COHESITY

Integrate CrowdStrike Falcon Logscale with Cohesity Data Cloud

Enhance the security visibility, investigation, and rapid response of Cohesity incidents

Version 1.2

August 2025

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 CrowdStrike Falcon Logscale platform with Cohesity Data Cloud to enhance the security visibility, investigation, and rapid response of Cohesity incidents to protect customer-critical data.

Table of Contents

Figures

Why Integrate CrowdStrike Falcon Logscale with Cohesity

Ransomware attacks have increased exponentially, causing billions in losses, and putting lives at risk while damaging trust and reputations all over the world. As cybercriminals get more inventive, they're locking up production systems, destroying backups, and stealing sensitive data, which leaves your enterprise with no option but to pay a ransom.

Defense in depth is the key to minimizing risk. An organization must have a backup system that reliably and securely makes continuous or frequent backups. The system must protect the organization from a variety of attacks and 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. It can be your first warning of trouble if your other tools have failed to detect and block the attackers. For more information, refer to the Accelerate Anomaly Detection whitepaper. Cohesity enhances your organization's ability to react quickly in a coordinated manner by integrating with the CrowdStrike Falcon Logscale platform.

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 CrowdStrike Falcon Logscale 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 most effectively assess an attack's scope and quickly remediate the threat.

Customer Benefits

The CrowdStrike Falcon Logscale platform can ingest, index, and analyze alert data with unparalleled speed and efficiency. By integrating anomaly logs into CrowdStrike Logscale, organizations can experience several benefits, including:

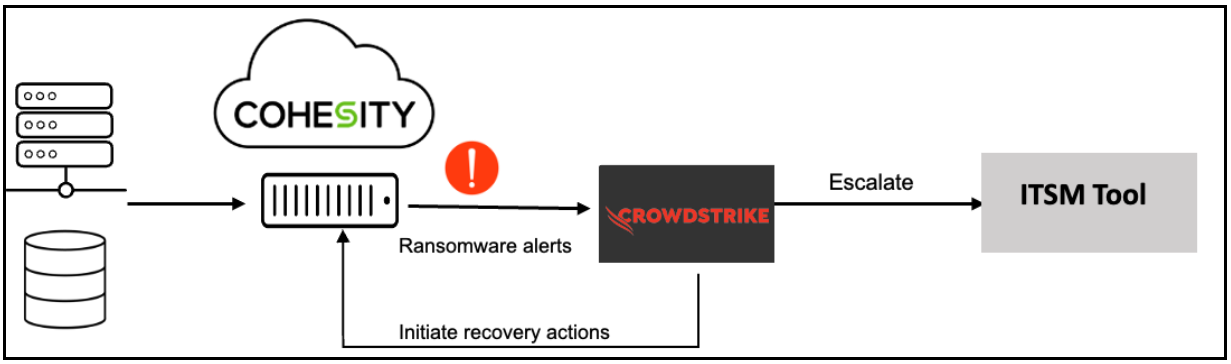
- **Unified threat visibility** – Allows organizations to have a unified view of anomaly events and data protection activities. Security and data protection teams can access a centralized dashboard within CrowdStrike Falcon Logscale to monitor and analyze the Cohesity-generated anomaly events in real time.
- **Intelligent threat detection and response** – Combined Cohesity and CrowdStrike Falcon Logscale capabilities enable advanced threat detection and response. The integration empowers security teams to identify and respond to security incidents quickly.
- **Compliance Adherence** – Cohesity's integration with CrowdStrike supports compliance and auditing requirements. Organizations can adhere to regulatory standards by leveraging the combined capabilities.

Integrate Cohesity with CrowdStrike Falcon Logscale

CrowdStrike Falcon Logscale platform, a leading platform renowned for its ability to ingest, index, and analyze log data with unparalleled speed and efficiency in transforming raw data into actionable intelligence, is an invaluable asset for businesses seeking to leverage their data for strategic decision-making. To do that, Logscale provides a web-based interface that can aggregate data, create alerts, visualize streaming data, and perform system monitoring, all using customizable dashboards and workflows.

Cohesity provides **Cohesity for CrowdStrike Falcon Logscale integration** available on the Cohesity marketplace that uses a push-based model by secure CrowdStrike REST APIs to collect Anomaly alerts for improved operational intelligence and data management.

Figure 1: Actionable Intelligence (detection and investigation) with Cohesity and CrowdStrike Integrated



