Dragos Platform Integration Guide

The Dragos Platform is operational technology (OT) cybersecurity technology that delivers unmatched visibility of your industrial control system (ICS) assets and communications. It rapidly pinpoints threats through intelligence-driven analytics, identifies and prioritizes vulnerabilities, and provides best-practice playbooks to guide teams as they investigate and respond to threats.

Deployment Type

This integration supports **vendor cloud**, **private cloud**, and **on-premises** deployments through **port 443**.

If you already know that your environment supports these deployments, continue to the next step. If you are unsure whether your organization supports these deployments, please ensure your organization's compatibility before continuing.

Required Information and Setup

To integrate GreyMatter with Dragos, collect the following details:

- URL
- API ID
- Key Secret

See instructions below to gather the required information.

Enable API Keys

API Key access is disabled within Dragos by default. To enable:

1. Open **Admin** in Dragos.
2. Click **SiteStore Management**.
3. Click **Authentication Providers**.
4. Enable API Key Access.

Collect API Key and Secret

1. In Dragos, navigate to **Admin**.
2. Select **Users**.
3. Click + **Add New API Key**.
4. In the Generate New API Key Box, add the **Name** (i.e. My External App).
5. Click **Generate Key**.
6. Copy the API Key and secret from the message box.

Warning: This is the only time the secret is displayed. Once the message box is closed, there is no way to retrieve the secret. If the secret is lost, delete the API key and generate a new one.

7. Click **Ok**.

Add ReliaQuest IP Adresses

If your environment does not allow public access, you'll need to whitelist the ReliaQuest IP addresses within Dragos.

See the RQ IP Allowlist.

Permissions and Functionality

Permissions

GreyMatter Capability	Action(s)	Required Permission
Detect	Detection at Source – Vendor Authored	notification:read notification:update vulnerability:read vulnerability:update network:read
Respond	Enrich Host/Asset	asset:read vulnerability:read

Respond

Playbook Name	Description	Required Input Variables
Enrich Device	Returns details about a given asset including associated vulnerabilities.	Asset ID • Found in the top right corner of any asset record. • Provided with vulnerability detections. • Example: 41

Detect

Dragos supports **Detection at Source (Vendor Authored).**
Notifications: Retrieves alert notification records. **Note Syncing** *is not* supported. **State Syncing** *is* supported**.**
Vulnerabilities: Retrieves Vulnerability detections. **Note Syncing** *is no*t supported. **State syncing** is.

Asset Inventory

Asset Inventory provides a comprehensive overview of your digital environment by integrating directly with Dragos Platform, providing real-time insights into what assets you own, their status, and potential risks.