

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 Similarity 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:

PASSIVE DNS (0)

WHOIS

GREYNOISE

SUGGESTED ENRICHMENTS...

GreyNoise Info for 51.81.64.17

View on GreyNoise Visualizer

Details

25

1 - 4 of 4 items

Key	Value	
Last Seen	2021-01-11	
First Seen	2020-12-12	
Classification	benign	
Actor	Natlas	

Metadata

25

1 - 7 of 7 items

Key	Value	
ASN	AS16276	
City	Johns Creek	
Country	United States	
Country Code	US	
Region	Georgia	

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 Info for 66.249.65.221

[View on GreyNoise Visualizer](#)

Also Found in GreyNoise RIOT Dataset

Details

25 ▾

1 - 4 of 4 items

Key	Value	⚙
Last Seen	2021-04-06	
First Seen	2017-12-25	
Classification	benign	
Actor	GoogleBot	

Metadata

25 ▾

1 - 7 of 7 items

Key	Value	⚙
ASN	AS15169	
City	Dallas	
Country	United States	
Country Code	US	

GreyNoise RIOT IP Response:

Enrichments

PASSIVE DNS (100)

WHOIS

ANOMALI_SAMPLEAPP

GREYNOISE

SUGGESTED ENRICHMENTS...

GreyNoise RIOT Info for 8.8.8.8

View on GreyNoise Visualizer

Details

25

1 - 7 of 7 items

Key	Value	
Last Updated	2021-10-14T09:52:46Z	
Category	public_dns	
Name	Google Public DNS	
Trust Level	1 - Reasonably Ignore	
Description	Google's global domain name system (DNS) resolution service.	
Explanation	Public DNS services are used as alternatives to ISP's name servers. You may see devices on your network communicating with Google Public DNS over port 53/TCP ...	
Reference URL	https://developers.google.com/speed/public-dns/docs/isp#alternative	

GreyNoise IP Similarity Response:

GreyNoise Similarity Intel for 91.241.39.125

Showing first 50 IPs of 171 IPs that have a similarity score of 90% or above to 91.241.39.125

View IP Similarity UI on GreyNoise Visualizer

Similar IPs

25

1 - 25 of 50 items

IP	Score	Classification	Actor	Last Seen	Organization	Features Matched
61.0.91.131	100%	unknown	unknown	2023-02-07	National Internet Backbone	os, ports, useragents
105.214.4.69	100%	unknown	unknown	2023-02-25	MTN SA	os, ports, useragents
105.214.90.204	100%	unknown	unknown	2023-02-15	MTN SA	os, ports, useragents
190.43.252.1	100%	unknown	unknown	2023-01-26	Telefonica del Peru S.A.A.	os, ports, useragents
178.158.35.238	100%	unknown	unknown	2023-01-25	Dubrovskaya Nataliya Vladislavovna	os, ports, useragents
37.1.4.134	100%	unknown	unknown	2023-02-15	Rial Com JSC	os, ports, useragents
176.105.213.134	100%	malicious	unknown	2023-02-07	NPK Home-Net Ltd.	os, ports, useragents
185.129.240.20	100%	unknown	unknown	2022-12-19	Shabakieh Isfahan Co PJSC	os, ports, useragents
103.47.219.87	100%	unknown	unknown	2023-02-14	Fastnet Communication Pvt. Ltd.	os, ports, useragents
180.244.66.207	100%	unknown	unknown	2023-01-18	PT Telekomunikasi Indonesia	os, ports, useragents

GreyNoise IP Timeline View:

GreyNoise Timeline Details for 91.241.39.125

Showing Daily Summary of events for last 30 days. Only days with events will display.

