GreyNoise Enrichment for Anomali ThreatStream

The GreyNoise Enrichment for Anomali ThreatStream enhances observables to help identify activity related to widespread internet scanning or harmless services, freeing up time to investigate other, more critical observables. Additionally, the Vulnerability Enrichment provides context on CVEs along with additional data points on levels of observed In-The-Wild exploitation.

The enrichment supports both the paid and free GreyNoise users. For free users, only the IP enrichment tab will return data and will be rate-limited according to the free user limits.

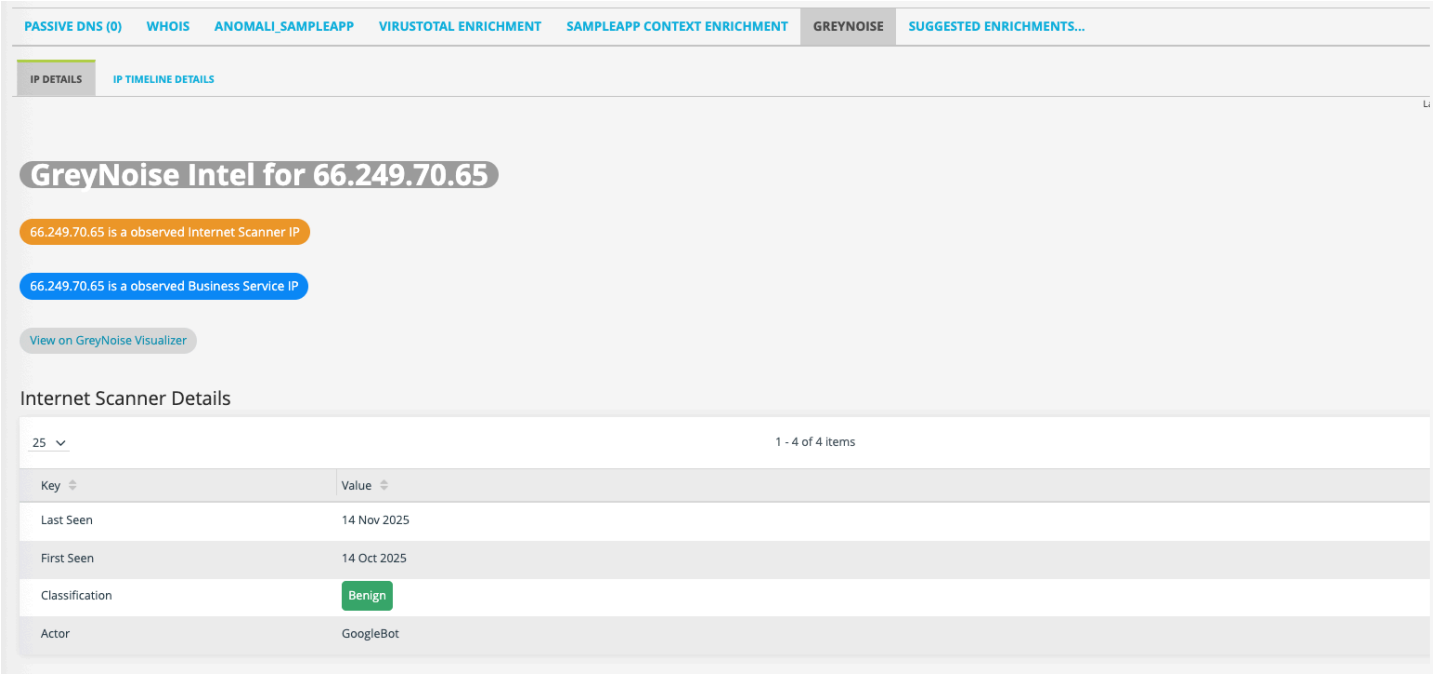
The IP enrichment provides the following information for IP address observables: intent, tags, first seen, last seen, geo-data, ports, OS, and JA3. It also identifies IP addresses associated with benign services, VPN services, and TOR exit nodes. Paid users will also have access to the IP Timeline functionality, which provides a daily overview of scanning activity.

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

The Vulnerability enrichment provides details about a CVE, including vendor and product information, as well as additional data on CVSS scores and exploitation statistics. Observed indicators in GreyNoise are also noted and can be linked back to ThreatStream if used alongside the GreyNoise Feed capability.

