ReversingLabs Spectra Intelligence for Anomali ThreatStream

Configuration and usage guide

Author: Mislav Sever

Proprietary and Confidential

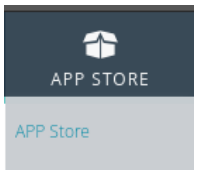
Table of Contents

Introduction

The ReversingLabs Spectra Intelligence enrichment app for Anomali ThreatStream is a set of pivot and context-based enrichment functions that can be used to enrich threat hunting and analysis by introducing new and unique insights into the security workflow.

It returns data transformations and enrichment visualizations from ReversingLabs Spectra Intelligence, the industry's most comprehensive source of reputation data, into Anomali ThreatStream workflows.

Activating the app



To activate the enrichment pack, click on the App Store in the ThreatStream top navigation bar and find the ReversingLabs Spectra Intelligence app. After you do that, configure the app using your Spectra Intelligence account credentials. In case you do not have an active account, contact the ReversingLabs sales department

Note: Spectra Intelligence accounts used for authenticating ReversingLabs Enrichments require the following Spectra Intelligence account roles:

- TCA-0101 File Reputation
- TCA-0103 Historic Multi-AV Scan Records
- TCA-0104 File Analysis - Hash
- TCA-0301 RHA1 Functional Similarity
- TCA-0321 RHA1 Analytics
- TCA-0401 URI to Hash Search
- TCA-0407 Network Reputation
- TCA-0403 URL Threat Intelligence
- TCA-0405 Domain Threat Intelligence
- TCA-0406 IP Threat Intelligence

After registering and receiving the Spectra Intelligence account credentials, select the "I have credentials" option and enter the following information:

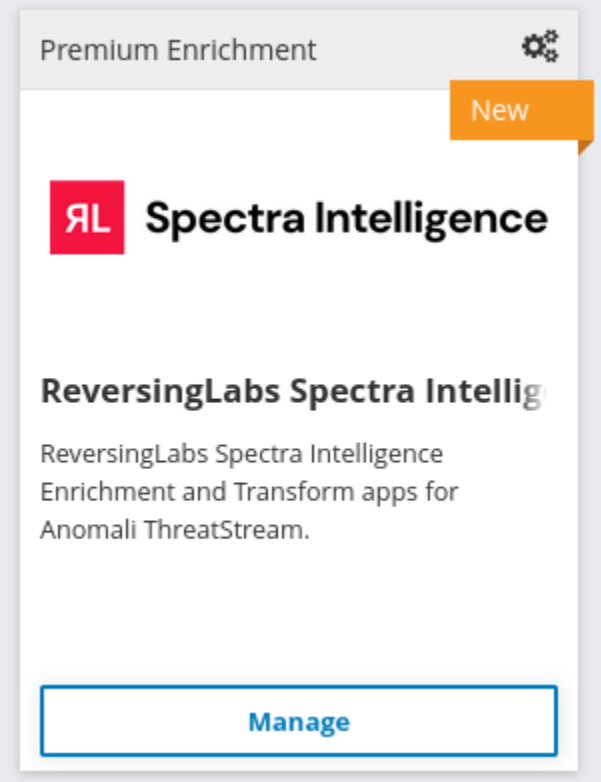
- Spectra Intelligence username - the username for the ReversingLabs Spectra Intelligence web services provided by ReversingLabs.

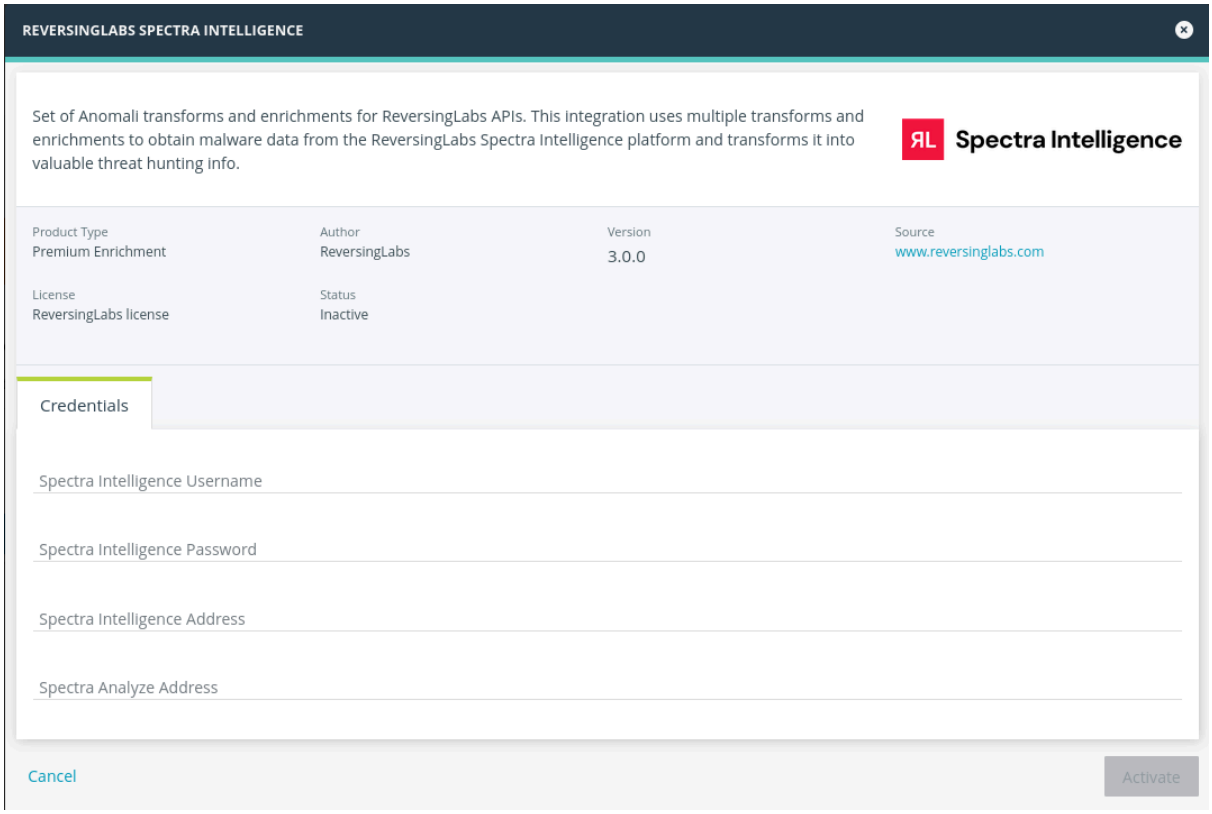
- Spectra Intelligence password - the password for the ReversingLabs Spectra Intelligence web services provided by ReversingLabs.

- Spectra Intelligence address (optional) - the base address of the ReveringLabs Spectra Intelligence (can be entered with or without the “https://” protocol prefix). If left blank, it will use the default value. Use the default address unless instructed otherwise.

- Spectra Analyze address (optional) - the base address of the designated ReversingLabs Spectra Analyze instance, if available. This optional parameter must be entered with the “http://” or “https://” protocol prefix.

After clicking the Activate button, a confirmation message will appear in the upper right corner. The configuration is now complete.




REVERSINGLABS SPECTRA INTELLIGENCE
Set of Anomali transforms and enrichments for ReversingLabs APIs. This integration uses multiple transforms and enrichments to obtain malware data from the ReversingLabs Spectra Intelligence platform and transforms it into valuable threat hunting info.
Spectra Intelligence
Product Type
Premium Enrichment
Author
ReversingLabs
Version
3.0.0
Source
www.reversinglabs.com
License
ReversingLabs license
Status
Inactive
Credentials
Spectra Intelligence Username
Spectra Intelligence Password
Spectra Intelligence Address
Spectra Analyze Address
Cancel
Activate

Supported Observable Types

Pivot-Based Enrichments

ReversingLabs pivot-based enrichments for Anomali ThreatStream support the following observable types, grouped by the transform function:

File Reputation
- SHA-1 hash
- SHA-256 hash
- MD5 hash

Latest AV Detections
- SHA-1 hash
- SHA-256 hash
- MD5 hash

Functionally Similar File Hashes
- SHA-1 hash

Domain to Hash Index
- Domain

IPv4 to Hash Index
- IPv4 address

Email Address to Hash Index
- Email address

URL to Hash Index
- URL

Files Downloaded From a URL
- URL

Files Downloaded From a Domain
- Domain

URLs Found on a Domain
- Domain

Domains Related to a Domain
- Domain

Files Downloaded From an IP Address

- IPv4 Address

URLs Downloaded From an IP Address

- IPv4 Address

IP to Domain Resolutions

- IPv4 Address

The following transforms return only results classified as malicious or suspicious:

- File Reputation
- Functionally Similar File Hashes
- Domain to Hash Index
- IPv4 to Hash Index
- Email Address to Hash Index
- URL to Hash Index

If an unsupported hash type is used as a hash observable, the transform function will not perform a transformation, and an appropriate exception message will be returned. Check the Additional debugging section for more information.

Context-Based Enrichments

ReversingLabs context-based enrichments for Anomali ThreatStream support the following observable types:

- SHA-1 hash
- SHA-256 hash
- MD5 hash
- Domain
- IPv4 address
- URL

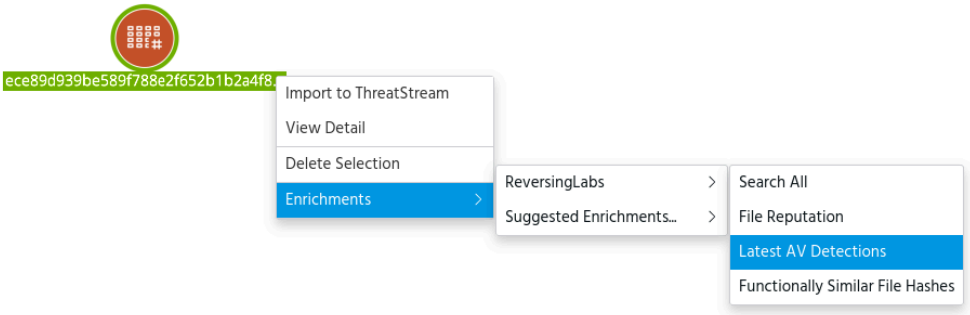
Unlike some pivot-based enrichments, context-based enrichments are not filtered to show only results classified as malicious or suspicious.

