Falcon Adversary Intelligence Integration Guide

With CrowdStrike Falcon Adversary Intelligence, you gain access to real-time endpoint protection, robust security analytics, and threat intelligence that helps keep your data safe and secure. With the addition of ReliaQuest's GreyMatter, you now have even greater visibility and proactive management over your network security. This powerful integration ensures your endpoint is protected, not only against current threats, but future threats that may come your way. You can trust this integration to be a powerful shield of protection and offer peace of mind when it comes to your cybersecurity.

Important: If you are integrating multiple CrowdStrike products with GreyMatter, you will only need one API client ID configured with the unique required permissions for all applicable CrowdStrike products.

For example, CrowdStrike Falcon Insight and CrowdStrike Falcon Adversary Intelligence integrations with GreyMatter require one API client ID configured with the API permissions for both Insight & Falcon Adversary Intelligence. You should submit one request for API client ID creation and include the API account permissions for both Insight & Falcon Adversary Intelligence together. Please refer to each product's documentation for each product's specific API requirements.

Deployment Type

This integration requires **vendor cloud** deployments.

If you already know that your architecture supports one of these deployments, continue with setup. If you are unsure whether your organization can use one of these deployment types, please ensure compatibility before continuing.

Required Information and Setup

To integrate GreyMatter with Crowdstrike Falcon Adversary Intelligence, collect the following details:

- URL
  - Default: https://api.crowdstrike.com
- Client ID
- Client Secret

See instructions below to gather the required information.

Create API Clients

1. Within Crowdstrike, select Support and Resources, Resources and Tools, and then API Clients and Keys.
2. Click **Create API Client**.
3. Enter the **API Client details**:

- Client Name (required) can be something like “GreyMatter Falcon Adversary Intelligence Integration”
- Description (optional)
- API Scopes (required):
  - Select the Read and/or Write boxes next to a scope to enable access to its endpoints.
  - At least one scope must be assigned.

4. Click **Create** to generate the client ID and secret.

Save the Client ID and Secret for input on the GreyMatter Connections Settings page later.

Functionality

Permissions

See Crowdstrike API Documentation.

GreyMatter Capability	Tech Action	Required Permission
Respond	Analyze File	Sandbox (Falcon Intelligence Recon) - Read & Write
	Analyze URL	Sandbox (Falcon Intelligence Recon) - Read & Write
	Enrich Hash	Indicators (Falcon Intelligence) - Read
	Enrich IP	Indicators (Falcon Intelligence) - Read
	Enrich Domain	Indicators (Falcon Intelligence) - Read
	Enrich URL	Indicators (Falcon Intelligence) - Read

Respond

Playbooks

PLAYBOOK NAME	DESCRIPTION	REQUIRED INPUT VARIABLE(S)
Analyze File	Initiates a sandbox analysis on the specified file hash and returns a report ID, which is used in the “Scan Results” playbook. * In the CrowdStrike Falcon console, navigate to “Counter Adversary Operations” > “Intelligence Operations” > “Sandbox” to view sandbox submissions. The file must be manually or automatically uploaded into the Falcon Sandbox first. If you have Falcon Prevent, automatic submissions can be enabled to see analysis on all Window, Mac, and Linux quarantined files. Hosts assigned to prevention policies with enabled Quarantine and Machine Learning settings automatically upload all quarantined files for Falcon Sandbox analysis.	**File Hash** SHA256 Example: 8ba410345941a054e733965b72235848b55417439a08d47a7a719ed8054e0738

Analyze URL	Initiates a sandbox analysis on the specified URL and returns a report ID, which is used in the “Scan Results” playbook. * In the CrowdStrike Falcon console, navigate to “Counter Adversary Operations” > “Intelligence Operations” > “Sandbox” to view sandbox submissions.	**URL** Example: https://www.example.com Note: URL must start with ‘http’, ‘https’ or ‘ftp’.
Scan Results	Retrieves a sandbox report summary, which can include information such as the threat level, threat score, and tags. In the CrowdStrike Falcon console, navigate to “Counter Adversary Operations” > “Intelligence Operations” > “Sandbox” to view sandbox submissions.	**Report ID** Example: f4450c1222eb482eb927572592606403_8b1339977b834908966bf2a4817cc84e
Enrich Hash	Returns IOC information on the hash, including malware families, threat types, and actors. In the CrowdStrike Falcon console, navigate to “Counter Adversary Operations” > “Intelligence Operations” > “Indicators” to view indicators of compromise.	**File Hash** SHA256 example: 805bd484b5301403590a05f27242ffb02e4544d7808082d33dcc305df26f2f69 MD5 example: fba5a91e225d11f257bd1ce20d0e2537
Enrich IP	Returns IOC information on the IP, including malware families, threat types, and actors. In the CrowdStrike Falcon console, navigate to “Counter Adversary Operations” > “Intelligence Operations” > “Indicators” to view indicators of compromise.	**IP Address** Example: 1.1.1.1
Enrich Domain	Returns IOC information on the domain, including malware families, threat types, and actors. In the CrowdStrike Falcon console, navigate to “Counter Adversary Operations” > “Intelligence Operations” > “Indicators” to view indicators of compromise.	**Domain** Example: domain.com
Enrich URL	Returns IOC information on the URL, including malware families, threat types, and actors. In the CrowdStrike Falcon console, navigate to “Counter Adversary Operations” > “Intelligence Operations” > “Indicators” to view indicators of compromise.	**URL** Example: https://www.example.com

*Note for these playbooks:

- There is a submission quota for the Falcon Sandbox that can be checked in the CrowdStrike Falcon Sandbox Console.

- This playbook runs on multiple detonation environments:
  - Windows 10, 64-bit
  - Windows 11, 64-bit
  - Windows 7, 64-bit
  - Linux Ubuntu 20, 64-bit (Analyze file only)
  - MacOS Catalina 10.15 (Analyze file only)
- Time required for analysis varies but is usually less than 15 minutes. Wait at least 15 minutes before running the Scan Results playbook.