Context Enrichment:

GreyNoise IP Response:



Business Service Details

25 1 - 7 of 7 items

Key	Value
Name	Google APIs and Services
Category	software
Trust Level	1 - Reasonably Ignore
Last Updated	14 Nov 2025
Description	Google LLC is an American multinational technology company that specializes in Internet-related services and products, which include online advertising technologies, a search engine, cloud computing
Explanation	Trusted commercial software commonly used by individuals and businesses for collaboration, content creation, entertainment, or various other functions. You may see devices communicating with Goo
Reference URL	https://google.com/

Metadata

25 1 - 13 of 13 items

Key	Value
ASN	AS15169
Source City	Moncks Corner
Source Country	United States
Source Country Code	US
Destination Countries	United States, Spain, India, France, Singapore, Australia, Germany, Brazil, Canada, United Kingdom, Finland, Indonesia, Iceland, Japan, South Korea, Malaysia, Netherlands, Norway
Destination Country Codes	US, ES, IN, FR, SG, AU, DE, BR, CA, GB, FI, ID, IS, JP, KR, MY, NL, NO, PH
Region	South Carolina
Latitude	33.1963
Longitude	-80.0143
Sensor Hits	1240
Sensor Count	78
Organization	Google LLC
Category	hosting

Additional

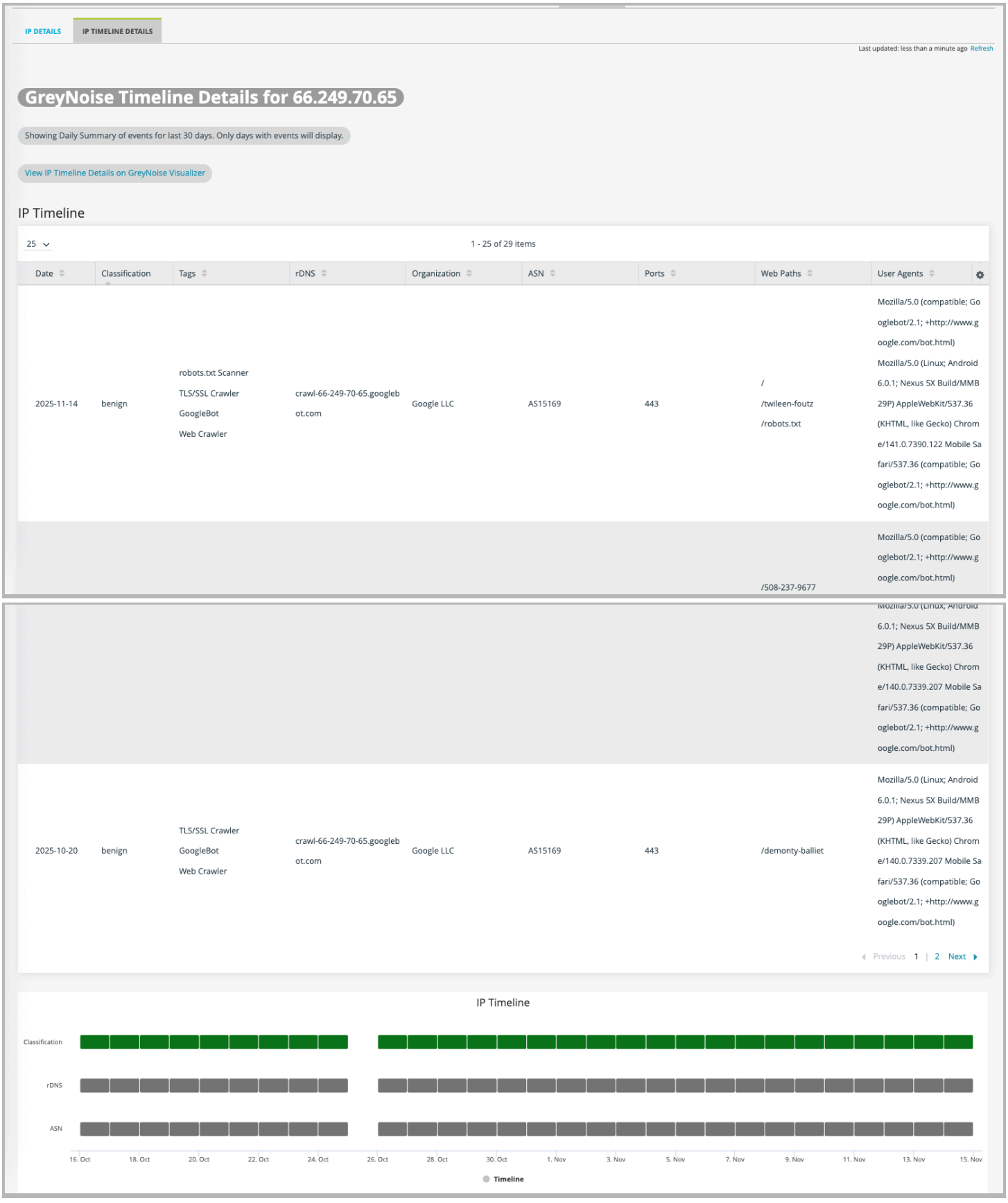
25 1 - 12 of 12 items