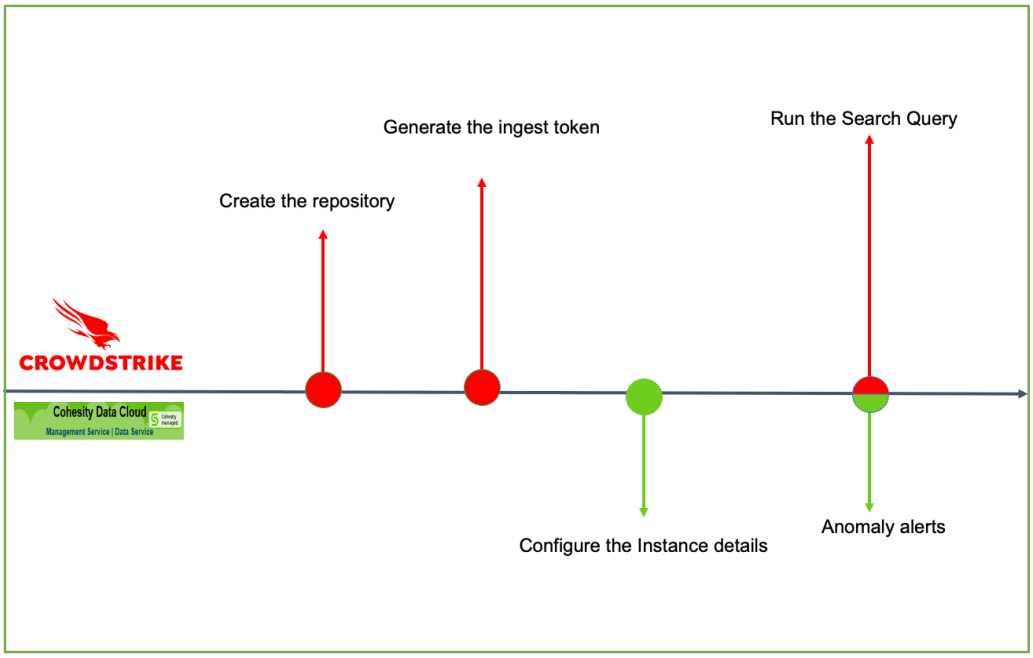
Cohesity Anomaly logs start ingesting on Falcon Logscale to be indexed and correlated within the Logscale dashboard. Within Logscale, security analysts can also run the search query to fetch meaningful results and create an incident based on the rules configured.

Integrate Cohesity Log Alerts to Falcon Logscale

You can integrate Cohesity with Falcon Logscale to stay updated with the anomaly alerts from your Cohesity Data Cloud for analysis, visualization, and intelligent action from Logscale Instance.

Follow the below steps to integrate Cohesity Data Cloud with the CrowdStrike Falcon Logscale platform.

Figure 2: Integration Workflow



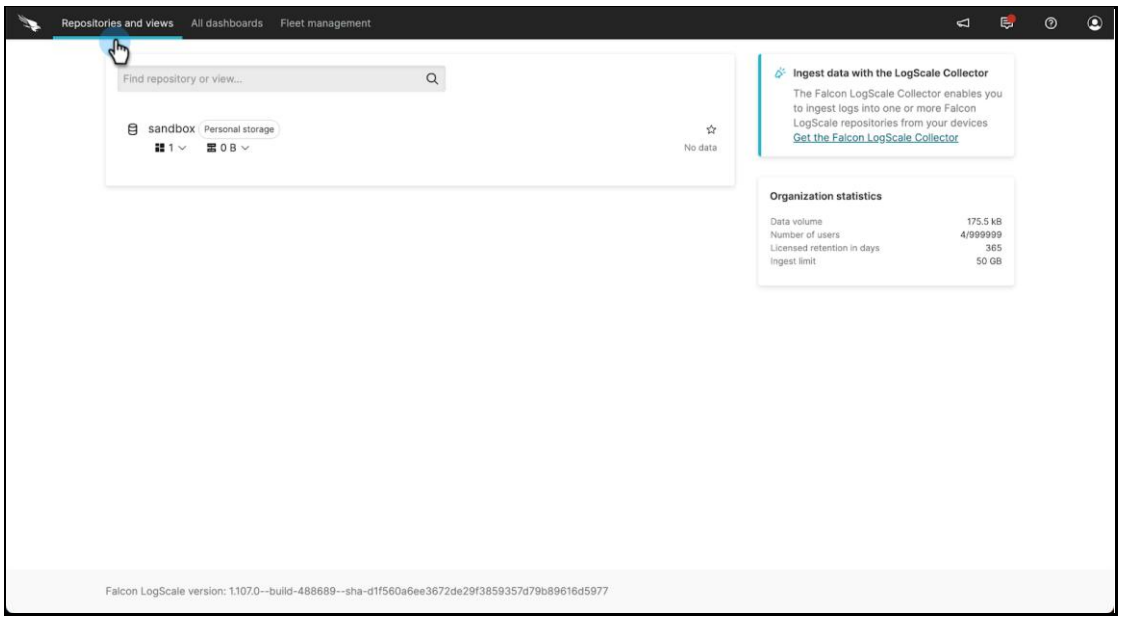
Create Repository

Data sent to Logscale needs to be stored in a repository. A repository in Logscale is where you store Cohesity alerts and metrics. The repository allows you to search and monitor your Cohesity log data in a much more comprehensive way.

