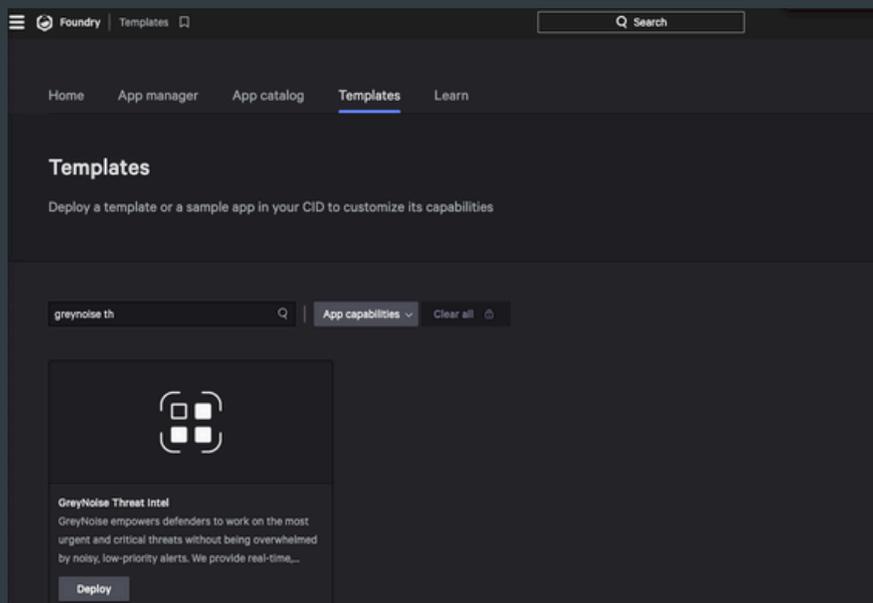


# SIEM Integration Overview: CrowdStrike NG-SIEM

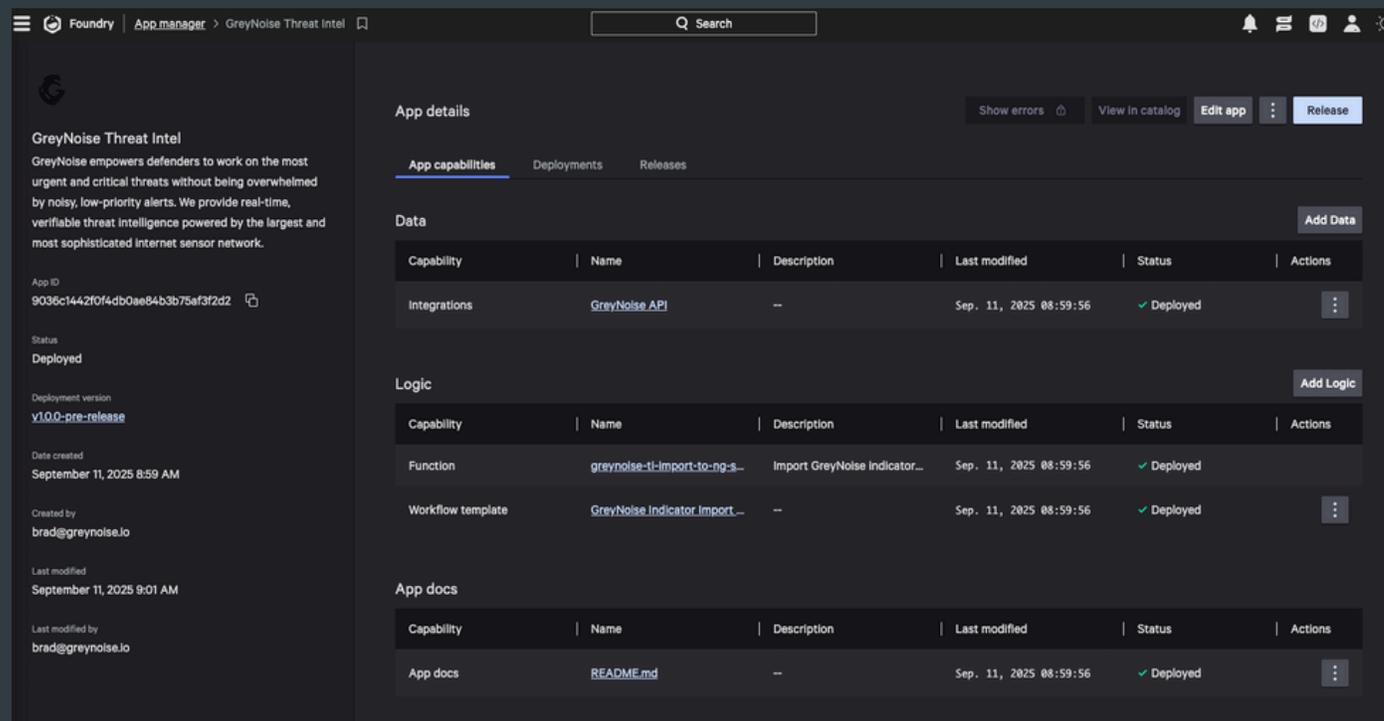
## Install Foundry App

The GreyNoise Threat Intel app for Foundry