Key	Value
Known Tor Exit Node	False
Spoofable	False
rDNS	crawl-66-249-70-65.googlebot.com
VPN	False
Port(s) / Protocol(s)	80/tcp 443/tcp
Tag(s)	Favicon Scanner GoogleBot TLS/SSL Crawler Web Crawler ads.txt Scanner robots.txt Scanner
CVE(s)	None

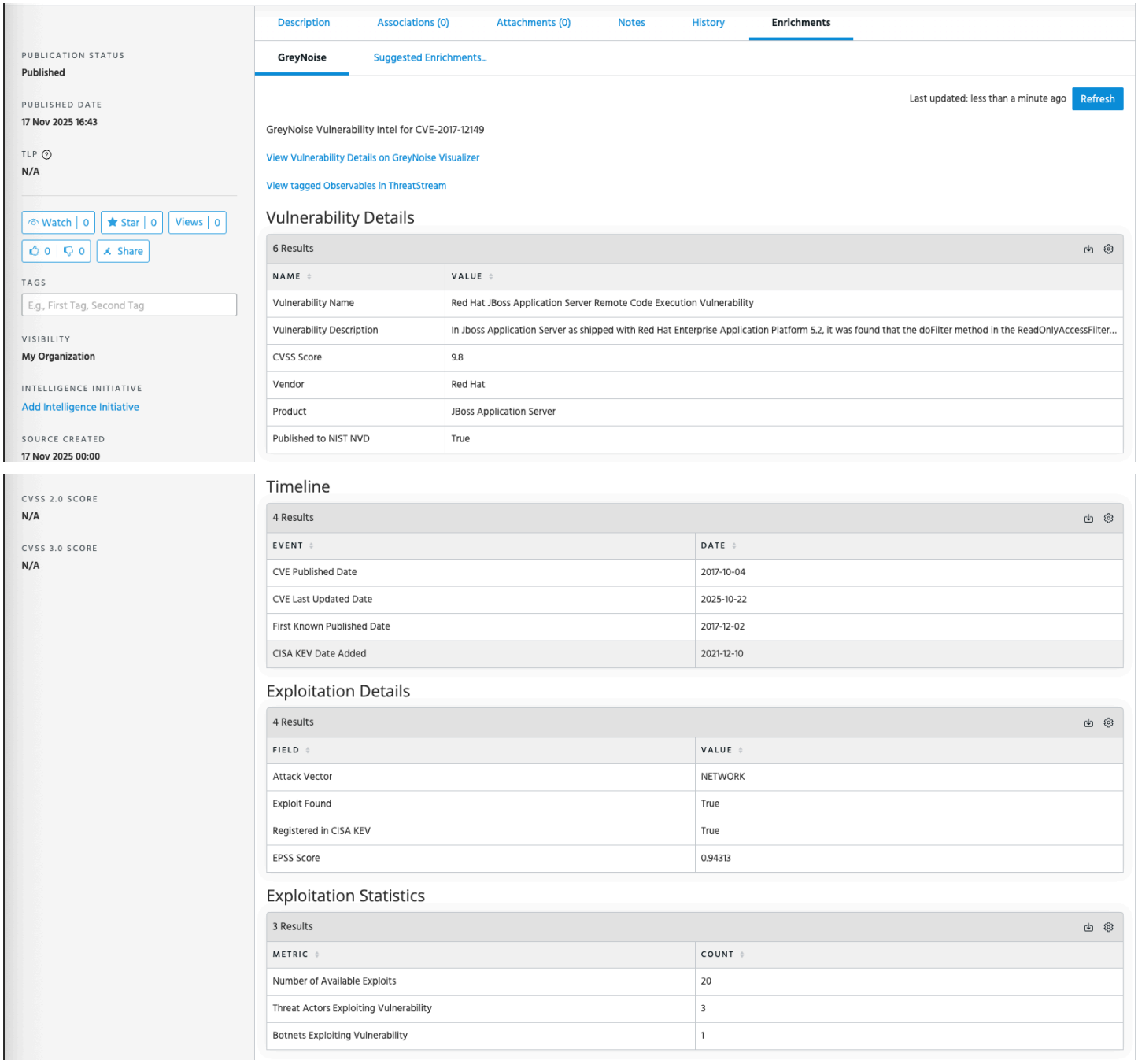
	robots.txt Scanner
CVE(s)	None
UserAgent String(s)	Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.7390.122 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com. Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.7339.207 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com. Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.7390.107 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com. Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.7390.107 Mobile Safari/537.36 (compatible; GoogleOther) Googlebot-Image/1.0
Path(s)	/8728-golders-green-mews /robots.txt /ndyalfp / /ads.txt /601-239-4255 /1709-buena-vista-circle-southeast /the-hourly-cost-to-connect-those /641-333-4805 /11483-salter-colvin-road Output limited to 10 of 37 items, see Visualizer for more details.
JA4(s)	t13d181300_e8a523a41297_43ade6aba3df t13i181200_e8a523a41297_43ade6aba3df
JA3(s) (fingerprint/port)	b4da7f95e46bf2cf5285fd609cf726e4 / 443 68d5c2bb987eb6e447614cea53c1c843 / 443
HASSH(s) (fingerprint/port)	None