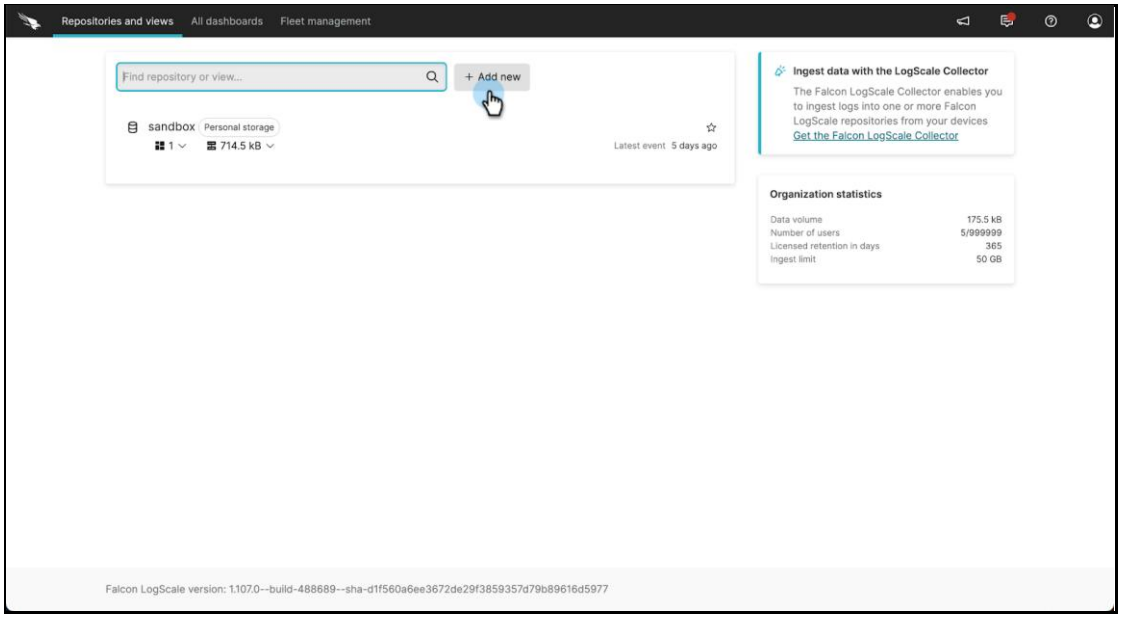
To create the **repository** on Falcon Logscale Instance:

1. Log in to **CrowdStrike Falcon Logscale** Instance.

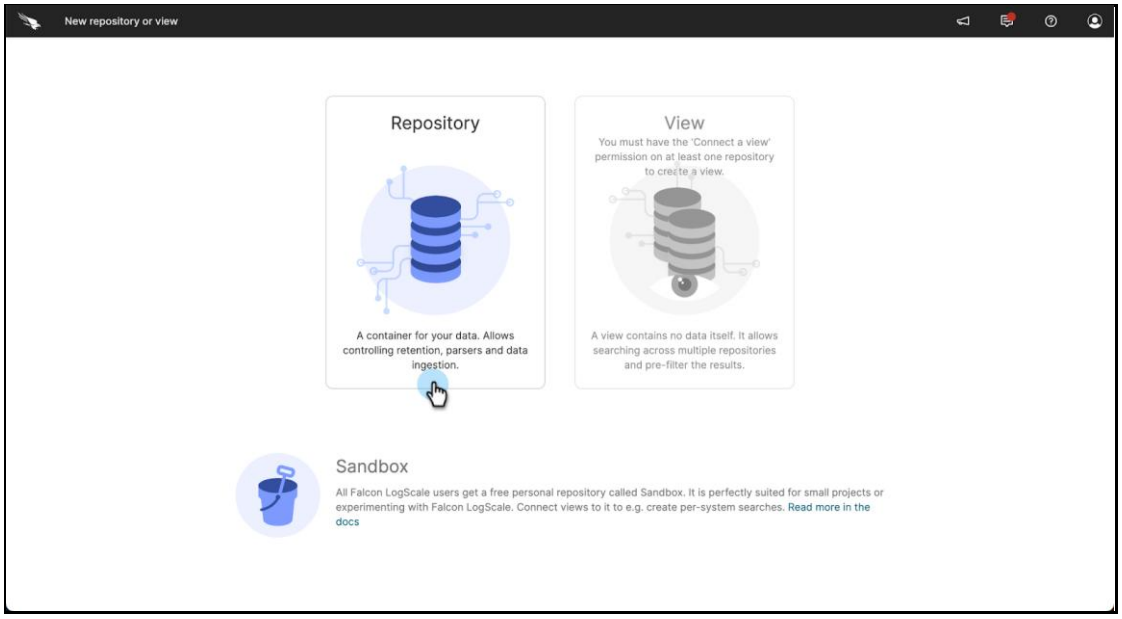
2. Select the **Repositories and views** tab.



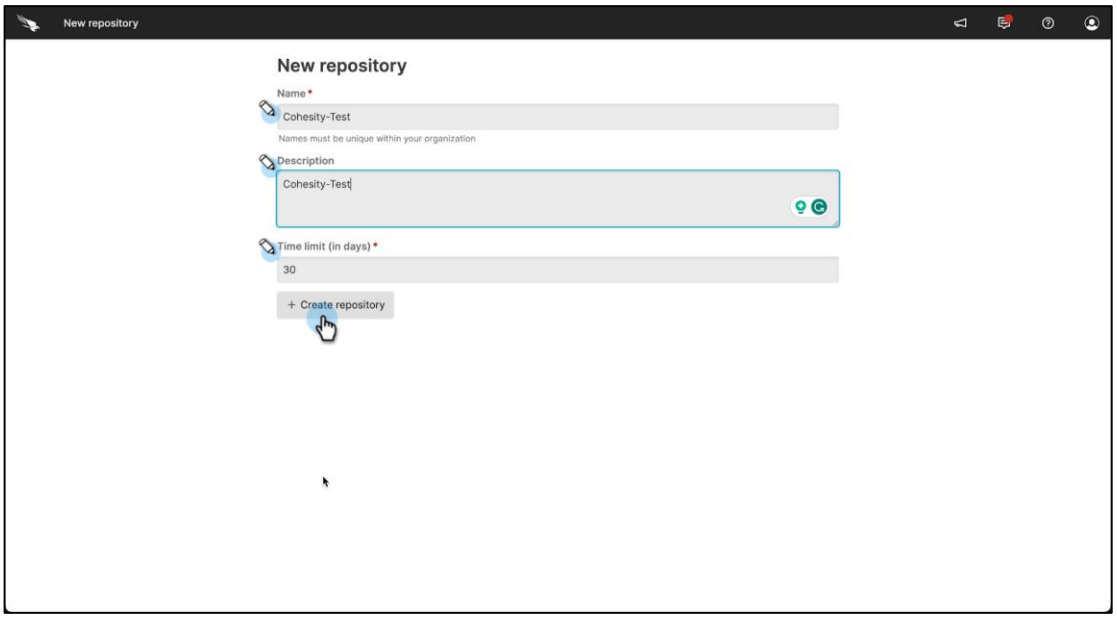
3. Click **Add new** item and choose the **Repository** option.