is located in the Templates section of Falcon Foundry.

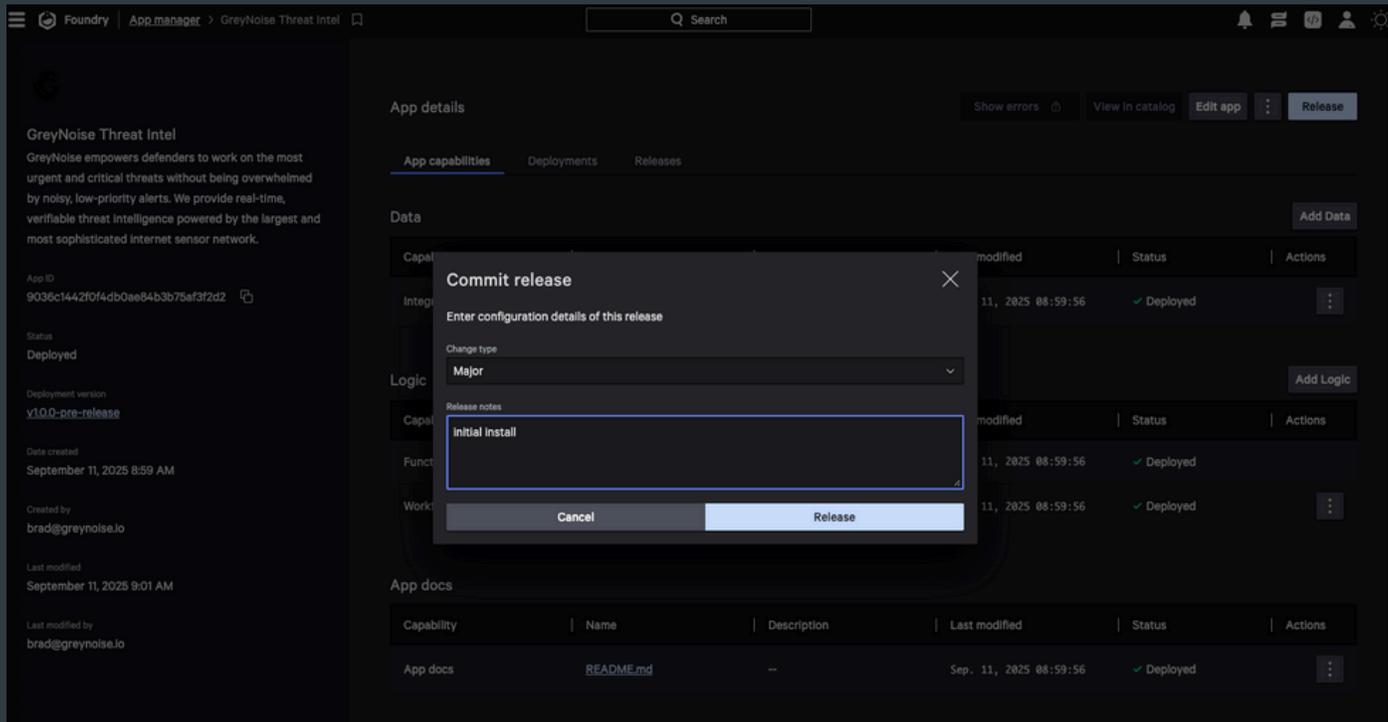
Navigate to Foundry --> Templates --> Search for GreyNoise Threat Intel. Then click the Deploy button.



