

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. 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)WHOISGREYNOISESUGGESTED 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 (0)WHOISGREYNOISESUGGESTED ENRICHMENTS...

GreyNoise RIOT Info for 8.8.8.8

View on GreyNoise Visualizer

Details

25 ▾

1 - 7 of 7 items

Key	Value	⚙
Last Updated	2021-04-06T09:55:39Z	
Category	public_dns	
Name	Google Public DNS	
Classification	Benign Service	
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 Pu...	
Reference URL	https://developers.google.com/speed/public-dns/docs/isp#alternative	

GreyNoise Community IP Response:

Enrichments

PASSIVE DNS (0)WHOISANOMALI_SAMPLEAPPGREYNOISESUGGESTED ENRICHMENTS...

GreyNoise Community Info for 109.201.137.165

View on GreyNoise Visualizer

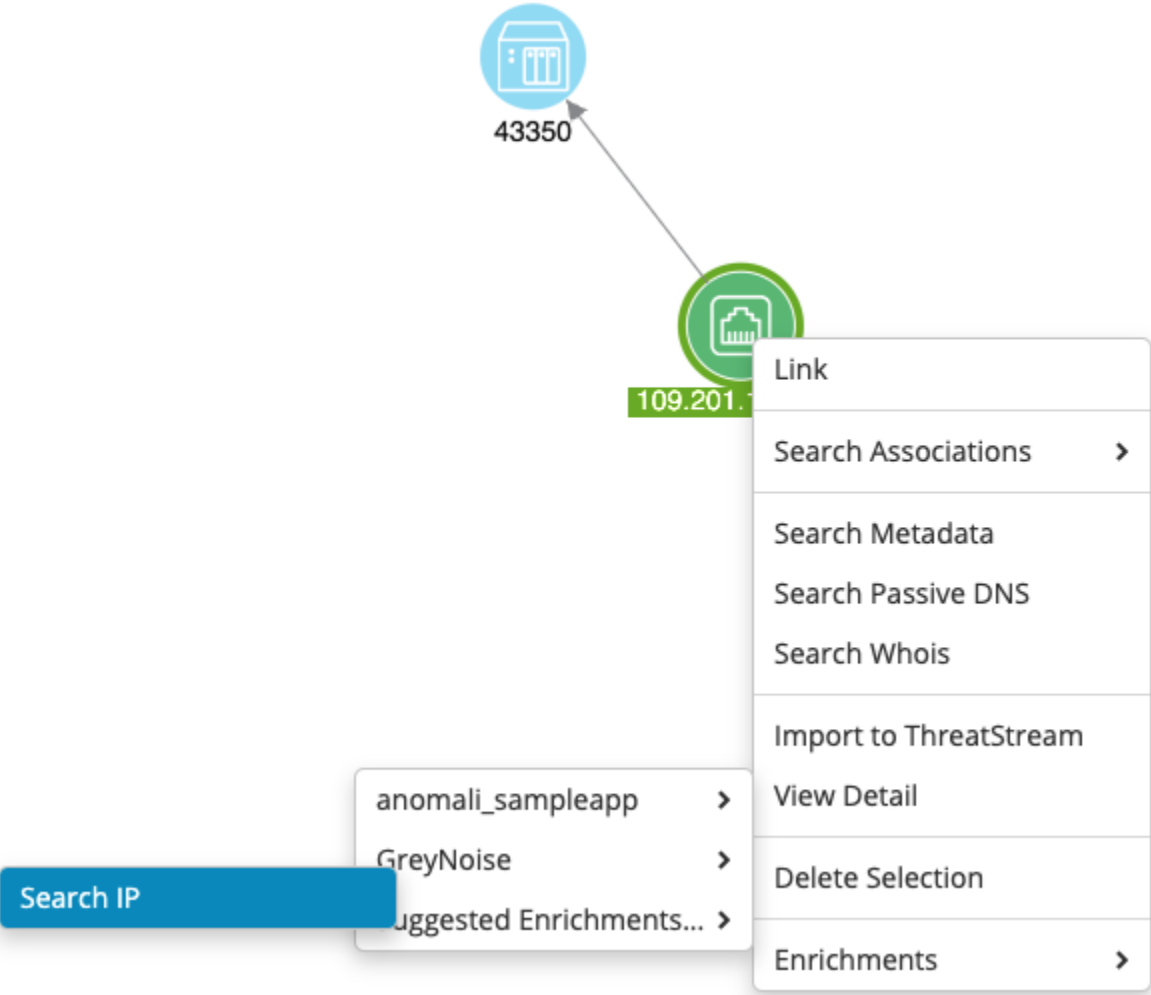
Details

25 ▾

1 - 5 of 5 items

Key	Value	⚙
Is Internet Background Noise	true	
Is Benign Service	false	
Classification	unknown	
Actor or Provider	unknown	
Last Seen	2021-05-17	

Pivot-Enrichment:



GreyNoise Noise IP Response:

Internet Noise

type: Tag

GN Classification: malicious

type: Tag

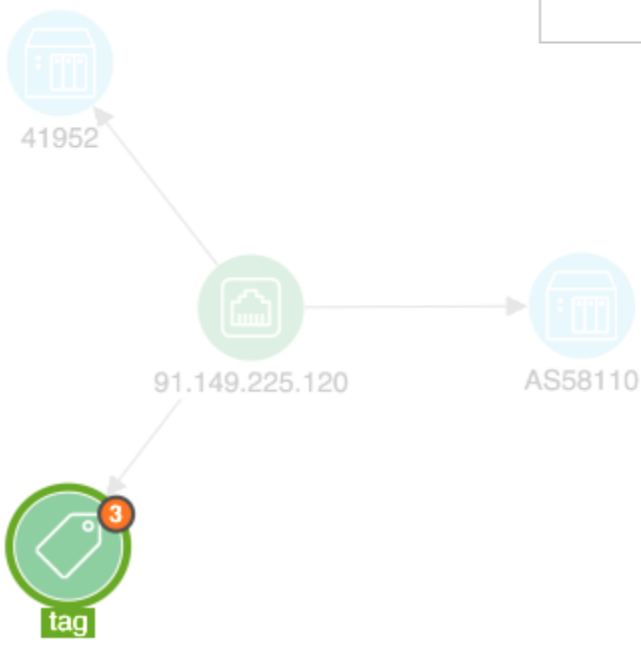
Known Tor Exit Node

type: Tag

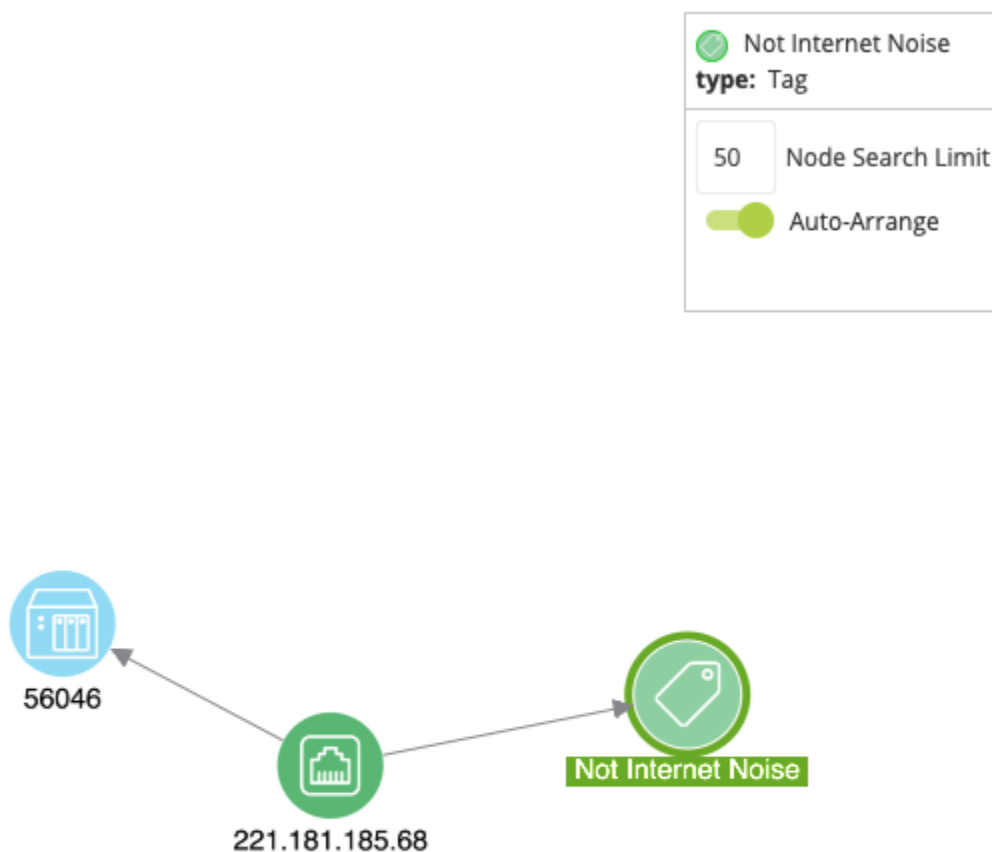
50

Node Search Limit

Auto-Arrange



GreyNoise Noise IP Response (Not Internet Noise):



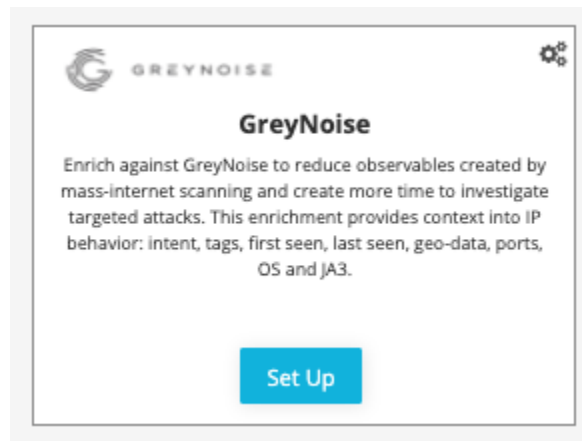
To read more about GreyNoise, see <https://greynoise.io>