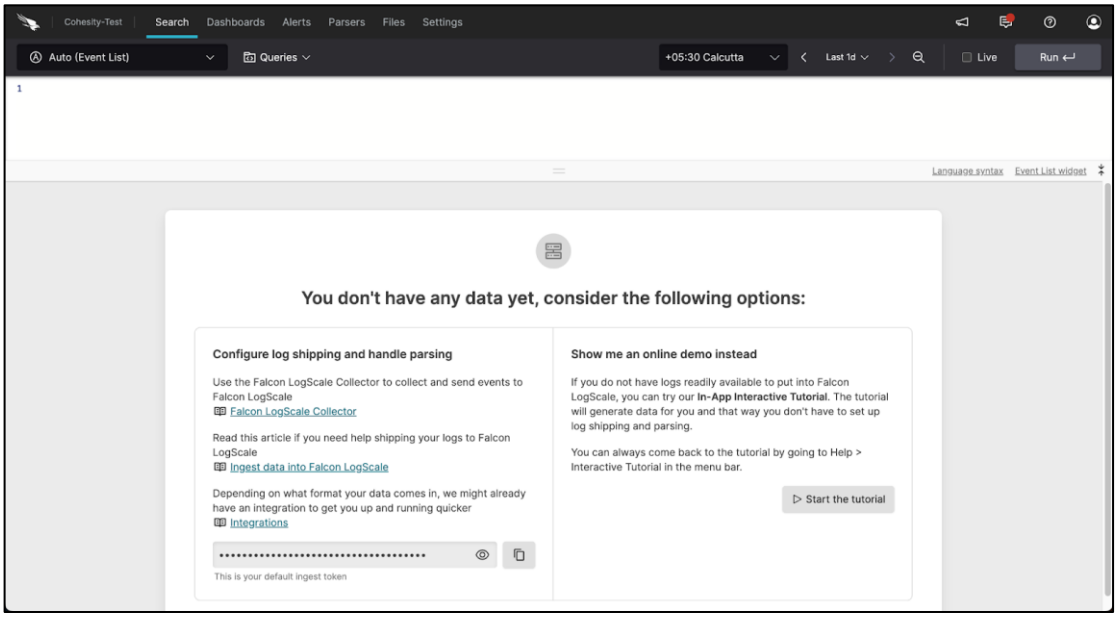
NOTE: You can also choose an existing repository to stream the alerts.



4. Enter the repository details:
   a. **Name** - < Enter the name of the repository.>
   b. **Description -** < Enter a description of repository.>
   c. **Time limit** - < Enter the no. of days for retention of logs.>



5. You'll see a screen with panels for administering the repository you just created.



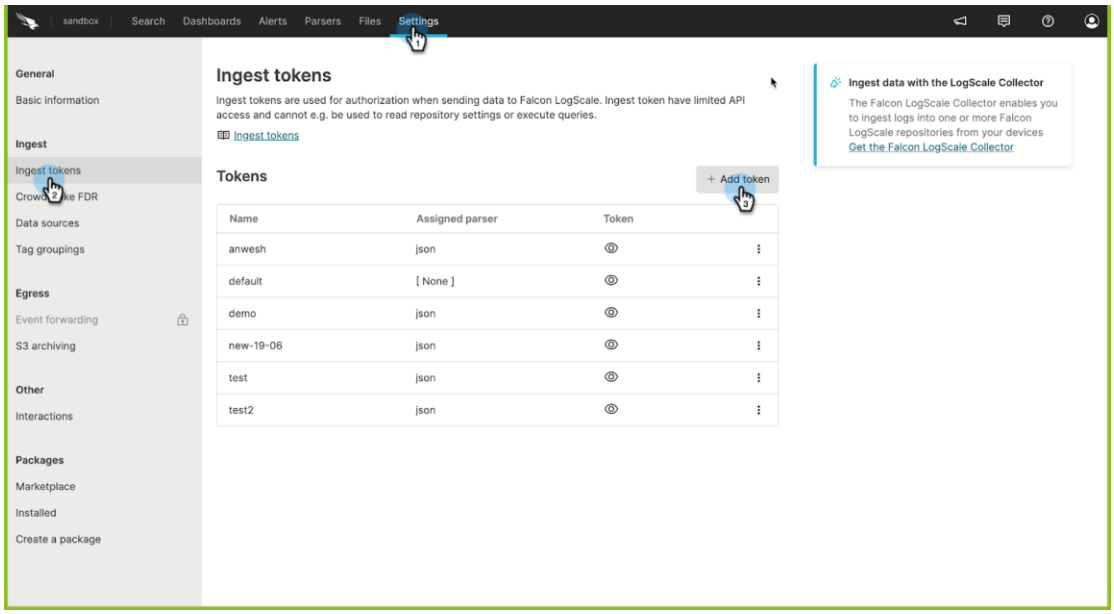
Generate New Ingest Token

After creating the Repository, you need to generate a New Ingest Token and then use the token while configuring data ingestion to your repositories from your Logscale Cloud account. An **Ingest Token** is a unique string that identifies a repository and allows you to send data to that repository.