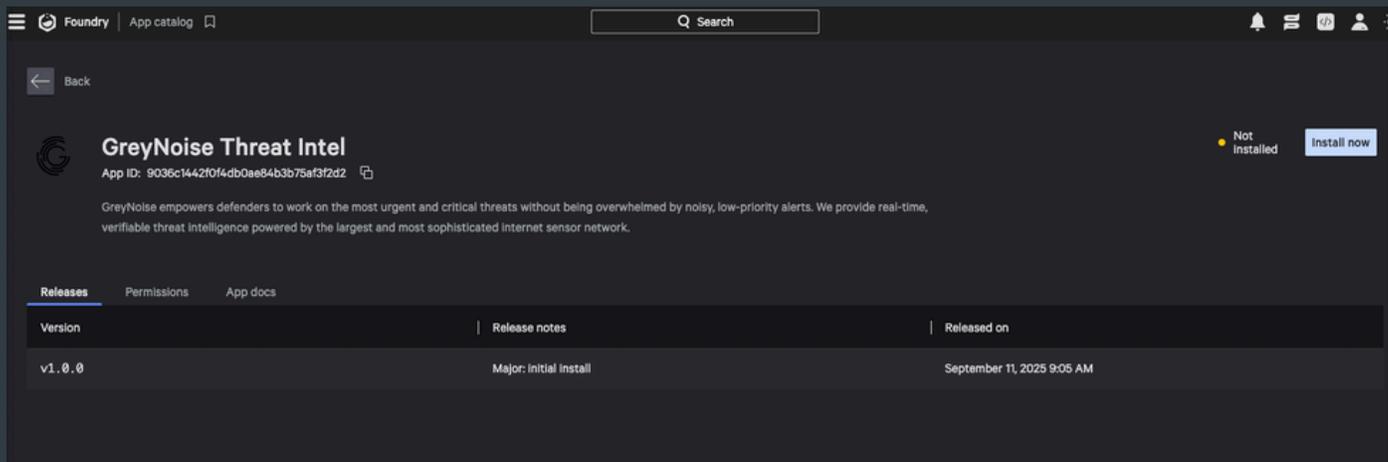
After the app template is deployed, navigate to Foundry --> App Manager --> Click on the GreyNoise Threat Intel App.



Click the Release Button to create the first Release available, selecting Major release and giving it a comment of something similar to "Initial Release":



The app is now available to be configured in the App Catalog. Click the Install Now button:



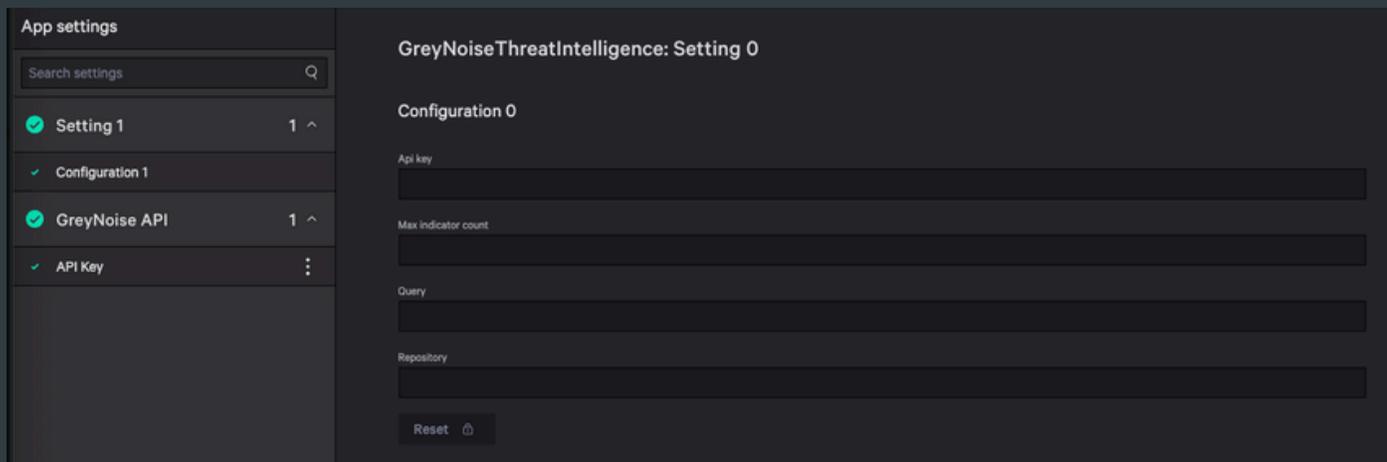
## Foundry App Components

The GreyNoise Foundry App for CrowdStrike Falcon includes three components:

- An integration to the GreyNoise API to use within Fusion SOAR Workflows
- A logic function that interacts with the GreyNoise API to create a Lookup File and uploads it to NG-SIEM
- A pre-built Workflow to run the logic function daily at 0300 UTC.

# Configure an Instance of the GreyNoise App

After installing the Foundry App, two configuration sections need to be configured.



## GreyNoise API Configuration

This setting section includes two values and enables the authentication for adding GreyNoise API actions into Fusion SOAR workflows.

**Name:** A name for the API credentials to help identify them, ie GreyNoise - Service Account Alpha

**API Key:** The API key to be used, from the GreyNoise Visualizer: Visualizer - My API Key

## Workflow Settings

This section provides the necessary settings for the automated workflow that creates and uploads the CSV file daily into the NG-SIEM Lookup files section.

**API Key:** The API key to be used, from the GreyNoise Visualizer: Visualizer - My API Key

**Max Indicator Count:** This option allows you to set a cap on the maximum number of indicators that will be stored in the lookup file. Ideally, this number should be larger than the total number of indicators in the defined query if you desire the file to contain all indicators from the query.

**Query:** The GreyNoise Query (GNQL) retrieves indicators from the GreyNoise API. By default, this should be set to `last__seen:1d` which will allow for all indicators observed in the last 24h to be stored in the lookup file.

**Repository:** This should be the name of the NG-SIEM lookup file repository that the Lookup File will be uploaded to with NG-SIEM. A default value of `search-all` will most commonly be used.

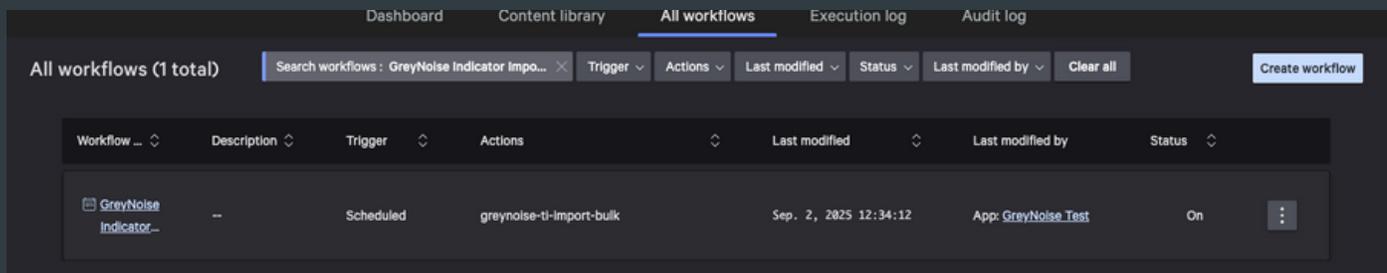
# Lookup File Workflow

The Foundry App installs and auto-enables a workflow to update the GreyNoise Lookup file daily. The workflow includes the following components:

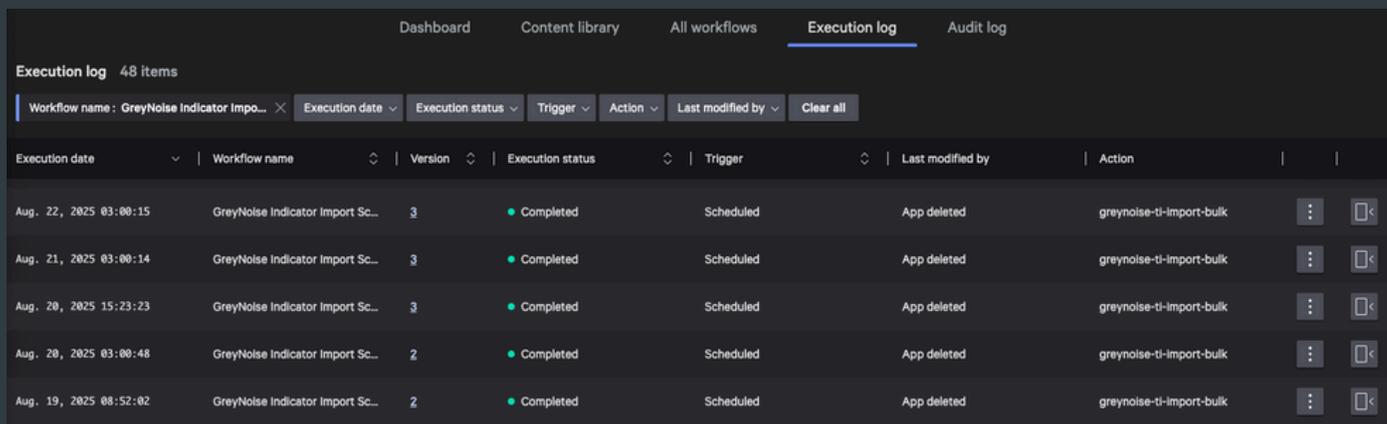
**Workflow: GreyNoise Indicator Import Scheduler**

**Function: greynoise-ti-bulk-import**

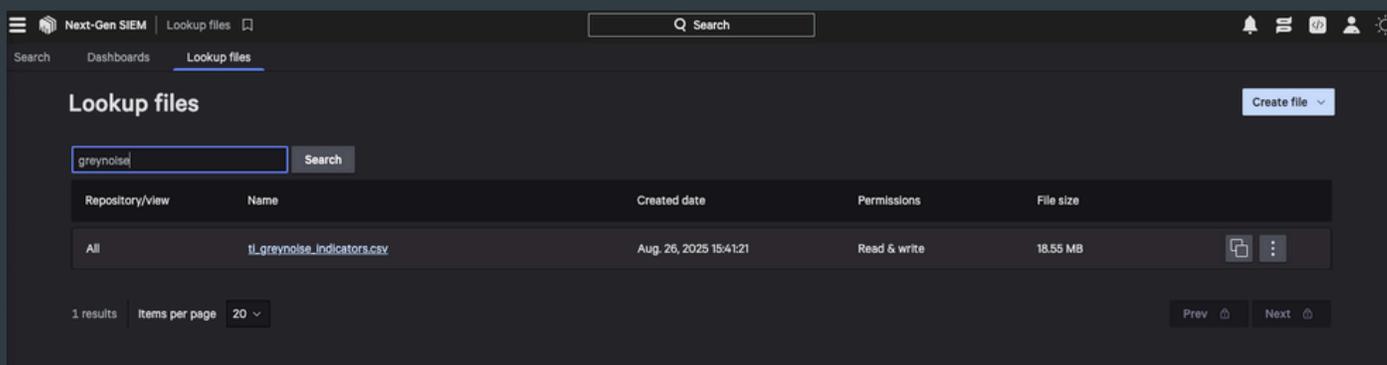
Once the settings are configured, the workflow can be found in the Fusion SOAR Workflows section and should be marked as enabled:



The execution log will show the state of each of the workflow runs:



This will then generate and update the `ti_greynoise_indicators.csv` file within NG-SIEM:



	source.ip	source.ip.greynoise.is.actor	source.ip.greynoise.is.classification	source.ip.greynoise.is.last_seen_timestamp	source.ip.greynoise.is.asn	source.ip.greynoise.is.source_country_code	source.ip.greynoise.is.s
1	37.120.175.157		unknown	2025-09-08 00:29:47	AS197540	DE	1
2	101.42.45.110		malicious	2025-09-08 00:02:10	AS45090	CN	0
3	94.176.35.15		unknown	2025-09-08 00:34:14	AS39501	IR	0
4	123.191.133.105		unknown	2025-09-08 00:59:52	AS4837	CN	0
5	217.208.31.152		unknown	2025-09-08 01:11:30	AS3301	SE	0
6	103.172.181.69		suspicious	2025-09-08 05:55:51	AS136442	MM	0

## Incorporating the Lookup File

The lookup file is designed to use the `match()` function to incorporate the GreyNoise data into the searches created within NG-SIEM. This additional metadata can then be used to filter out unnecessary events or to create additional alert types, depending on the use case.

The following is a sample search incorporating the lookup file:

Sampe NG-SIEM Query

```
#type = "greynoise-sensor-data"
| match(file="ti_greynoise_indicators.csv", field=[source.ip] , column=[source.ip], strict=false)
| "source.ip.greynoise.internet_scanner_intelligence.found" != True
```

Advanced event search

Search

1 #type = "greynoise-sensor-data"  
 2 | match(file="ti\_greynoise\_indicators.csv", field=[source.ip] , column=[source.ip], strict=false)  
 3 | "source.ip.greynoise.internet\_scanner\_intelligence.found" != True

Results Table: ti\_greynoise\_ind...

@timestamp	source.ip	source.ip.greynoise.is.classification	source.ip.greynoise.bs.trust_level	Vendor.session_id
Sep 8, 2025 11:00:35.599	148.72.158.192	malicious		dfa3e415ee3c4c28e73ab892629557
Sep 8, 2025 11:00:36.255	148.72.158.192	malicious		4537f2cb43aa6acab9d478944c104d
Sep 8, 2025 11:00:36.256	167.172.153.47	<no value>	<no value>	6440032520e024460317c2ef00645e
Sep 8, 2025 11:00:36.358	146.185.182.65	<no value>	<no value>	6d8fbf190d7c09c9b69dd754d7758a
Sep 8, 2025 11:00:36.430	146.185.182.65	<no value>	<no value>	892aec2238250d53a2451df6dcfb2
Sep 8, 2025 11:00:36.771	148.72.158.192	malicious		4d9e5bd042f5e9f1bca72a08fa08be
Sep 8, 2025 11:00:36.970	148.72.158.192	malicious		b4680eaffbcecd93cf56718d8320a
Sep 8, 2025 11:00:37.338	148.72.158.192	malicious		87f068eb9f7ddf71605992174459b5
Sep 8, 2025 11:00:38.086	103.240.6.24	<no value>	<no value>	17064ba2cec14a2fb216674d3531b8
Sep 8, 2025 11:00:38.934	148.72.158.192	malicious		e00a4534dd319208be38004576238f
Sep 8, 2025 11:00:42.381	148.72.158.192	malicious		978c4138bbd94ce26465154286cd
Sep 8, 2025 11:00:42.853	148.72.158.192	malicious		bd5a6d538bb2fab74c6cdf8cb81d
Sep 8, 2025 11:00:42.871	172.81.61.42	unknown		8ab5ca8d427828db76ad5711e772c4
Sep 8, 2025 11:00:45.849	104.255.152.19	<no value>	<no value>	bd9356368968440fa6ae01e1e66fe
Sep 8, 2025 11:00:46.657	148.72.158.192	malicious		6454bc67988cf80b32497425d913a0
Sep 8, 2025 11:00:50.028	118.26.105.52	<no value>	<no value>	7439e9afb6f521e1b618a2b2559c35
Sep 8, 2025 11:00:50.099	206.123.145.21	<no value>	<no value>	e5f280962a63d29ebb1da55d4460d4
Sep 8, 2025 11:00:50.291	35.159.62.55	<no value>	<no value>	bde248dbb534688420f595ecbafdd