[View IP Timeline Details on GreyNoise Visualizer](#)

IP Timeline

25

1 - 14 of 14 items

Date	Classification	Tags	rDNS	Organization	ASN	Ports	Web Paths	User Agents	
2023-03-11	malicious	Web Crawler, Telnet Brute...		Firma Informatyczna NSO...	AS199005	23/, 23/TCP, 80/TCP, 80/TC...	/	Mozilla/5.0 (Windows NT 1...	
2023-03-09	unknown	Web Crawler		Firma Informatyczna NSO...	AS199005	8080/TCP, 8080/TCP	/	Mozilla/5.0 (Windows NT 6...	
2023-03-05	unknown	Web Crawler		Firma Informatyczna NSO...	AS199005	8080/TCP, 8080/TCP	/	Mozilla/5.0 (Windows NT 1...	
2023-03-04	malicious	Web Crawler, Telnet Brute...		Firma Informatyczna NSO...	AS199005	23/, 23/TCP, 8080/TCP, 808...	/	Mozilla/5.0 (Windows NT 1...	
2023-03-01	malicious	Telnet Bruteforcer, Generi...		Firma Informatyczna NSO...	AS199005	23/, 23/TCP, 23/TCP			
2023-02-28	unknown	Web Crawler		Firma Informatyczna NSO...	AS199005	80/TCP, 8080/TCP, 80/TCP, ...	/	Mozilla/5.0 (Windows NT 6...	
2023-02-27	malicious	Telnet Bruteforcer, Mirai, ...		Firma Informatyczna NSO...	AS199005	23/, 23/TCP, 80/TCP, 8080/...	/	Mozilla/5.0 (Macintosh; Int...	
2023-02-26	malicious	Telnet Bruteforcer, Mirai, ...		Firma Informatyczna NSO...	AS199005	23/, 23/TCP, 23/TCP			
2023-02-24	malicious	Telnet Bruteforcer, Mirai, ...		Firma Informatyczna NSO...	AS199005	23/, 23/TCP, 23/TCP			
2023-02-22	malicious	Web Crawler, Telnet Brute...		Firma Informatyczna NSO...	AS199005	23/, 23/TCP, 80/TCP, 80/TC...	/	Mozilla/5.0 (Windows NT 1...	

IP Timeline

Classification

rDNS

ASN

Timeline

GreyNoise Community IP Response:

Enrichments

PASSIVE DNS (0)

WHOIS

ANOMALI_SAMPLEAPP

GREYNOISE

SUGGESTED ENRICHMENTS...

GreyNoise Community Info for 143.198.238.87

[View on GreyNoise Visualizer](#)