To generate the **Ingest Token:**

1. From the **Logscale** home screen, select the created repository.
2. Select the **Settings** tab.
3. From the left navigation bar, select **Ingest tokens** > **Add token** option.

NOTE: You can also use the default ingest token generated while creating the repository.

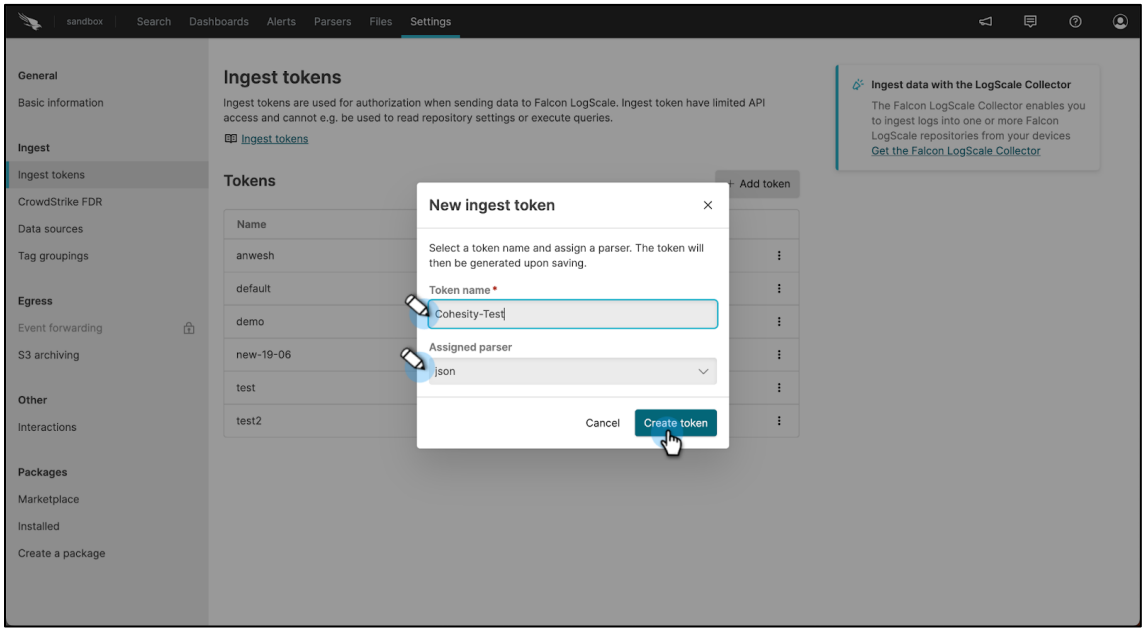


4. Enter the token details and select **Create Token.**

   a. **Token Name** - < Enter the name of the token.>

   b. **Assigned parsers** - < Select **JSON** from the popup list.>

NOTE: When you send logs to Logscale for ingestion, they will be parsed before they are stored in a repository.



NOTE: Ensure that you have the required permissions to create the ingest token and repository.

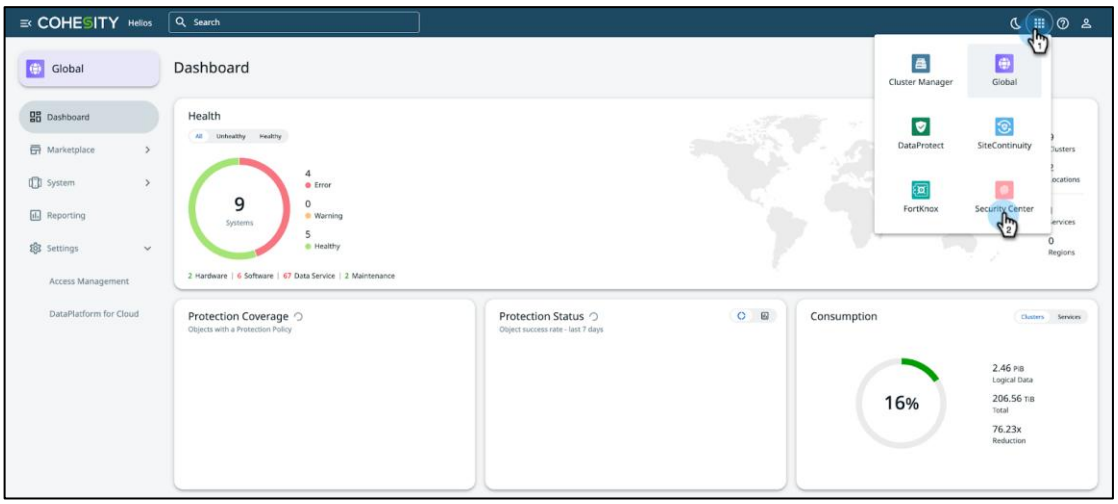
Configure Cohesity Security Center

Cohesity Security Center is an application that allows security admins and analysts to understand their security posture and access Cohesity's data security capabilities from one application.

