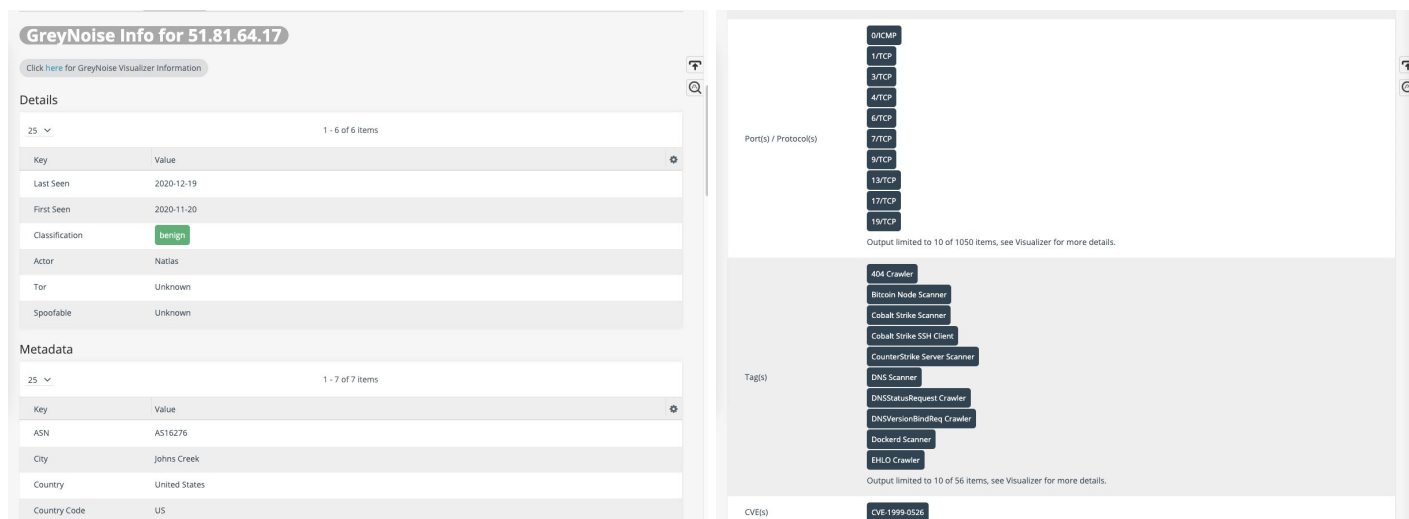


GreyNoise Enrichment Plugin for Anomali ThreatStream

The GreyNoise Enrichment plugin for Anomali ThreatStream enriches observables to identify activity associated with mass-internet scanning, creating more time to investigate other higher priority observables. This enrichment provides context into IP behavior: intent, tags, first seen, last seen, geo-data, ports, OS and JA3.

This is a Context Enrichment that displays enrichment data on the observable details pages.



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

The GreyNoise Enrichment plugin enables the following data transformations:

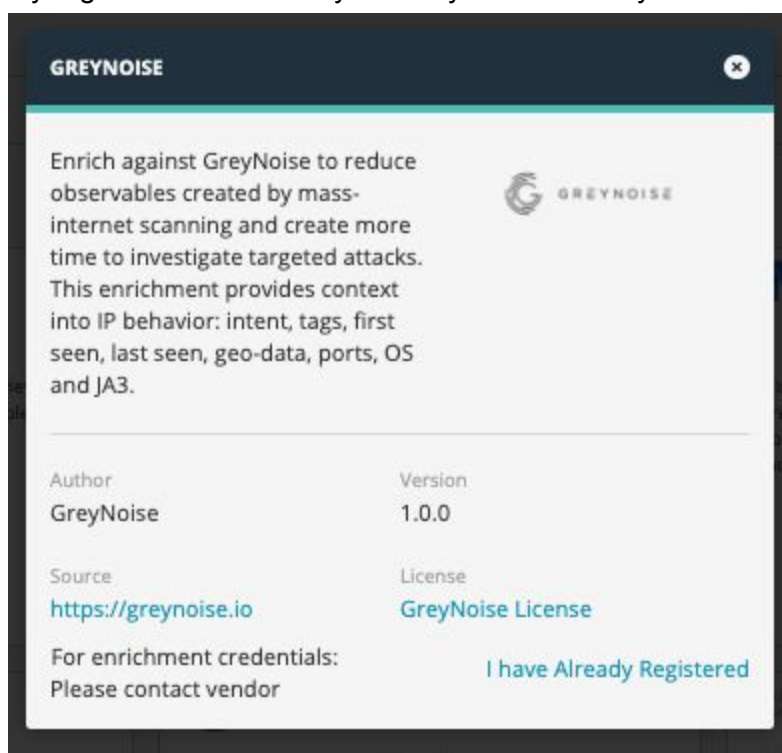
- enrichIP: returns IP context data from the GreyNoise Context API

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” and enter your GreyNoise API Key.



5. 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:

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