The GreyNoise Enrichment enables the following commands:

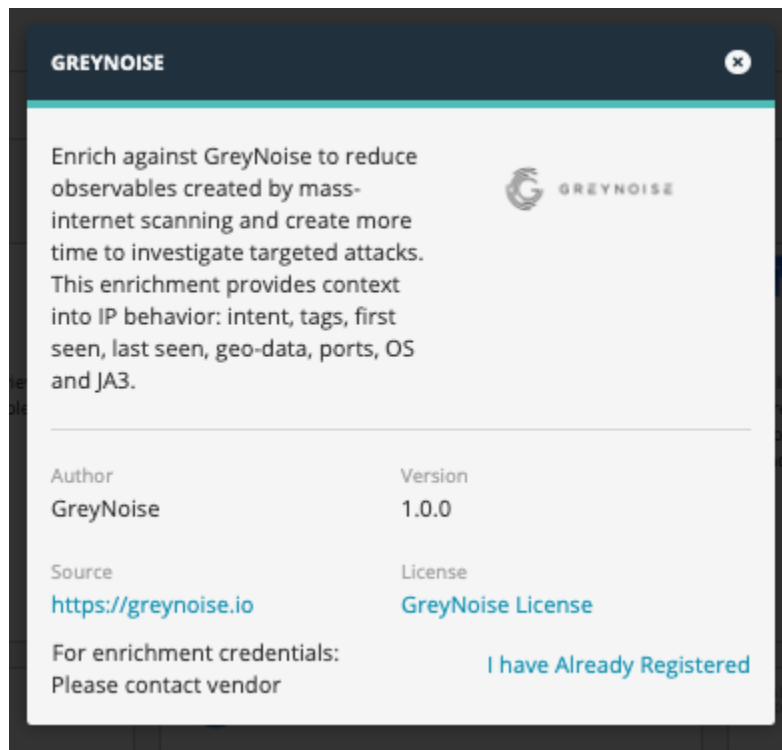
- Context Enrichment
 - enrichIP: returns IP context data from the GreyNoise Context and RIOT API
- Pivot Enrichment
 - Search IP: returns IP data points from the GreyNoise Context and RIOT API

To activate the GreyNoise enrichment:

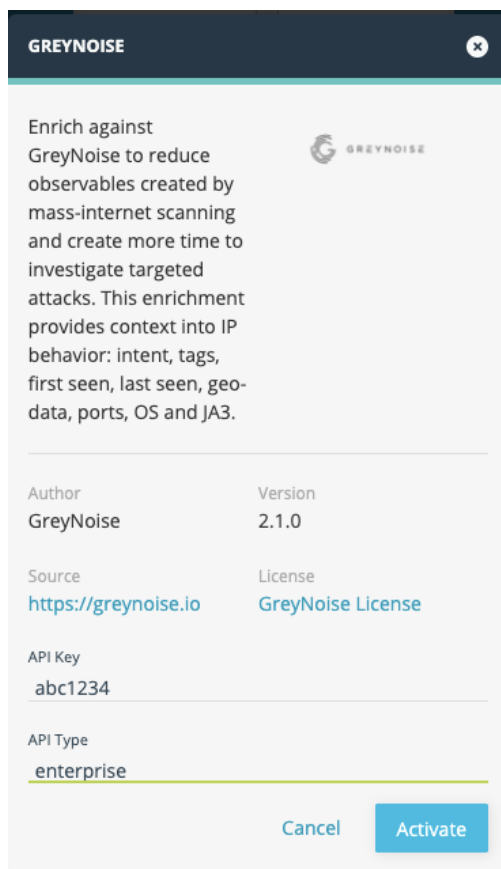
1. Log into the ThreatStream user interface
2. In the top navigation bar, click the settings icon, then click “Integrations”
3. Click “Set Up” in the GreyNoise Enrichment box



4. Click “I have already registered.”



5. Enter your GreyNoise API Key and select your API Type by entering either “enterprise” or “community” based on your API Key type



The screenshot shows a dialog box titled "GREYNOISE" with a close button (X) in the top right corner. The main text describes the enrichment service: "Enrich against GreyNoise to reduce observables created by mass-internet scanning and create more time to investigate targeted attacks. This enrichment provides context into IP behavior: intent, tags, first seen, last seen, geo-data, ports, OS and JA3." To the right of this text is the GreyNoise logo. Below the text is a table with the following information:

Author	Version
GreyNoise	2.1.0
Source	License
https://greynoise.io	GreyNoise License
API Key	
<input type="text" value="abc1234"/>	
API Type	
<input type="text" value="enterprise"/>	

At the bottom right of the dialog box are two buttons: "Cancel" and "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://developer.greynoise.io> or you can contact us at sales@greynoise.io to purchase an Enterprise Key.

Changelog:

v2.1.0

- Added support for Community API IP Lookups

UPGRADE NOTE: If you experience an issue upgrading to v2.1.0 of the integration, you may need to uninstall the previous version and perform a fresh install of v2.1.0+

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 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