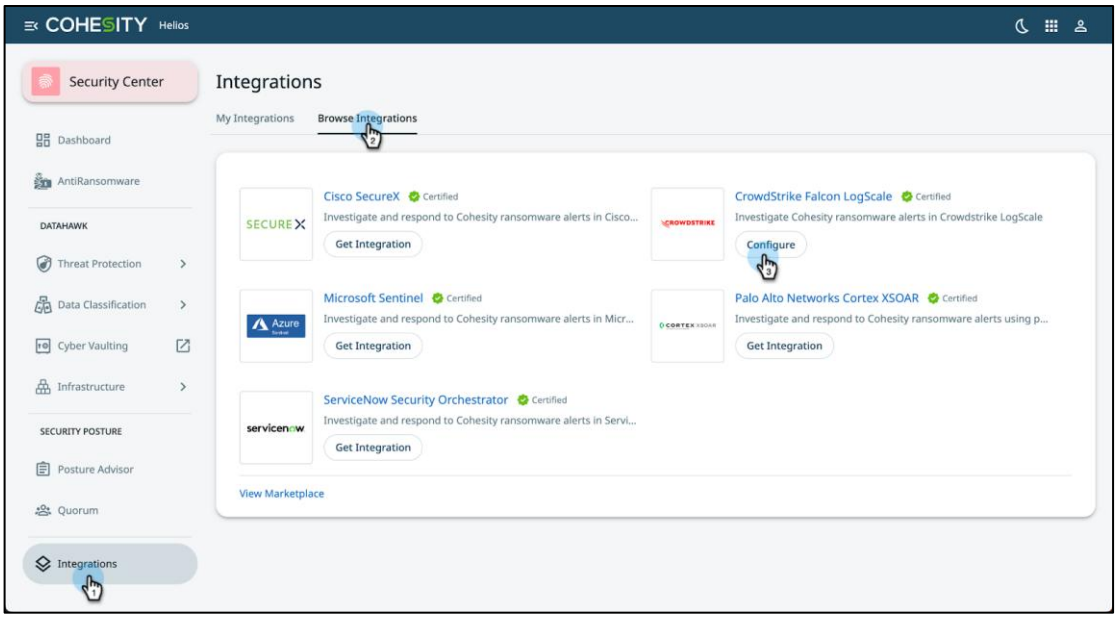
The next step is configuring the CrowdStrike Logscale instance details on the **Cohesity Security Center** to build a secure connection to fetch the anomaly alerts.

To add the **Logscale instance** details on **Cohesity Security Center**:

1. From the Cohesity dashboard, click the app-selector menu and click **Security Center**.



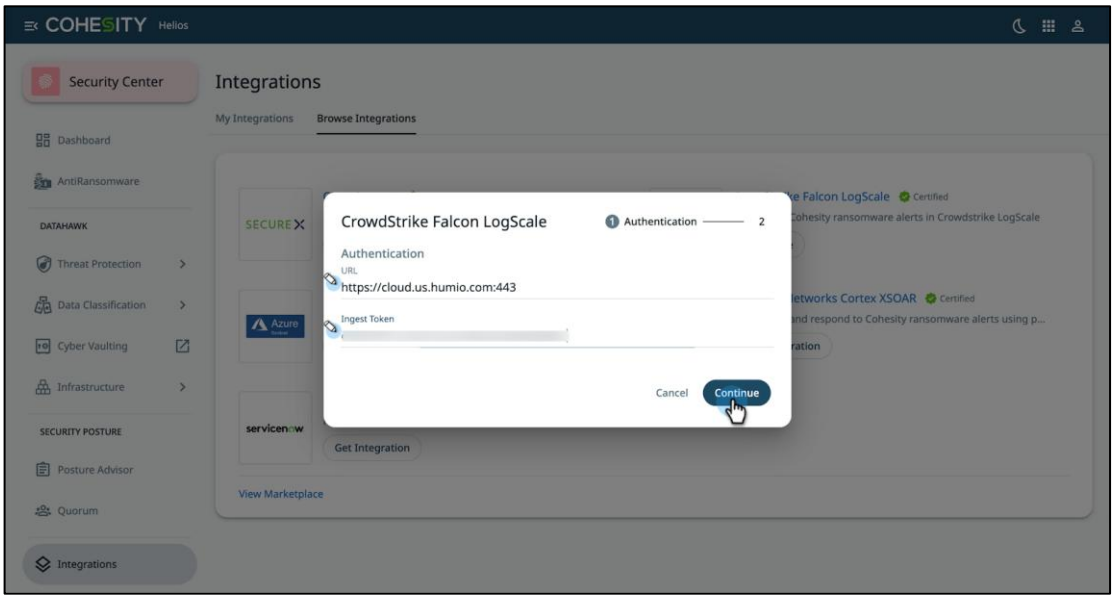
2. In **Security Center**, select **Integrations > Browse Integrations.** You will see the list of all Cohesity-developed security integrations. Select **Configure** under the listed **CrowdStrike Falcon Logscale** application.