Query status: Done Execution time: 42s 300ms Hits: 100 EPS: 2 Work: 5

Language syntax Event List widget

GREYNOISE greynoise.io/docs

Next-Gen SIEM | Advanced event search | Search

Search | Dashboards | Lookup files

Schedule search | Create correlation rule | Add to case | See in graph

All | Searches | Event List | -04:00 New York | Last th | Live | Run

```

1 #type = "greynoise-sensor-data"
2 | match(file="ti_greynoise_indicators.csv", field=[source.ip], column=[source.ip], strict=false)
3 | "source.ip.greynoise.internet_scanner_intelligence.found" != True

```

Results | Table: ti\_greynoise\_ind...

Last updated: 8 hours ago | Search table | Save

source.ip	source.ip.greynoise.bs.category	source.ip.greynoise.bs.name	source.ip.greynoise.bs.trust_level	source.ip.greynoise.is.actor	source.ip.greynoise.is.asn	source.ip.greynoise.is.classification	source.ip.g...
37.120.175.157	<empty string>	<empty string>	<empty string>	<empty string>	AS197548	unknown	2025-09-0
101.42.45.110	<empty string>	<empty string>	<empty string>	<empty string>	AS45090	malicious	2025-09-0
94.176.35.15	<empty string>	<empty string>	<empty string>	<empty string>	AS39501	unknown	2025-09-0
123.191.133.105	<empty string>	<empty string>	<empty string>	<empty string>	AS4837	unknown	2025-09-0
217.208.31.152	<empty string>	<empty string>	<empty string>	<empty string>	AS3301	unknown	2025-09-0
103.172.181.69	<empty string>	<empty string>	<empty string>	<empty string>	AS136442	suspicious	2025-09-0
123.18.103.191	<empty string>	<empty string>	<empty string>	<empty string>	AS45899	suspicious	2025-09-0
106.209.214.37	<empty string>	<empty string>	<empty string>	<empty string>	AS45609	unknown	2025-09-0
172.70.243.26	cdn	Cloudflare CDN	2	<empty string>	AS13335	unknown	2025-09-0
133.242.221.87	<empty string>	<empty string>	<empty string>	<empty string>	AS7684	unknown	2025-09-0
186.55.20.115	<empty string>	<empty string>	<empty string>	<empty string>	AS6057	malicious	2025-09-0
117.18.228.104	<empty string>	<empty string>	<empty string>	<empty string>	AS136255	suspicious	2025-09-0
109.87.101.244	<empty string>	<empty string>	<empty string>	<empty string>	AS13188	malicious	2025-09-0
94.26.48.117	<empty string>	<empty string>	<empty string>	<empty string>	AS48452	malicious	2025-09-0
106.209.189.114	<empty string>	<empty string>	<empty string>	<empty string>	AS45609	unknown	2025-09-0

Page Size 25 50 100 250

Query status: Done | Execution time: 42s 300ms | Hits: 100 | EPS: 2 | Work: 5 | LooScale version: 1.2011

Next-Gen SIEM | Advanced event search | Search

Search | Dashboards | Lookup files

Schedule search | Create correlation rule | Add to case | See in graph

All | Searches | Pie Chart | -04:00 New York | Last th | Live | Run

```

1 #type = "greynoise-sensor-data"
2 | match(file="ti_greynoise_indicators.csv", field=[source.ip], column=[source.ip], strict=false)
3 | "source.ip.greynoise.internet_scanner_intelligence.found" != True
4 | groupBy([source.ip.greynoise.is.classification])

```

Results | Data | Table: ti\_greynoise\_ind... | Events

vendor

Fields ↓ | No field names matched "vendor"

source.ip.greynoise.is.classification

- malicious 71.7% 38.0
- unknown 24.5% 13.0
- benign 1.9% 1.00
- suspicious 1.9% 1.00

Query status: Done | Execution time: 48s 936ms | Hits: 53 | EPS: 2 | Work: 2 | LooScale version: 1.2011

# Dashboards

The GreyNoise lookup file intelligence can also be incorporated into dashboards to monitor data sources and bring important information into view for users:

