GreyNoise Enrichment for Anomali ThreatStream

The GreyNoise Enrichment for Anomali ThreatStream enriches observables to identify activity associated with mass-internet scanning or known benign services, creating more time to investigate other higher-priority observables.

The enrichment supports both the GreyNoise Enterprise and Community APIs.

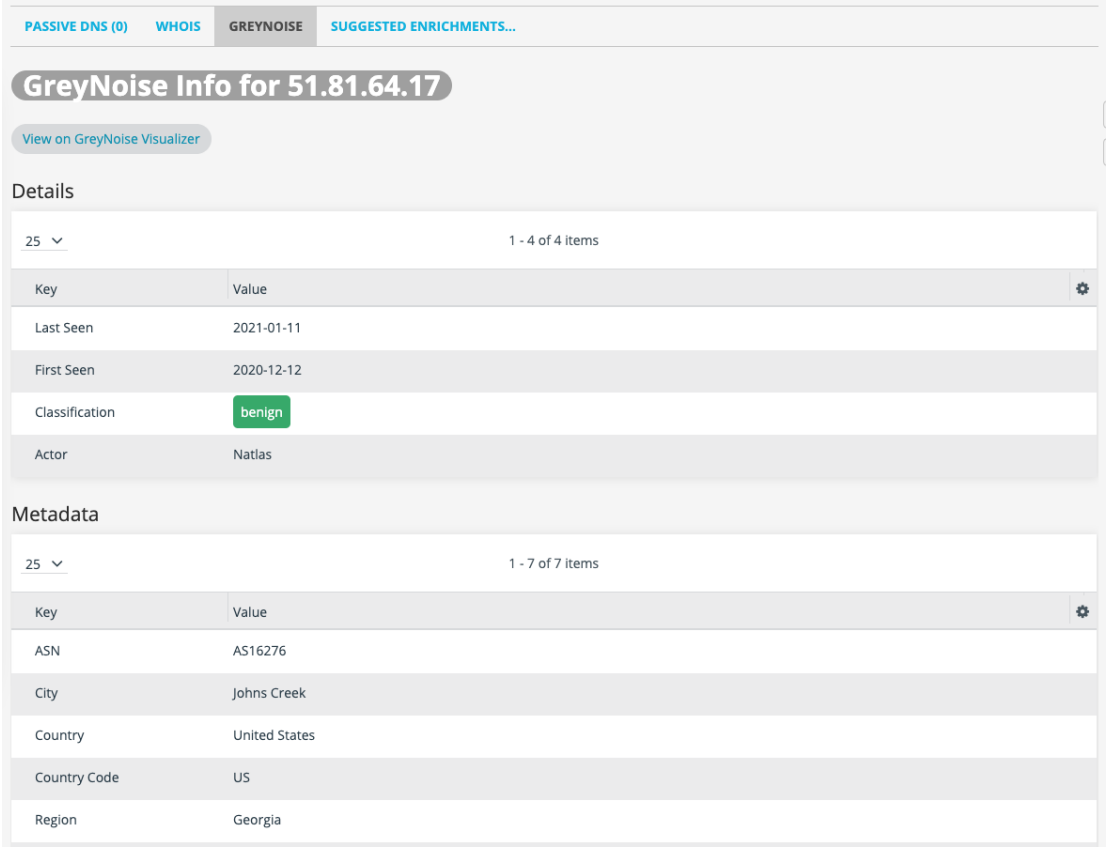
For Enterprise users, the enrichment provides the following information for IP address observables: intent, tags, first seen, last seen, geo-data, ports, OS, and JA3. It also identifies IP addresses belonging to benign services, VPN services, TOR exit nodes, and BOTs. If Enterprise users also have access to the IP Simiarlity or IP Timeline functionality, that information will also be included.

For Community users, a subset of the information is provided: intent, last seen, and actor/provider information.

Enrichment data is displayed on the GreyNoise tab in the Enrichments section of observable details pages or as part of the transform graph.

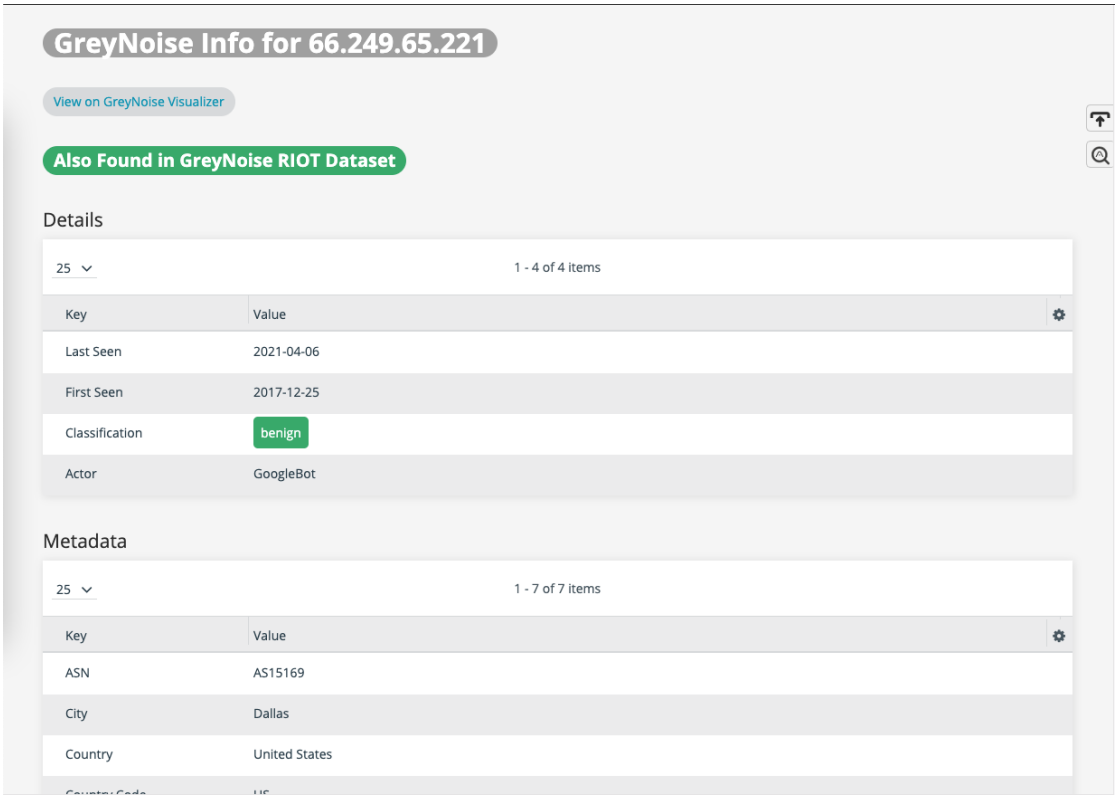
Context Enrichment:

GreyNoise Noise IP Response:

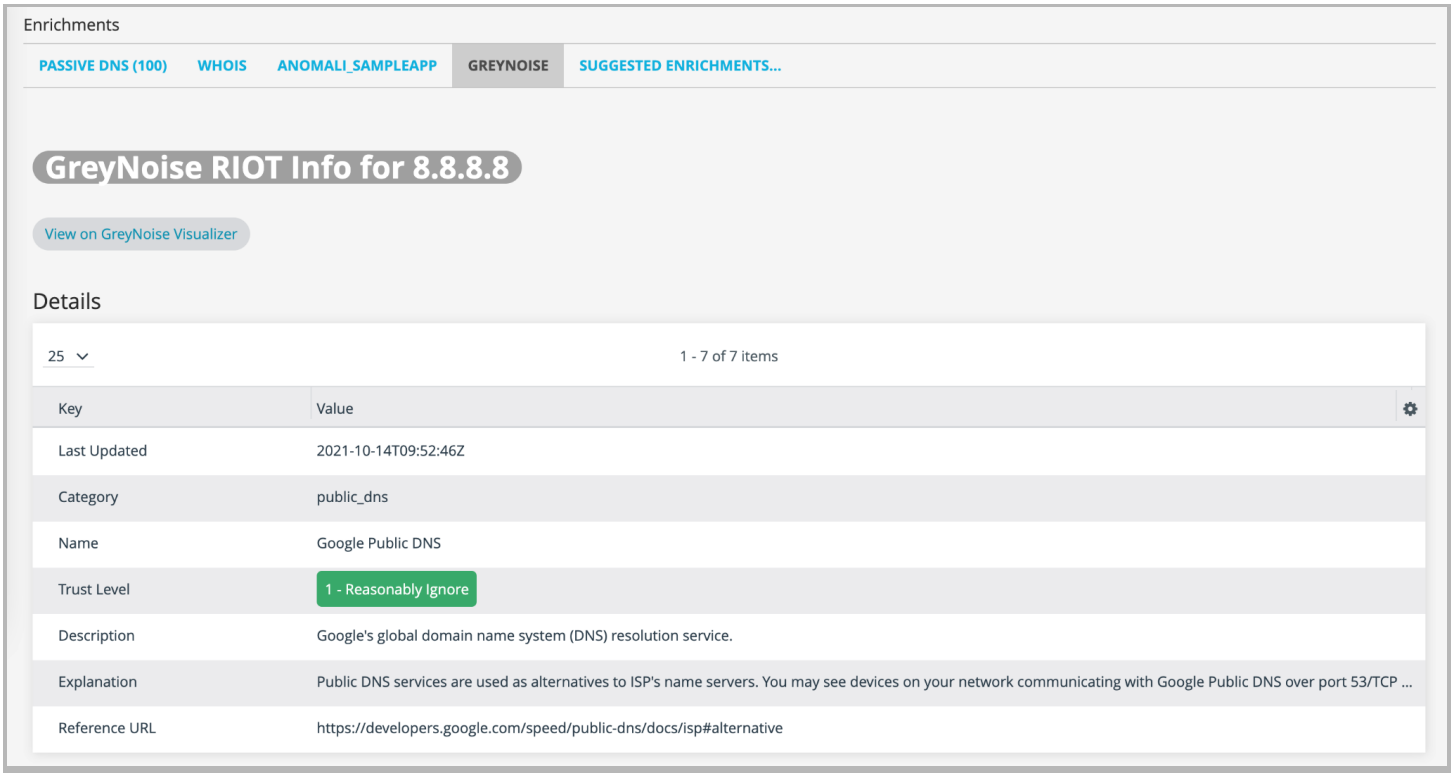


VPN Service	N/A
Port(s) / Protocol(s)	0/ICMP 1/TCP 3/TCP 4/TCP 6/TCP 7/TCP 9/TCP 13/TCP 17/TCP 19/TCP Output limited to 10 of 1031 items, see Visualizer for more details.
Tag(s)	404 Crawler Bitcoin Node Scanner Cobalt Strike Scanner Cobalt Strike SSH Client CounterStrike Server Scanner DNS Scanner DNSStatusRequest Crawler DNSVersionBindReq Crawler Dockerd Scanner EHLO Crawler Output limited to 10 of 54 items, see Visualizer for more details.
CVE(s)	CVE-1999-0526

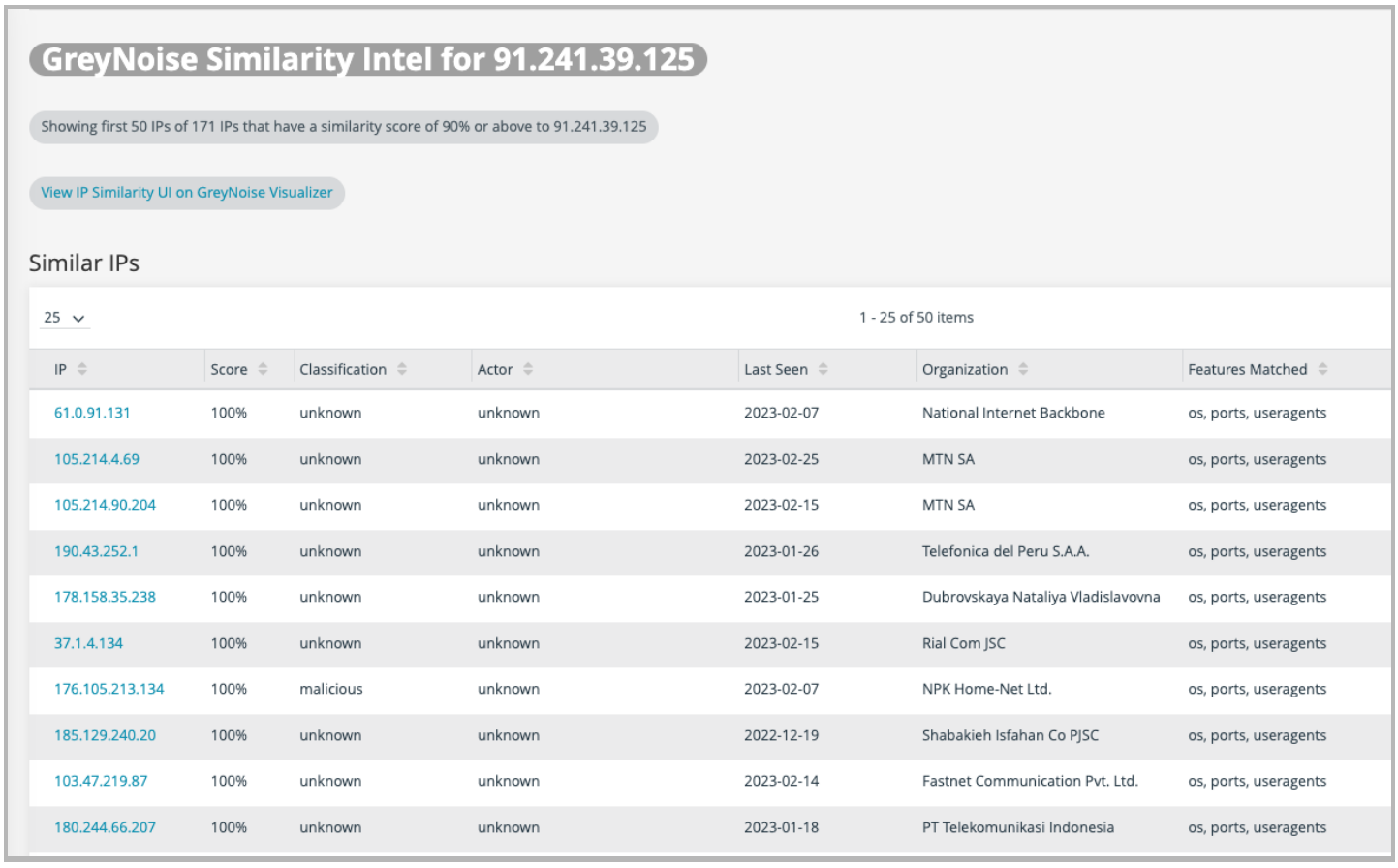
GreyNoise Noise IP Response with RIOT:



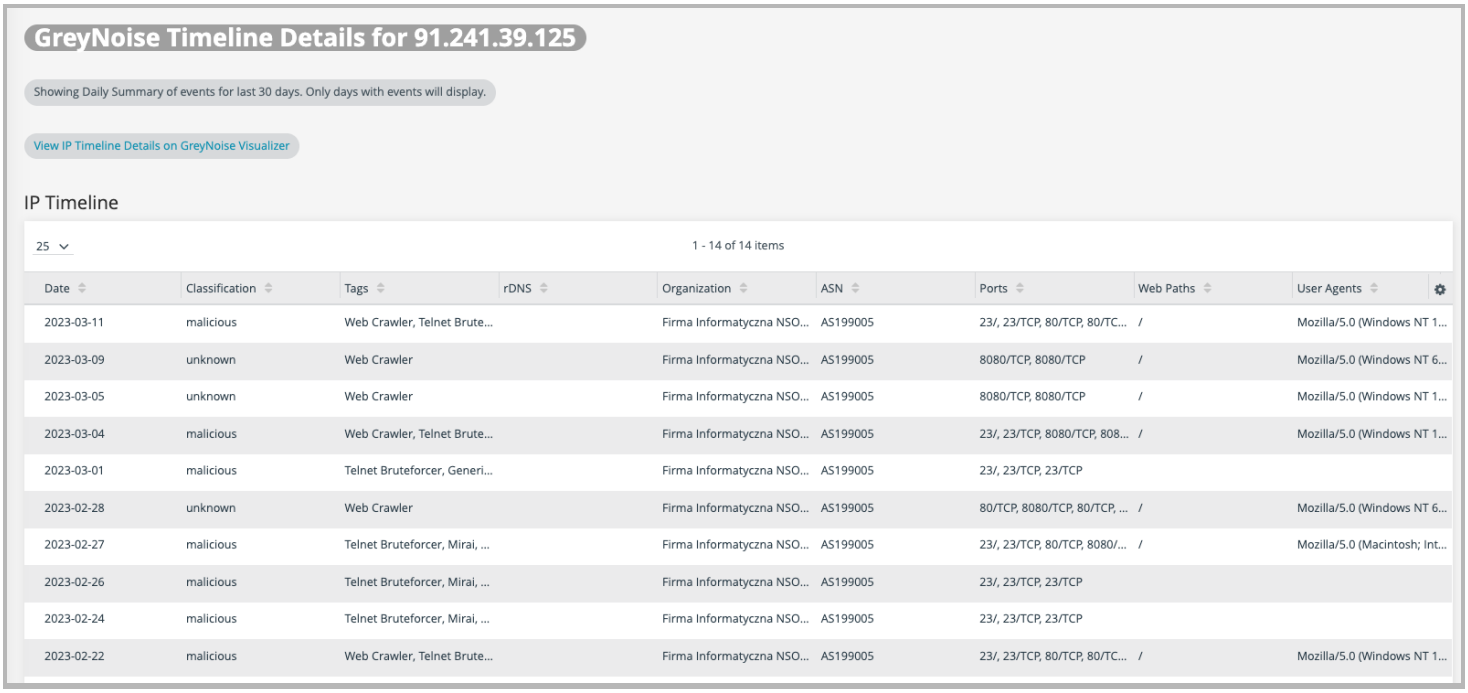
GreyNoise RIOT IP Response:



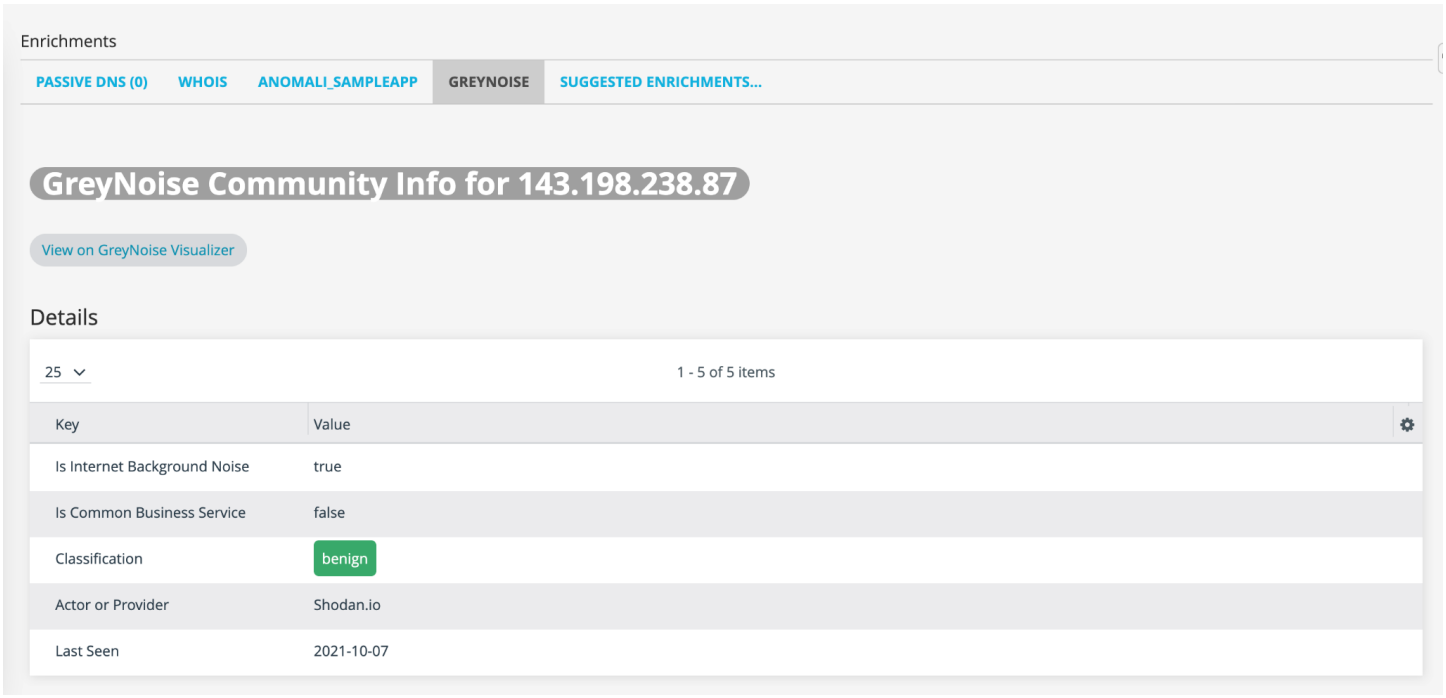
GreyNoise IP Similarity Response:



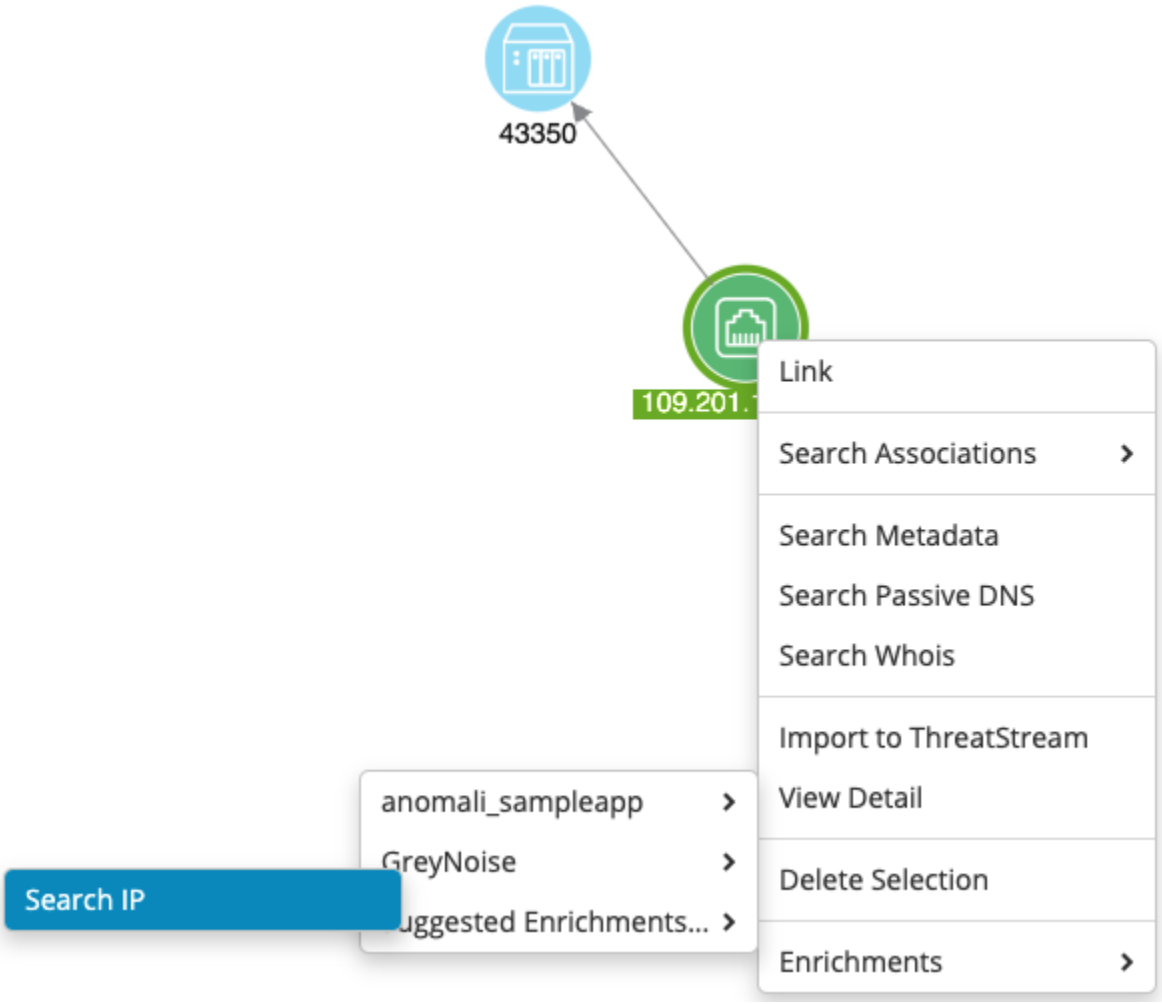
GreyNoise IP Timeline View:



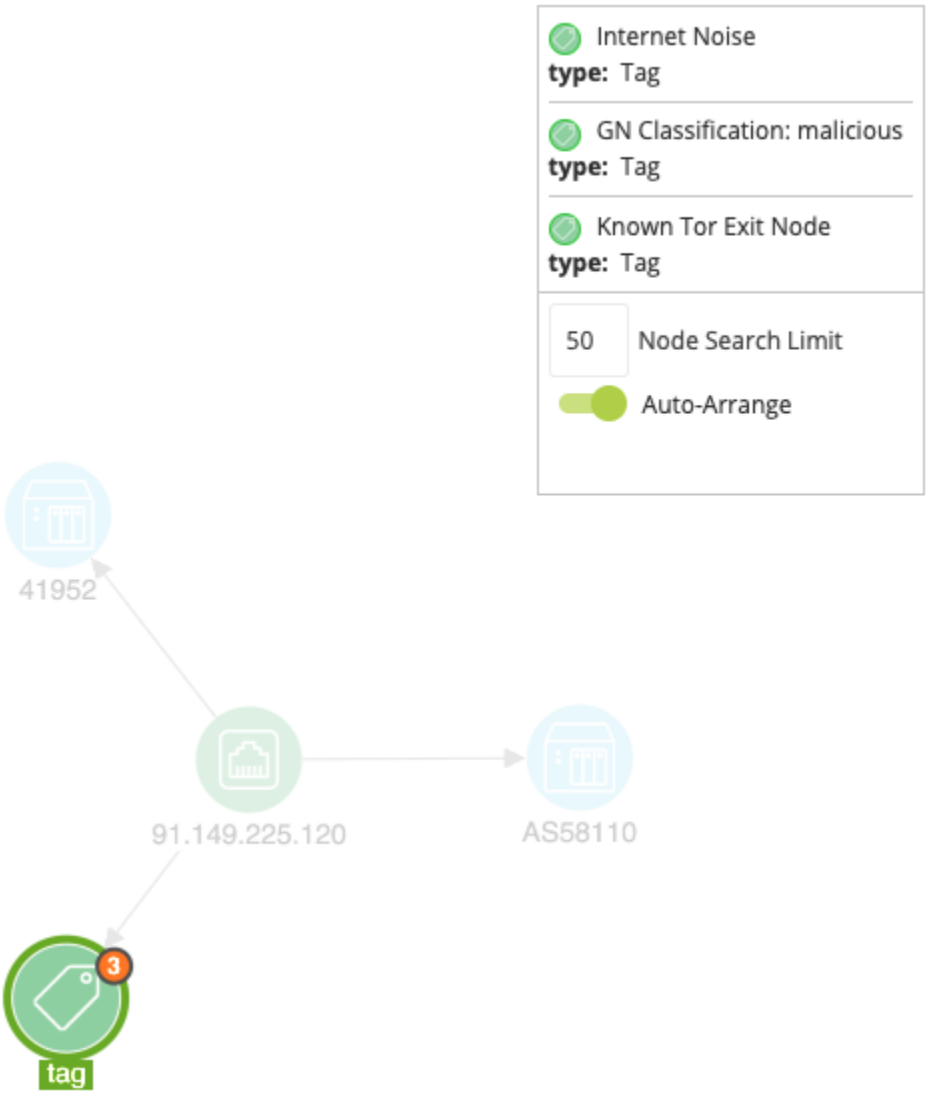
GreyNoise Community IP Response:



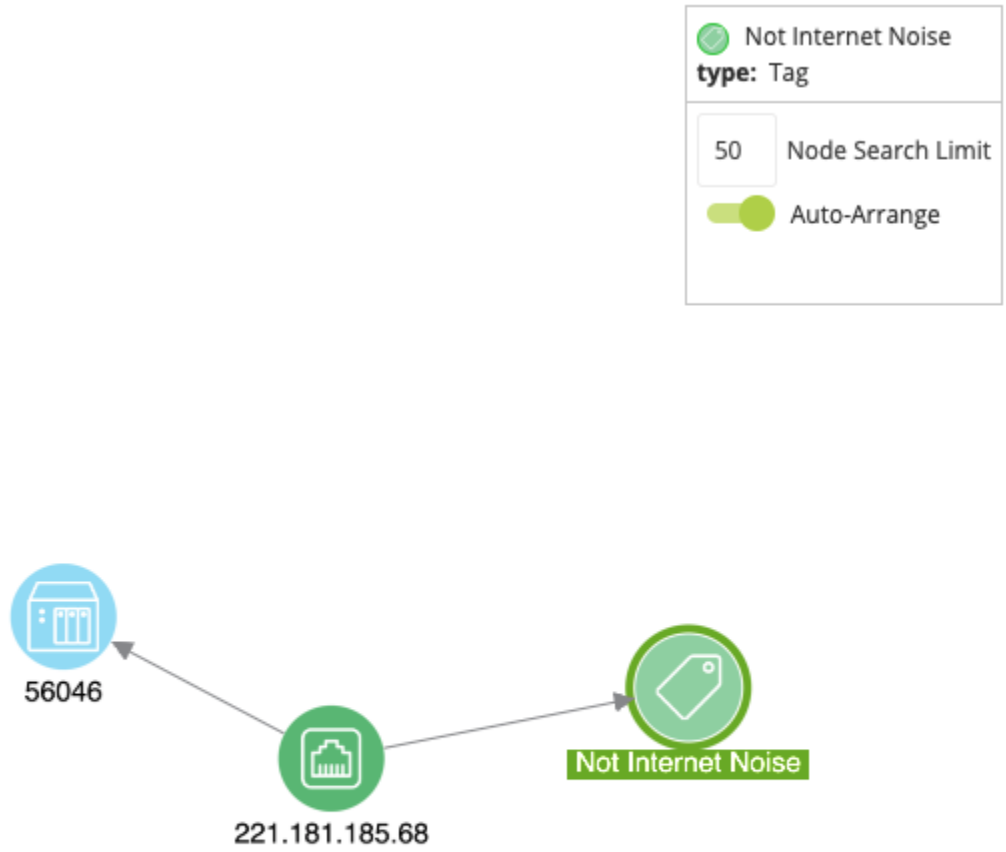
Pivot-Enrichment:



GreyNoise Noise IP Response:



GreyNoise Noise IP Response (Not Internet Noise):



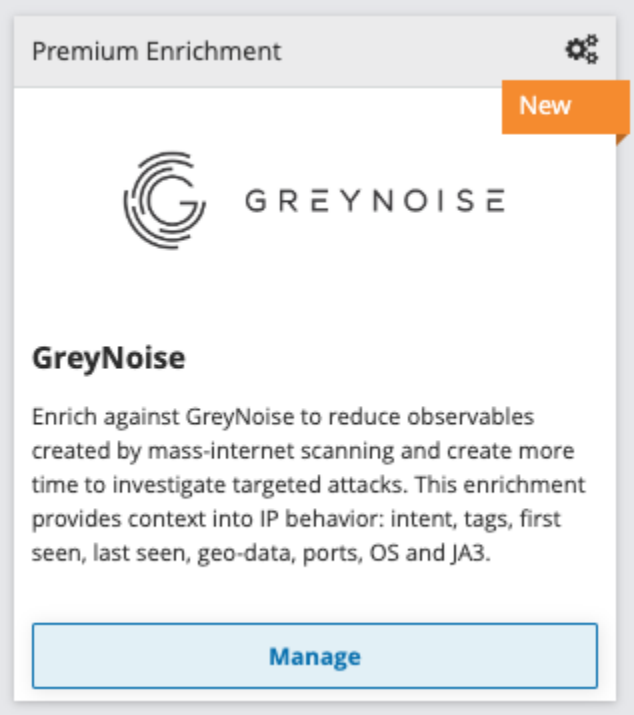
To read more about GreyNoise, see https://greynoise.io

The GreyNoise Enrichment enables the following commands:

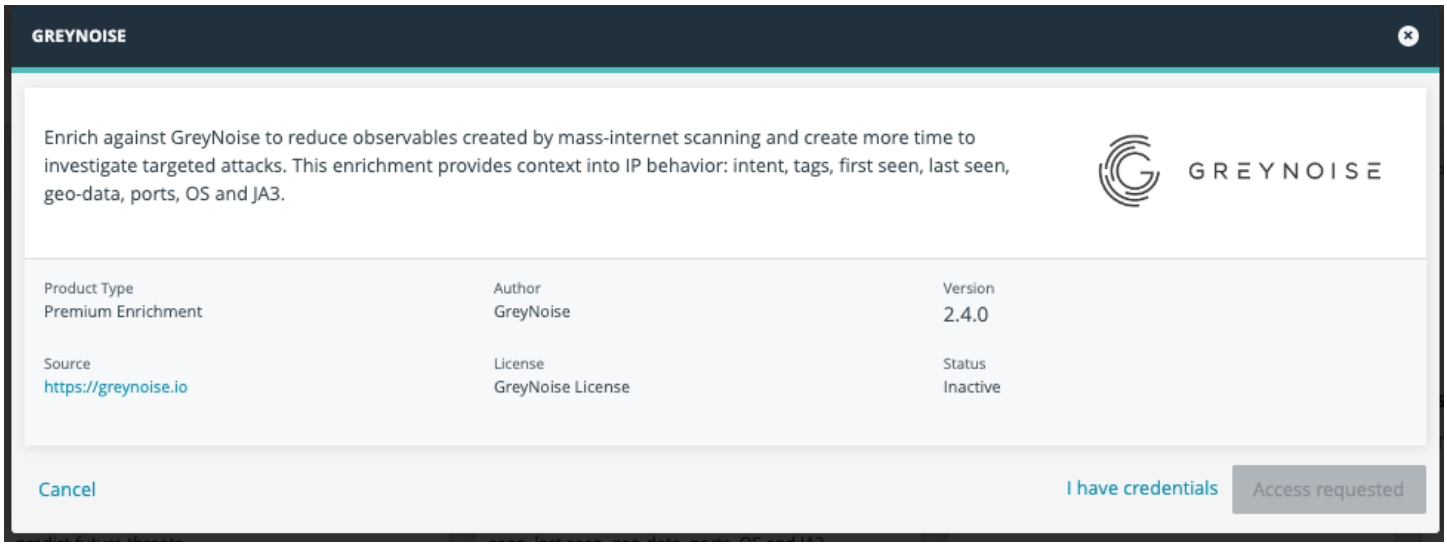
- Context Enrichment
  - enrichIP: returns IP context data from the GreyNoise Context and RIOT API
- Pivot Enrichment
  - Search IP: returns IP data points from the GreyNoise Context and RIOT API

To activate the GreyNoise enrichment:

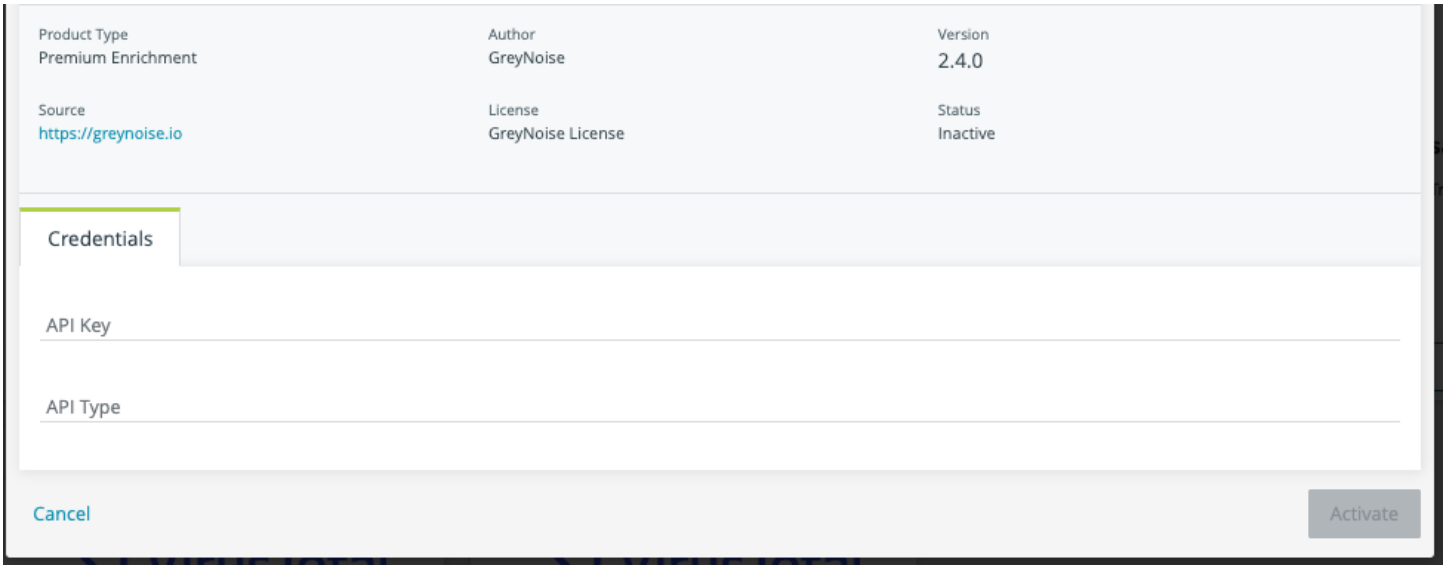
1. Log into the ThreatStream user interface
2. In the top navigation bar, navigate to the App Store and search for GreyNoise
3. Click “Manage/Get Access” in the GreyNoise Enrichment box



4. Click “I have credentials.”



5. Enter your GreyNoise API Key and select your API Type by entering either “enterprise” or “community” based on your API Key type. If no value or an incorrect value is entered, the default of “enterprise” will be used.



6. Click “Activate”. You should receive a “Successfully Activated Package” message. If an error occurs, please contact Anomali Support for assistance.

Note: If you do not have a GreyNoise API key, you can sign up for a 14-Day Free Trial at https://docs.greynoise.io or you can contact us at sales@greynoise.io to purchase an Enterprise Key.

Note: When you activate the GreyNoise Enrichment, if you configure the API type “community” and mistype your API key, your API queries will be processed as unauthorized queries. The GreyNoise API supports only a limited number of unauthorized queries. If you encounter a limitation unexpectedly, it might be due to authorization. Try re-entering the API key on the ThreatStream Integrations page. If this does not resolve the issue, contact sales@greynoise.io for help understanding your daily lookup limits.

Changelog:

v2.4.0

- Update IP Noise response to include Destination Country and Country Codes
- Renamed IP Noise response Country and Country Code to Source Country and Source Country Code
- Updated Visualizer Links
- Added support for IP Simalrity Information, when available to the Users API Key
- Added support for IP Timeline Information, when available to the Users API Key

v2.3.0

- Updates to metadata to define output types

v2.2.0

- Updated enrichment to hide some attributes when value is unknown to streamline the output
- Updated base URL for links to Visualizer
- Updated terminology around RIOT IPs for clarity
- Added RIOT Trust Level values

v2.1.0

- Added support for Community API IP Lookups

v2.0.0

- Add Pivot-Based Enrichment

v1.1.0

- Add support for Rule It Out (RIOT) IP Lookups

v1.0.4

- Add error handling for bad/missing API key

v1.0.3

- Code improvements
- Added missing VPN/VPN_Service and HASSH fields

v1.0.2

- Code improvements

v1.0.1

- Removed "seen" from table view as all returned results are seen
- Split data into 3 tables to help with analyst review of data
- Limited results to 10 for all list fields and included message on the total number of results found
- Replaced blank response with "None" or "Unknown", where applicable
- Added better error handling for non-200 response

v1.0.0

- Initial release
- Built enrichIP transform to use GreyNoise Context API lookup