3. Enter the **Falcon Logscale Instance** authentication details and click **continue.**

a. **URL -** < Enter the Logscale URL instance. >

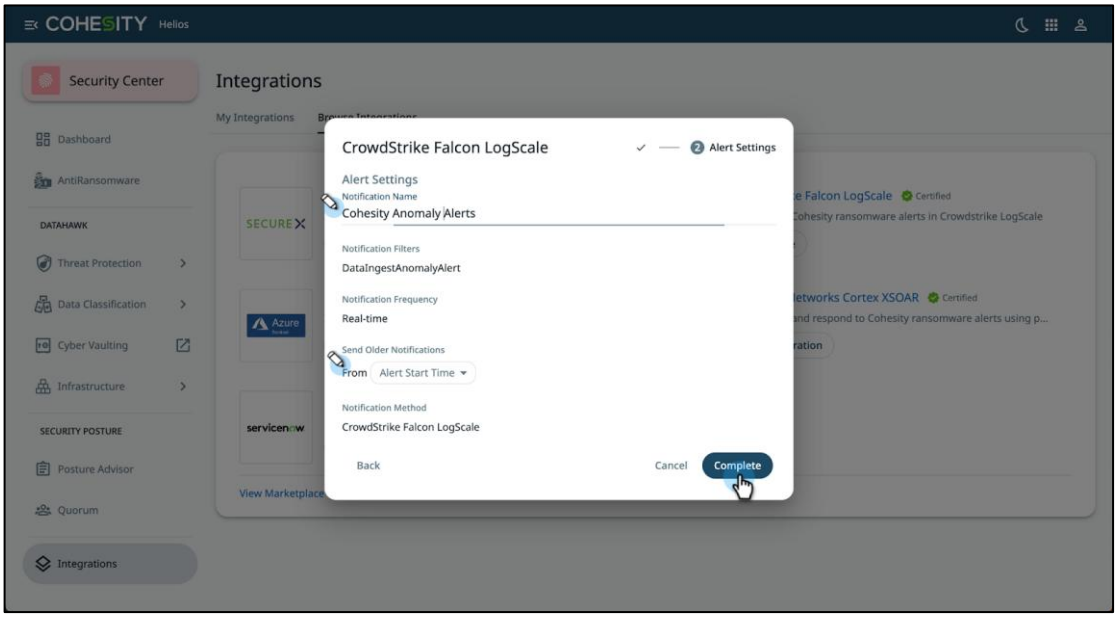
b. **Ingest token -** < Enter the ingest token generated in step 2.>



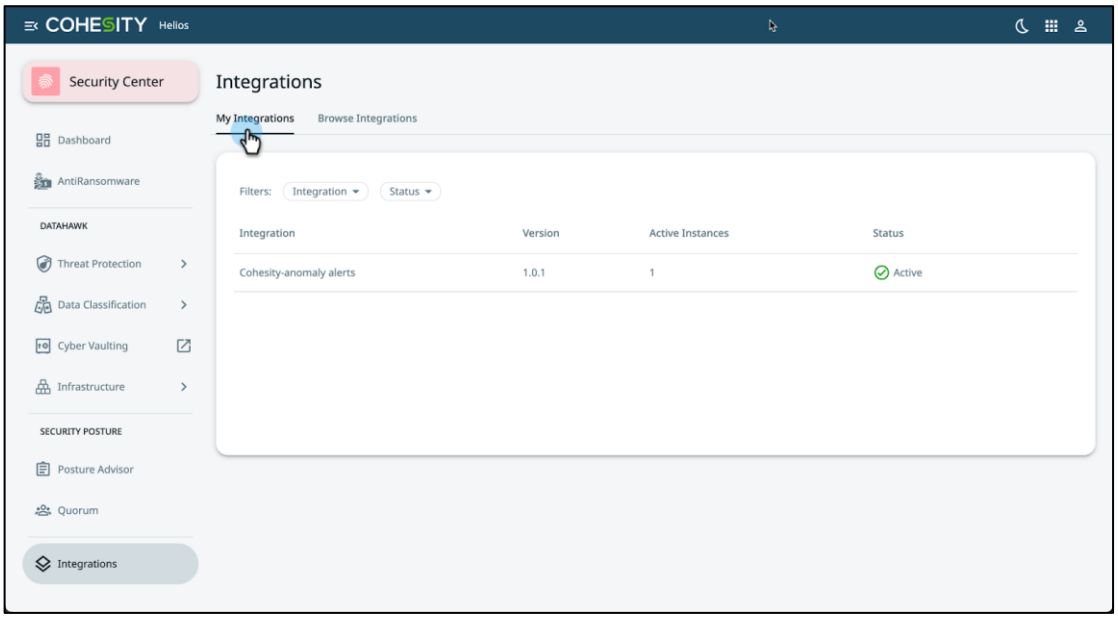
4. Enter the **Alert Setting** details and click **Complete.**

a. **Alert Notification name -** < Enter the notification name.>

b. **Alert start time -** < Select the time frame from which to capture the alerts.>