Associations

GreyNoise IP Timeline View:



Vulnerability Enrichment:



Exploitation Activity - IPs Observed

3 Results

TIME PERIOD	BENIGN IPS	THREAT IPS
Last 1 Day	0	91
Last 10 Days	0	108
Last 30 Days	0	132

Time Period

This Vulnerability does not have any comments yet.

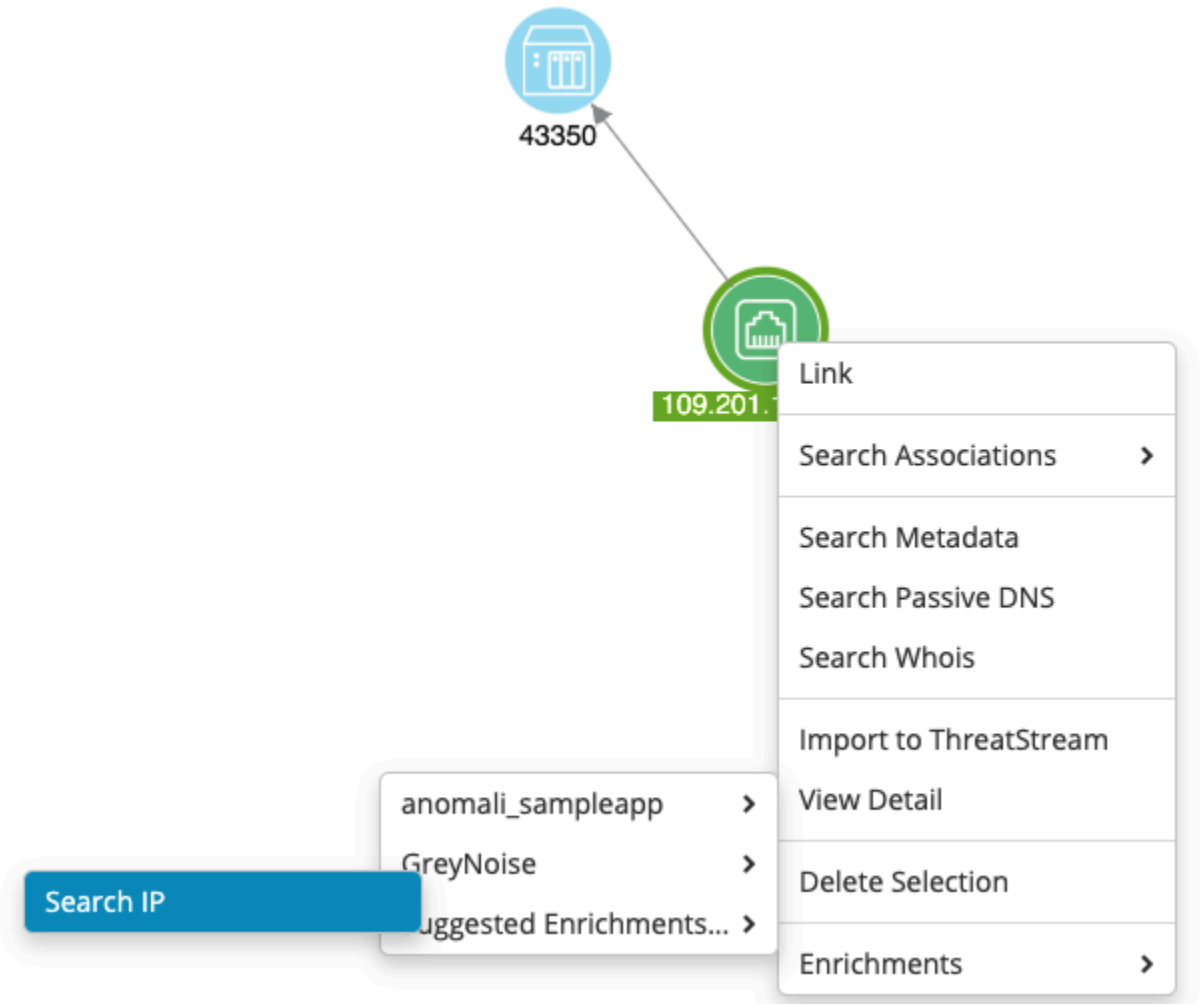
Add a comment

Private

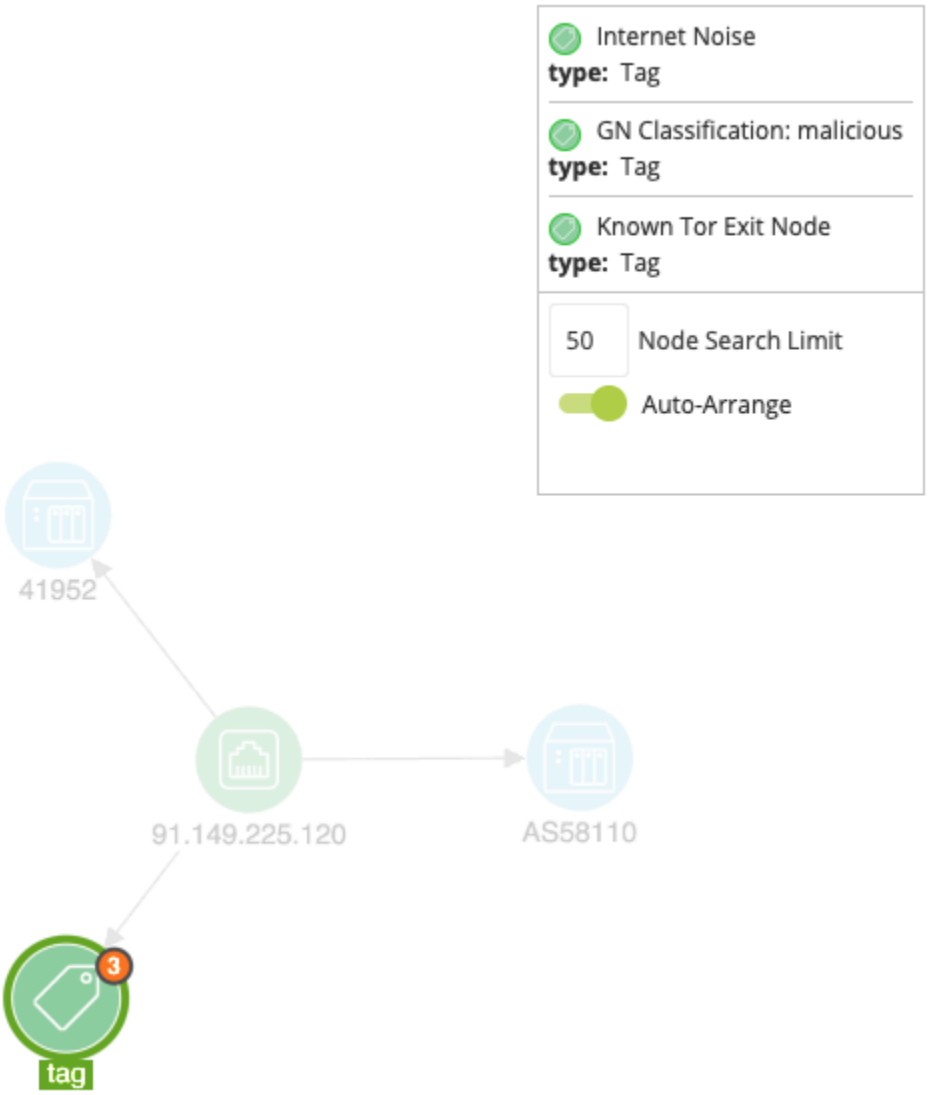
