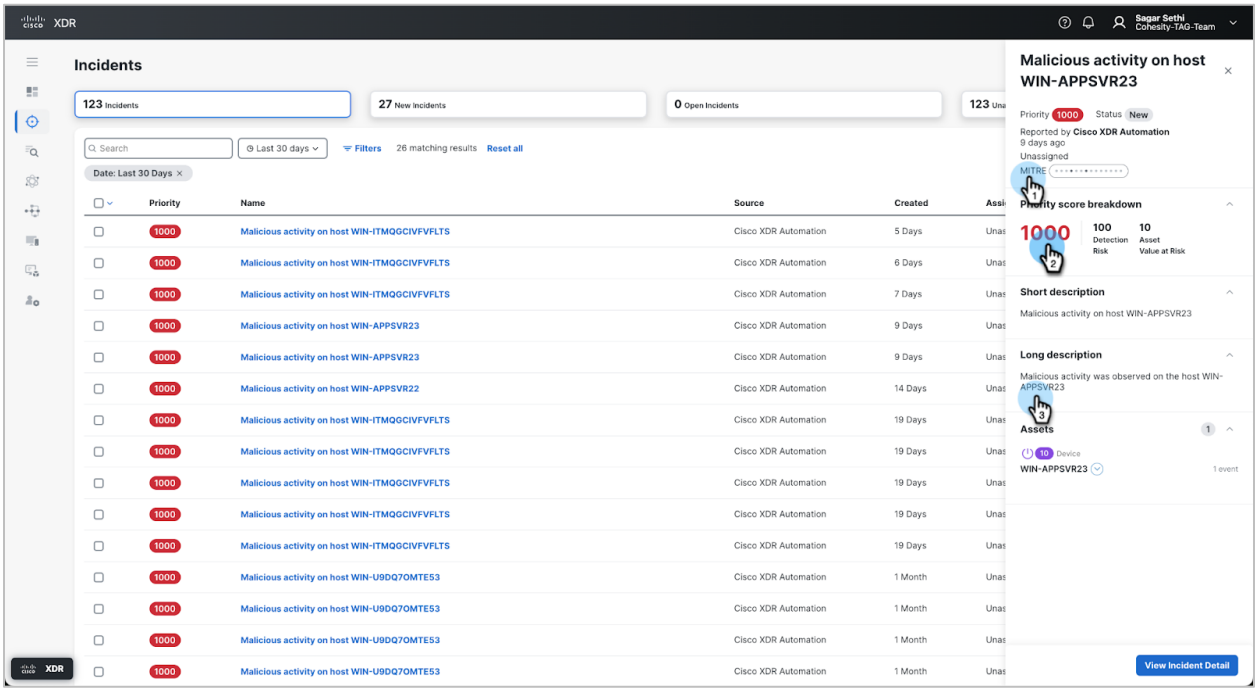
3. Click on **Submit** to see the automation rule **"Enrich Incident with Cohesity"** created**,** which will be triggered based on the condition set.