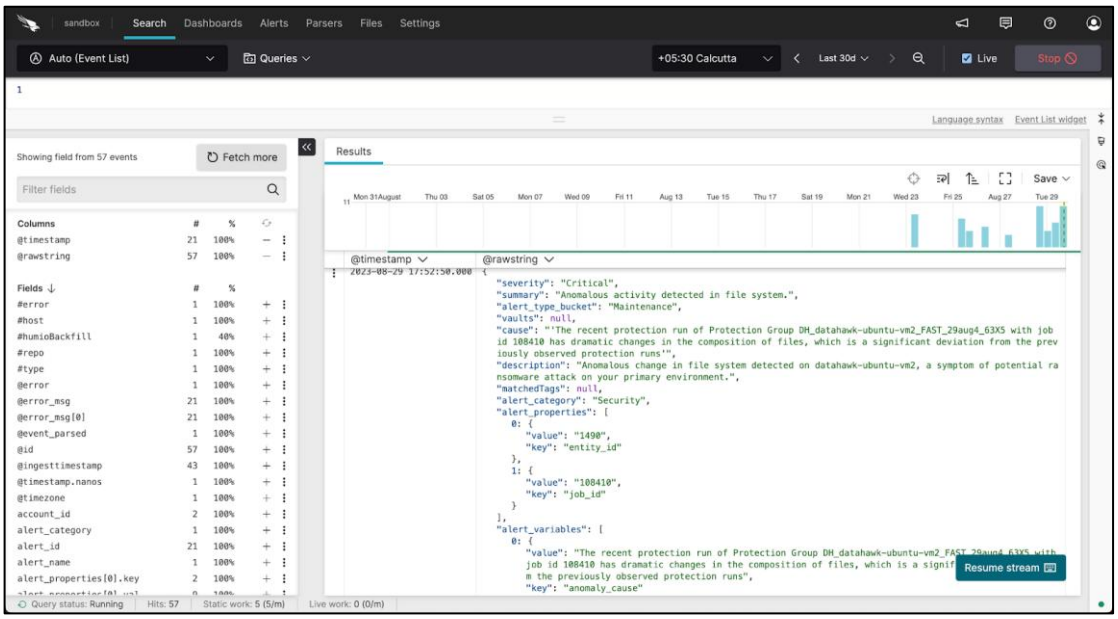


5. Select **My Integrations** tab to see the successful integration status as **Active.**



NOTE: You can also Pause or Delete the instance details if it's no longer required to send anomaly logs to CrowdStrike.

6. You will see the anomaly alerts being pushed to CrowdStrike Logscale under the selected repository.

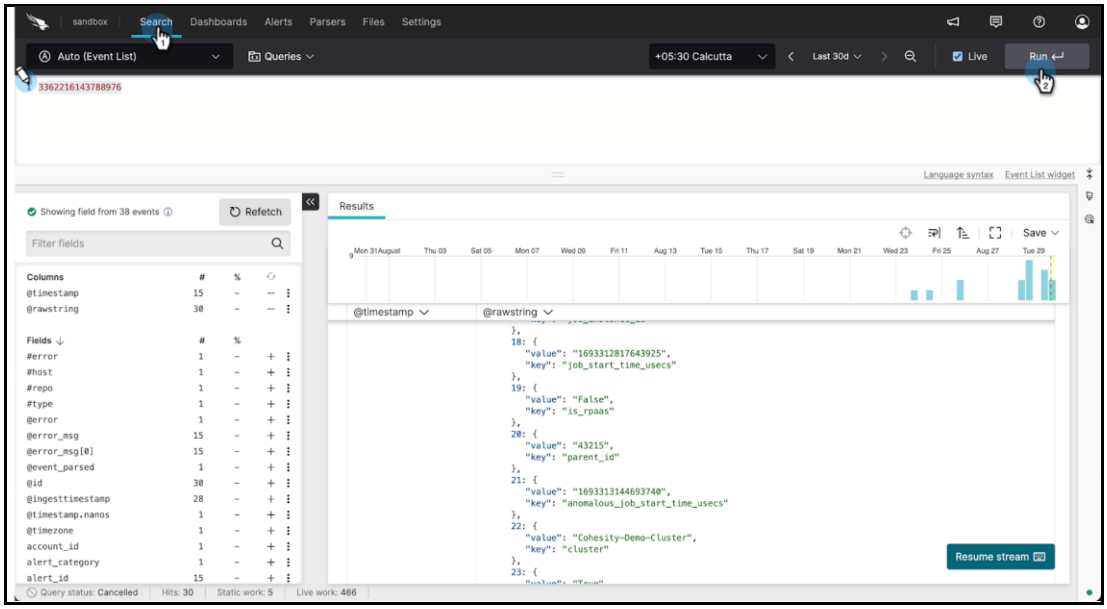


Search Data in Repository

Once you have your Cohesity alerts stored and streaming into Logscale, you can search the data stored in a repository by entering items and queries in the field box in the **Search** tab, leveraging the Logscale Query Language Syntax.

To run the search query to fetch the Cohesity log data:

1. Select the repository and select the **Search** tab.
2. Type one or more search terms in the **Search** box with the required time interval and select **Run.**



3. The search results appear in the event list. In the above example, we filter by selecting only alerts containing the **cluster id=336221614378897** anywhere in the alerts data within that repository.
4. You can also create a dashboard to monitor event logs with Logscale more efficiently.

Conclusion

In conclusion, the integration of CrowdStrike Falcon Logscale 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.

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:

- Rob Young, Product Manager, Competitive Intelligence
- Mukunda Gogoi, Engineering
- Sheetal Venkatesh, Product Management
- Subash Babu, Staff Technology Editor

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.2	Aug 2025	Republished with latest template
1.1	July 2024	Republishing
1.0	Oct 2023	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 44 of the Fortune 100.

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