Open Sans 15

Type something

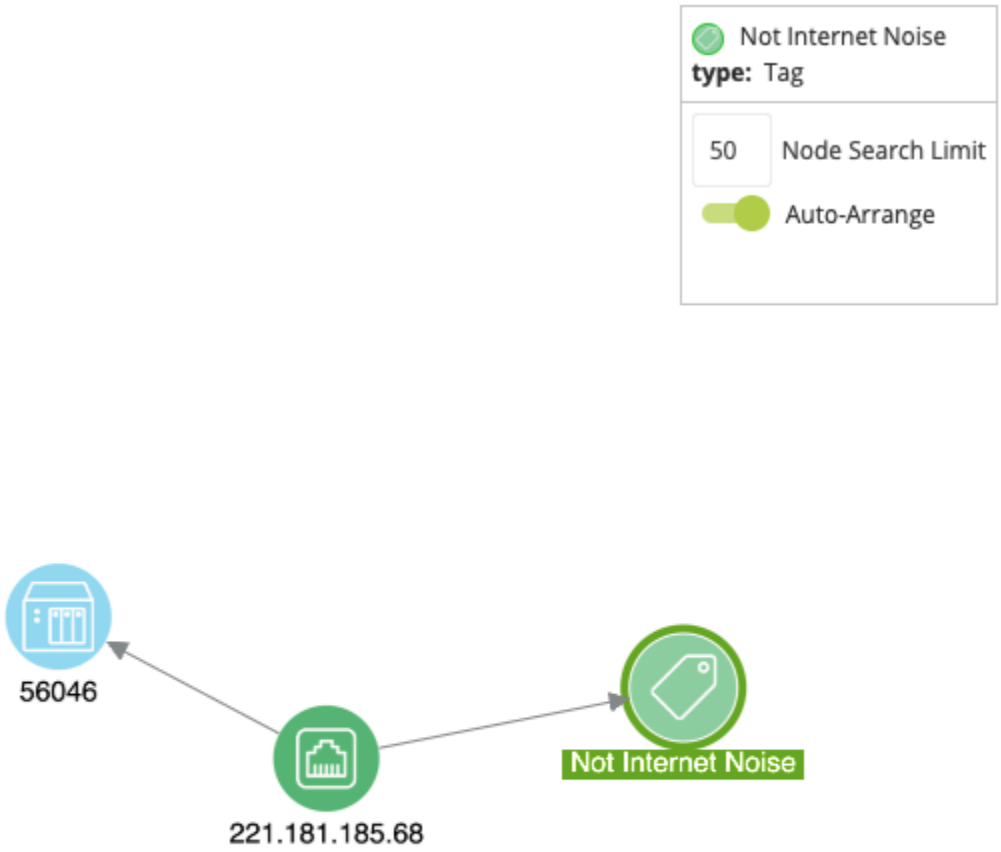
Pivot-Enrichment:



GreyNoise Noise IP Response:



GreyNoise Noise IP Response (Not Internet Noise):