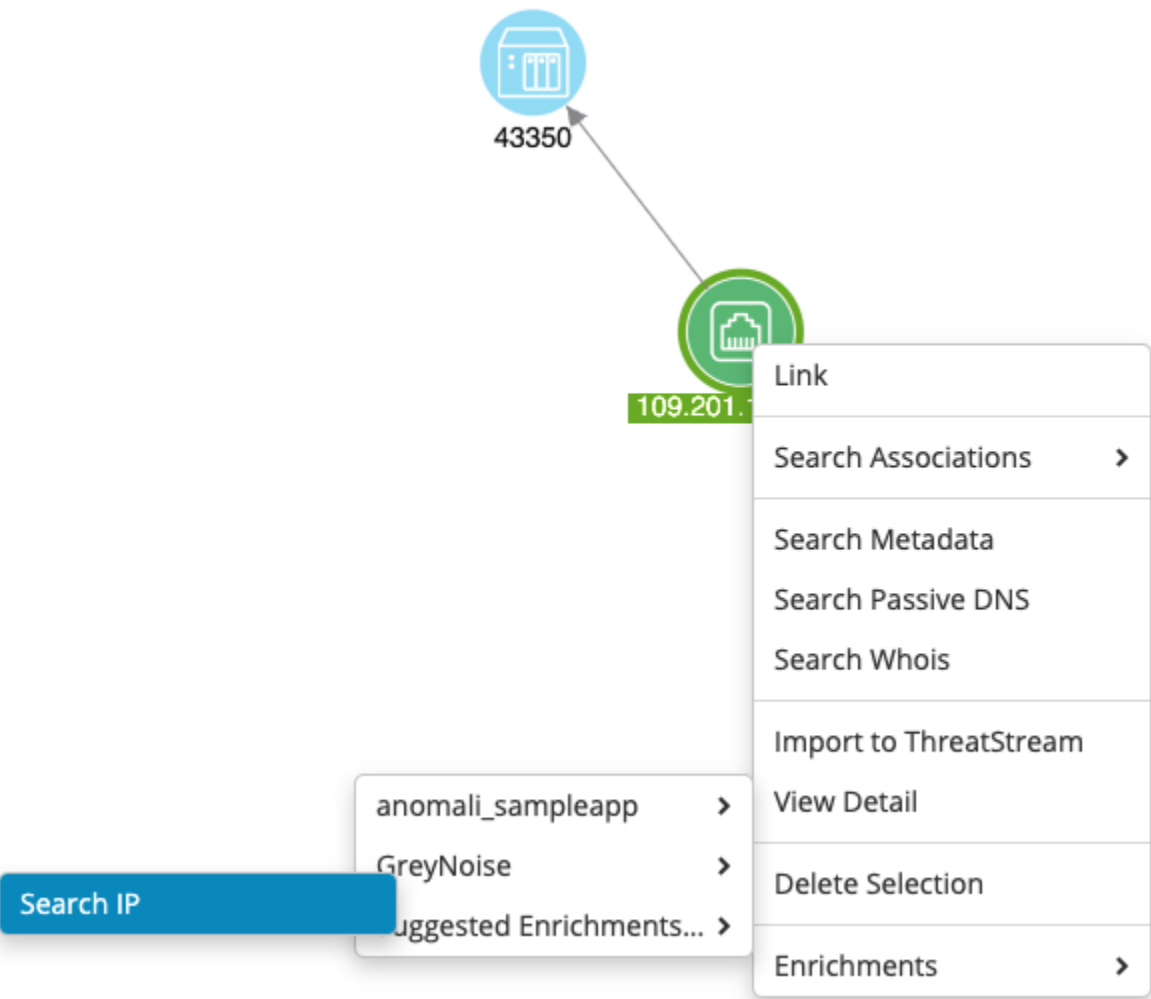
Details

25 ▾

1 - 5 of 5 items

Key	Value	⚙
Is Internet Background Noise	true	
Is Common Business Service	false	
Classification	<div>benign</div>	
Actor or Provider	Shodan.io	
Last Seen	2021-10-07	

Pivot-Enrichment:



GreyNoise Noise IP Response:

Internet Noise

type: Tag

GN Classification: malicious

type: Tag

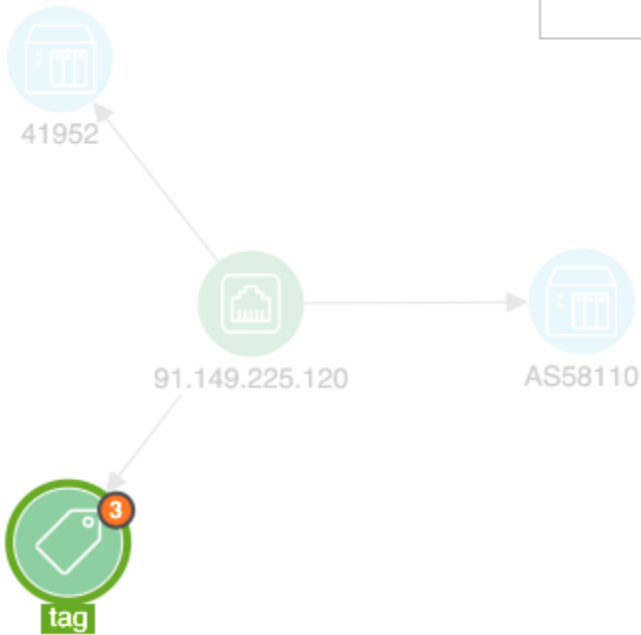
Known Tor Exit Node

type: Tag

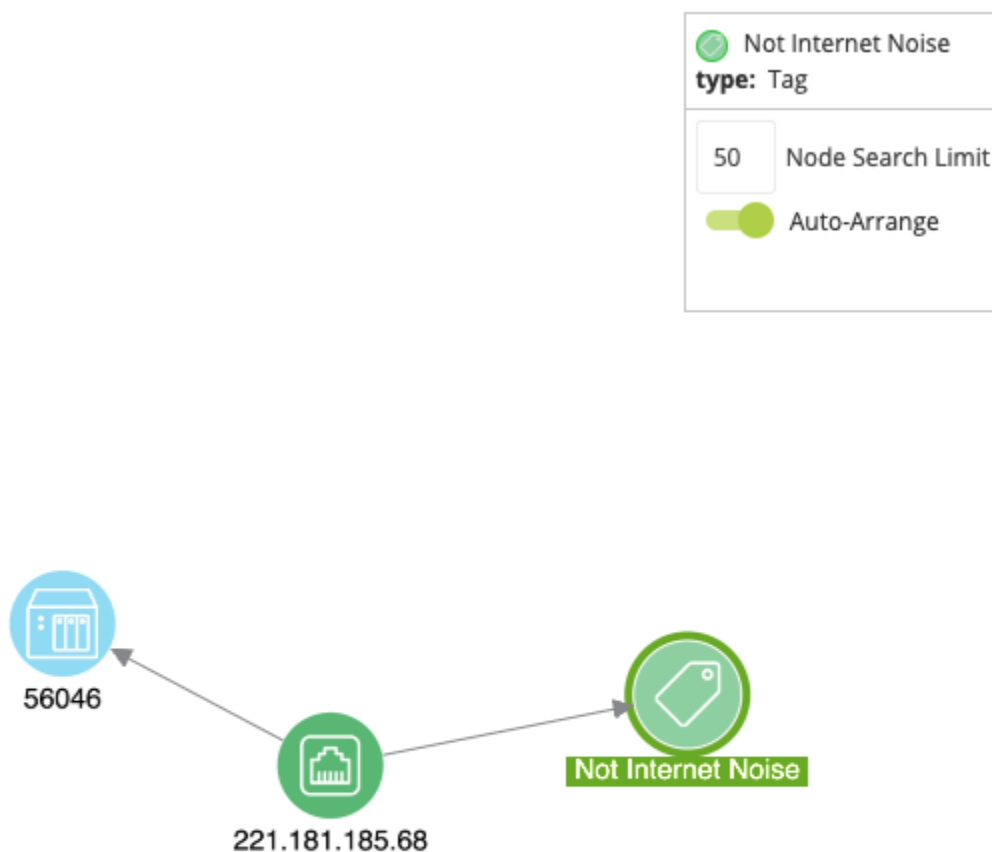
50

Node Search Limit

Auto-Arrange



GreyNoise Noise IP Response (Not Internet Noise):



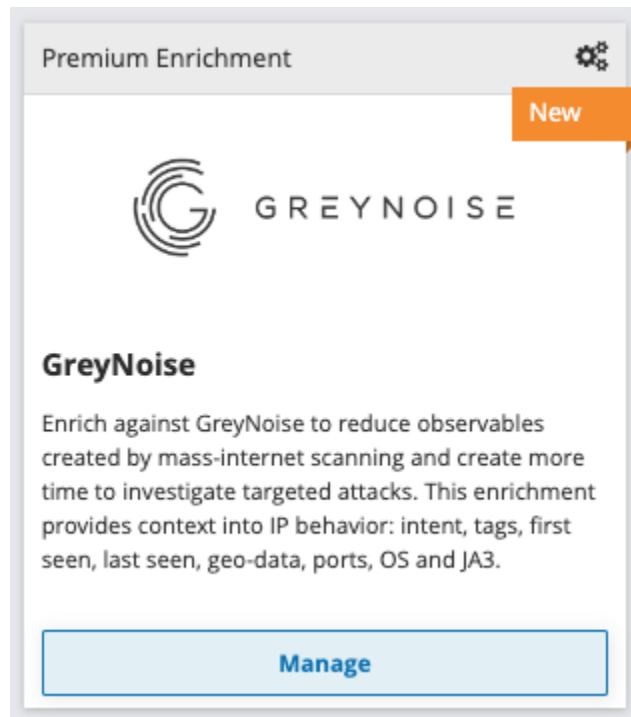
To read more about GreyNoise, see <https://greynoise.io>