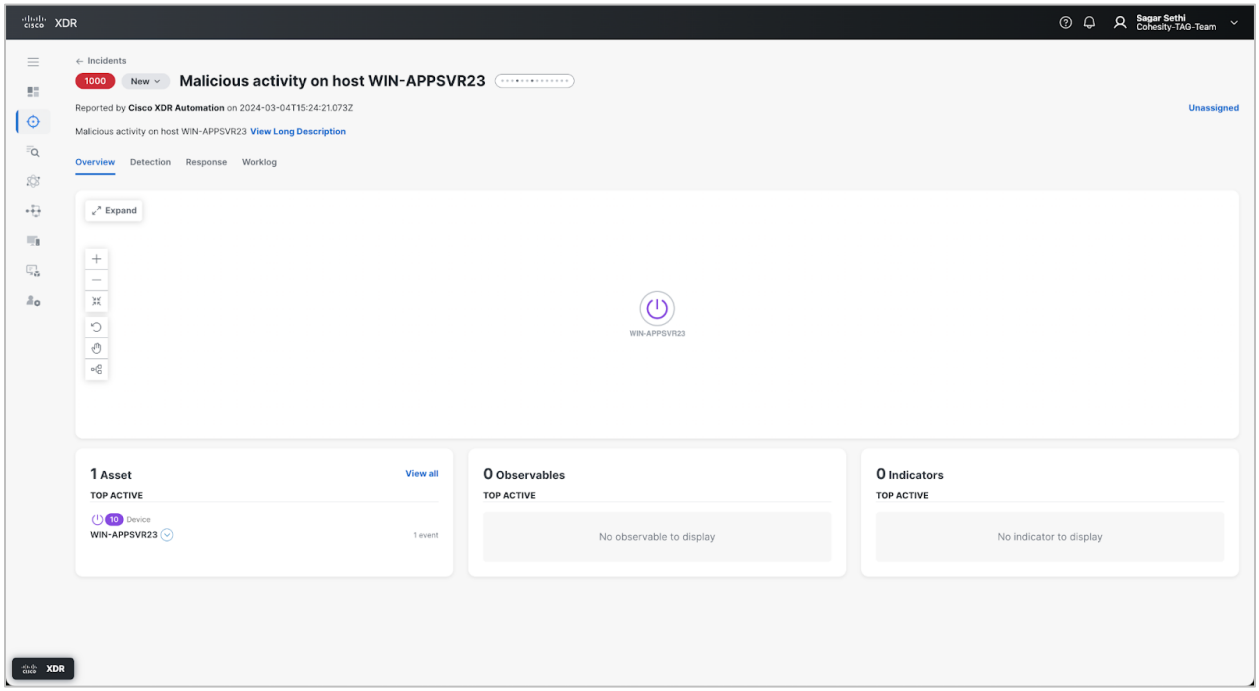
Investigate the Incident

After you successfully configure the workflows on Cisco XDR, you can investigate Anomaly alert triggers from the Cisco XDR more quickly, effectively, and efficiently, thereby reducing your mean time to resolve (MTTR).

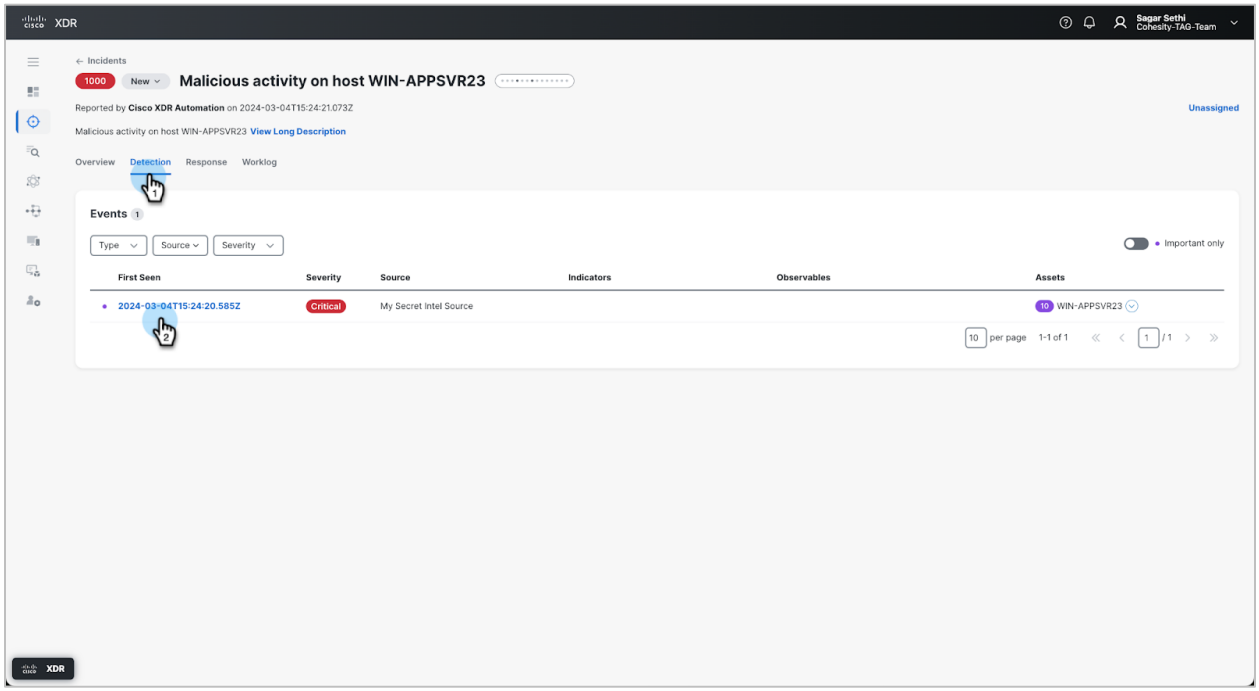
1. From the **Cisco XDR** console, select **Incidents**. The details provide more information about the incident to help you diagnose, contain, and remediate the threat. The page contains the header, attack graph, and additional tabs to access the **Overview, Detection, Response Action, and Worklog** pages.
2. For each incident, you can see the time it occurred, the status**,** and the description of the incident. MITRE Tactics &Techniques connect and reveal the attack chain and **Priority Score** to decide which incidents to handle first.



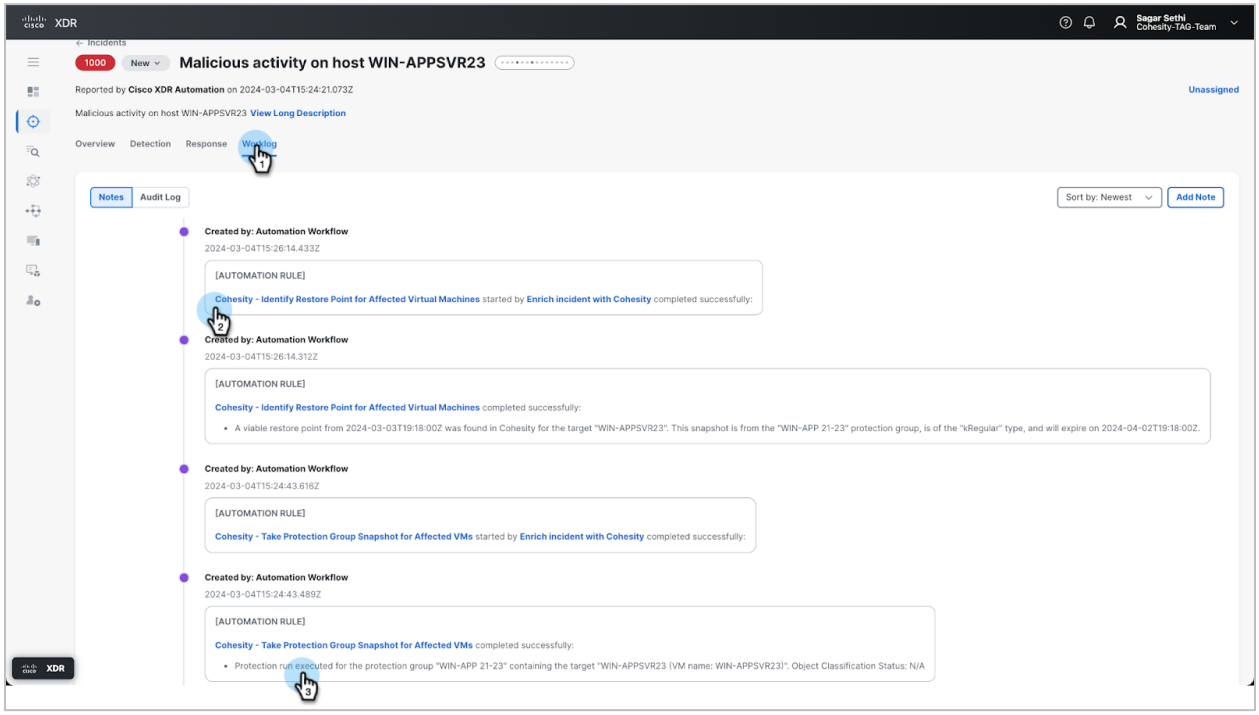
3. To view more details about the alerts and entities in the incident, select **View Incident details** on the **incident page** and review the relevant tabs that summarize the incident information.



4. **The Detection page** shows all of the detection parts of the incident. You will see the **First seen** details and detection source for this incident as “My secret Intel source” to dive into the alert data across different timelines and understand the chronological sequence of alerts for this incident detected early in the attack chain.

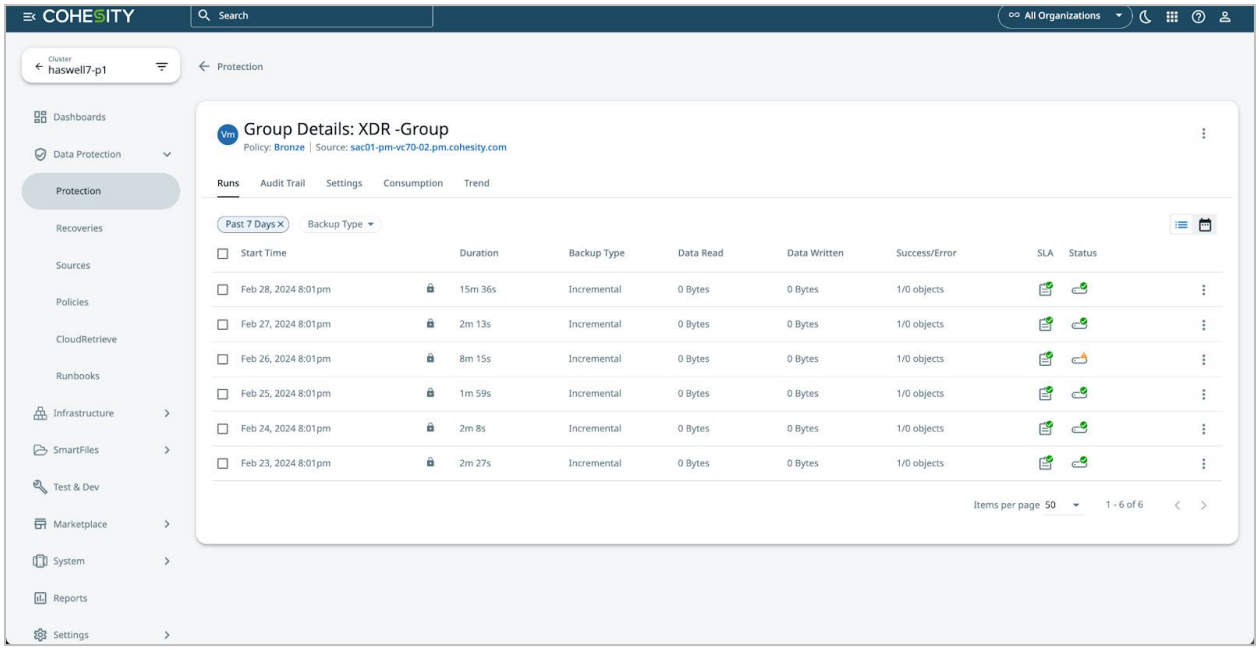


5. **The Worklog** page in the incident details is used to enter notes about the findings while investigating the incident and to view the audit log of changes made to the incident, such as **triggered workflow actions** for the affected source. You can see that the workflow is triggered by an automation rule as soon as an incident is created in Cisco XDR.
6. Once triggered, the workflow retrieves the list of virtual machine assets associated with the incident and then determines the most **recent and viable restore point** for each virtual machine and takes the immediate snapshot of the workload along with all workloads in the protection group that will be back up.

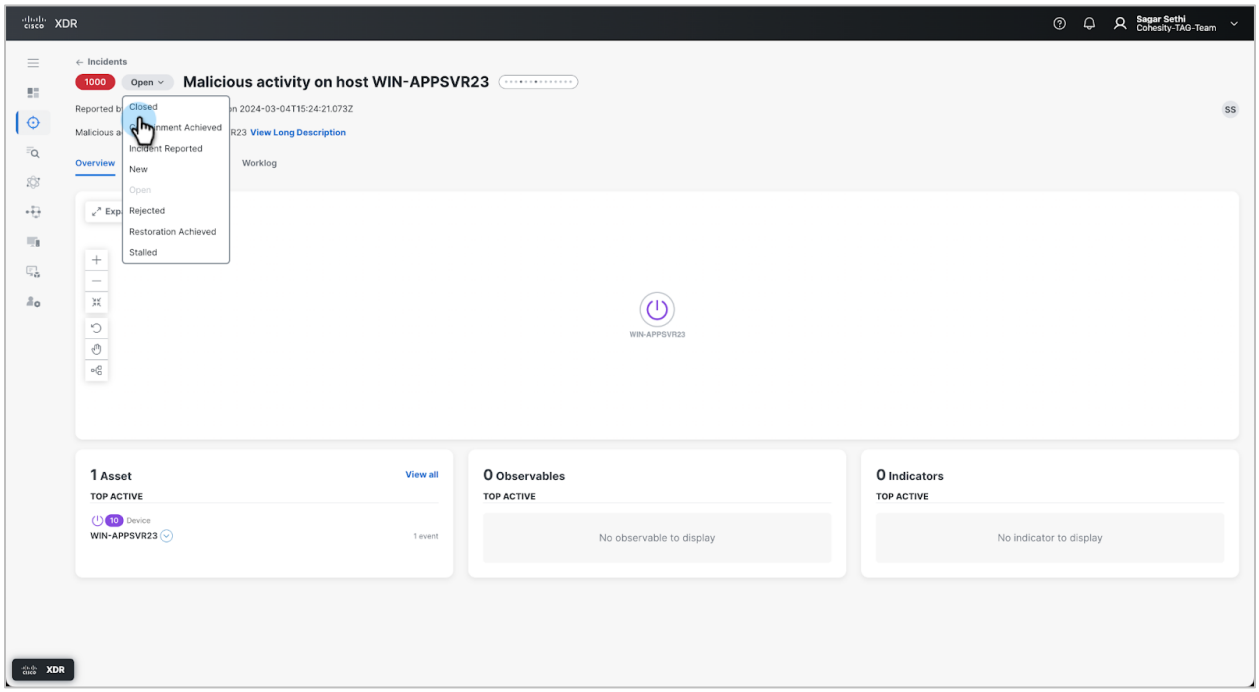


7. Any data sensitivity information associated with the Impacted Workload is identified by the Cohesity Data Hawk data classification engine and added to incident notes.

8. From **Cohesity Data Protect Dashboard**, select Data **Protection> Protection**. You will see a **snapshot of the protection group** job automatically triggered for each virtual machine mentioned in the incident on Cohesity Data Protect. This ensures that a backup is created for high value before it is compromised, which will be critical for future forensics analysis.



9. Once the investigation is complete, analyst can close the incident from **Incidents> Status.**



Conclusion

Cyber resiliency is all about minimizing the disruption to an organization’s business processes and minimizing data loss during a cyberattack. Cohesity integration with Cisco XDR helps InfoSec teams automatically capture a snapshot of business-critical information at the beginning of a ransomware outbreak, taking us one step closer to delivering a near-zero RPO during a catastrophic attack and making it simple to protect, secure, and recover your data.

Appendix A: Glossary

Terms	Description
RTO	Recovery Time Objective (RTO) is defined as the maximum acceptable amount of time that can pass before an organization restores functionality to an application, service, data, or other digital asset that is inaccessible due to an outage or data loss incident.
RPO	Recovery Point Objective **(RPO)** is the maximum acceptable amount of data loss an organization can tolerate before causing harm to the business. RPO is calculated in time—between the downtime event and the last backup.
XDR	Extended Detection and Response (XDR) collects and correlates data across email, endpoints, servers, cloud workloads, and networks, enabling visibility and context into advanced threats. Threats can then be analyzed, prioritized, hunted, and remediated to prevent data loss and security breaches.
Workflows	Built with Atomic Actions, workflows enable you to take response actions from an observable throughout Cisco XDR.
MITRE ATT&CK	A globally accessible knowledge base of adversary tactics and techniques based on real-world observations and a foundation for developing specific threat models and methodologies
MTTD	Mean Time To Detect **(MTTD)** measures the average time it takes to detect an incident or disruption.
MTTR	Mean Time To Recover**(MTTR)** measures the average time it takes to respond to and resolve an incident or disruption.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Sagar Sethi is a Staff Technical Solutions Engineer at Cohesity. In his role, he focuses on various aspects of Data Security that secure Cohesity products and solutions.

Other essential contributors include:

- Karthick Radhakrishnan, Director, Technical Solution Engineering
- Surya Swaminathan, Sr. Technical Solutions Engineer
- Rob Young, Product Manager, Competitive Intelligence
- Kishan Nerella, Engineering
- Subash Babu, Staff Technology Editor
- Sheetal Venkatesh, Product Management
- Damien Philip, Cisco Alliance Field CTO

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.0	Mar 2024	First 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 42 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.