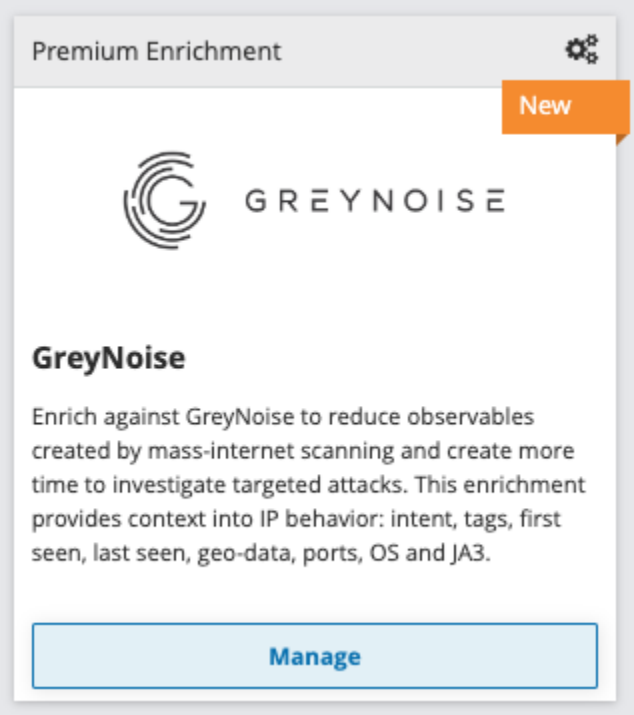
To read more about GreyNoise, see https://greynoise.io

The GreyNoise Enrichment enables the following commands:

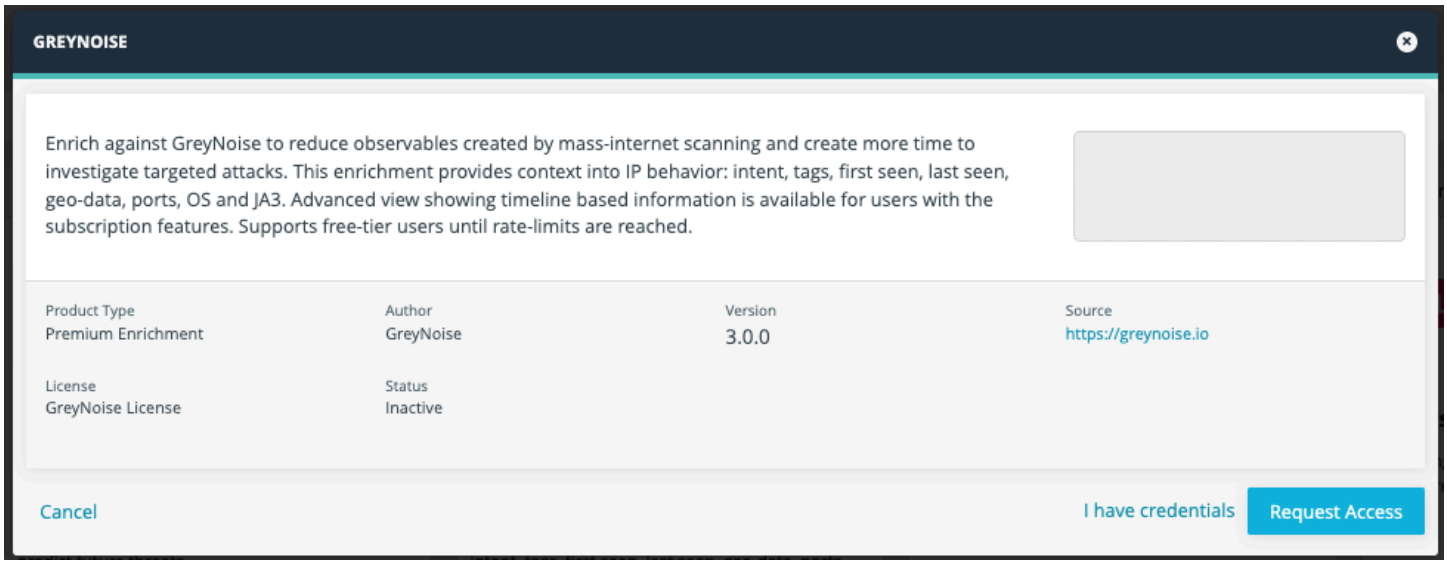
- Context Enrichment
  - enrichIP: returns IP context data from the GreyNoise IP Lookup API
  - enrichIPTimeline: returns a daily summary of internet scanning from the GreyNoise Timeline API
  - enrichVulnerablity: returns CVE context data from the GreyNoise CVE Lookup API
- Pivot Enrichment
  - Search IP: returns IP data points from the GreyNoise IP Lookup API

To activate the GreyNoise enrichment:

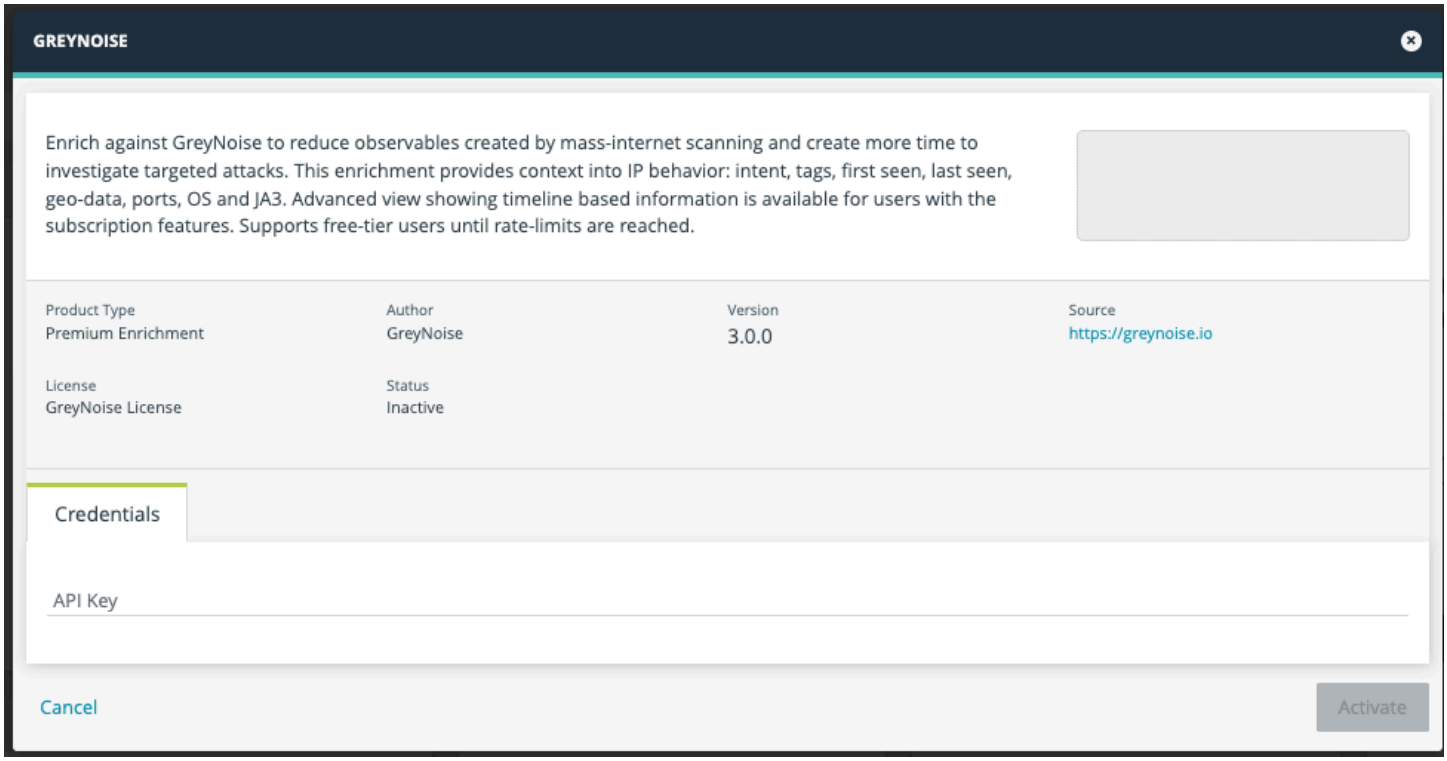
1. Log in to the ThreatStream user interface
2. In the top navigation bar, navigate to the App Store and search for GreyNoise
3. Click “Manage/Get Access” in the GreyNoise Enrichment box



4. Click “I have credentials.”



5. Enter your GreyNoise API Key.



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://viz.greynoise.io/signup, or you can contact us at sales@greynoise.io to purchase an Enterprise Key.

Changelog:

v3.0.0

- Added enrichVulnerability context lookup
- Update to use GreyNoise v3 Endpoints, adds additional fields and information
- Corrected issues with the IP Timeline Tab not displaying data due to API changes
- Remove the IP Similarity Tab due to the deprecation of the feature
- Code clean-up and documentation

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