The GreyNoise Enrichment enables the following commands:

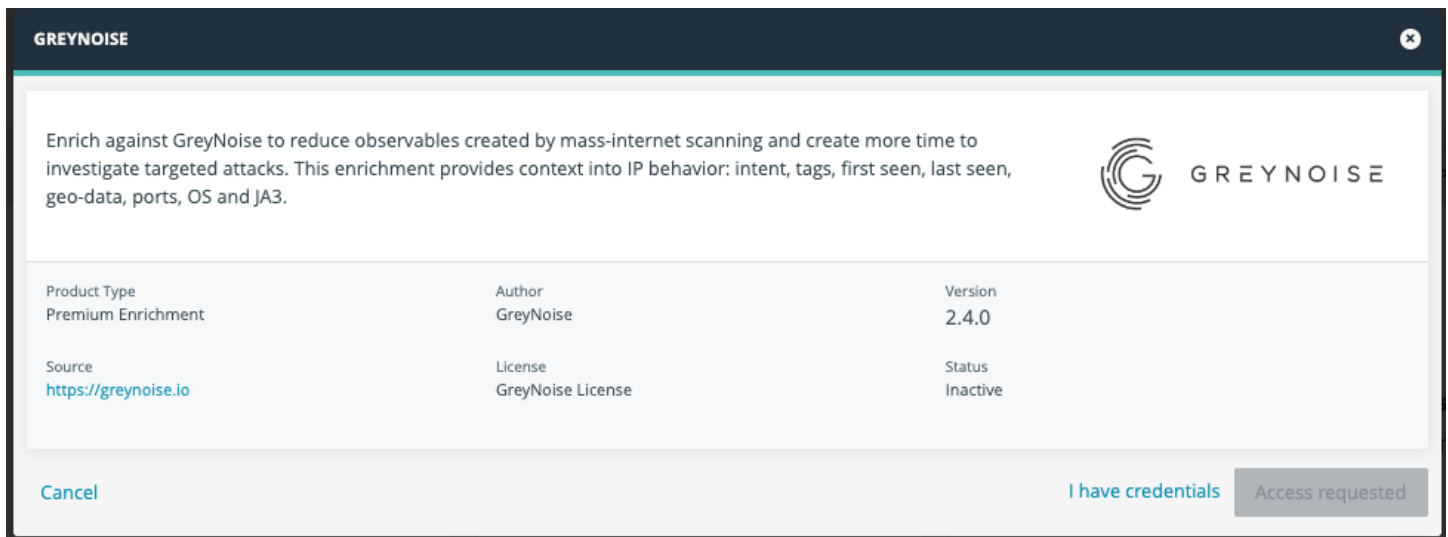
- Context Enrichment
 - enrichIP: returns IP context data from the GreyNoise Context and RIOT API
- Pivot Enrichment
 - Search IP: returns IP data points from the GreyNoise Context and RIOT API

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.

Product Type Premium Enrichment	Author GreyNoise	Version 2.4.0
Source https://greynoise.io	License GreyNoise License	Status Inactive

Credentials

API Key

API Type

Cancel

Activate

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 Similarity 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