Usage

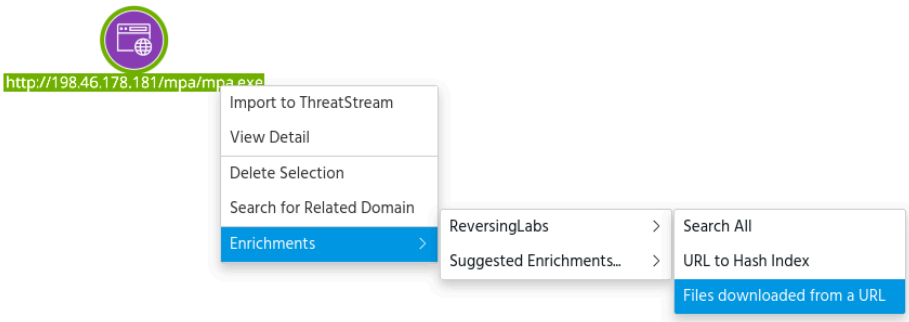
Pivot-Based Enrichments

Pivot-based enrichments are used to dynamically trigger actions over various types of observables. Each type of observable displays only actions that were made for its specific type.

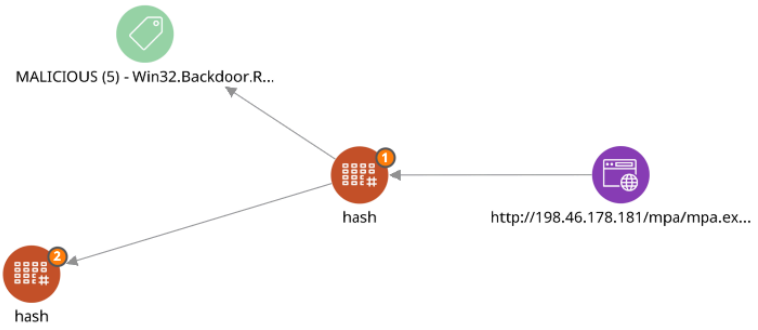
Example 1:
Trigger Latest AV Detections on a SHA-1 hash. The result will consist of multiple tags carrying malware names given to this sample by various AV scanners used in ReversingLabs cloud services.



Example 2:
Trigger Files downloaded from a URL on a URL observable.



Next step - trigger File Reputation on the resulting hash.



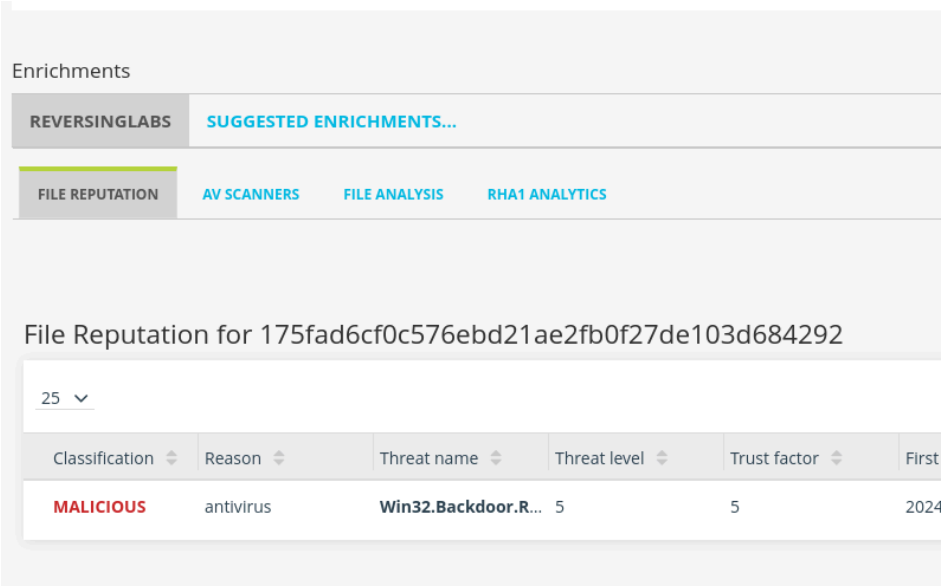
This scenario tells us that the sample found on the URL is malicious and has a name and a risk score in ReversingLabs.
Additional steps can include triggering Functionally Similar File hashes to fetch all similar hashes that are classified as malicious or suspicious.

Context-Based Enrichments

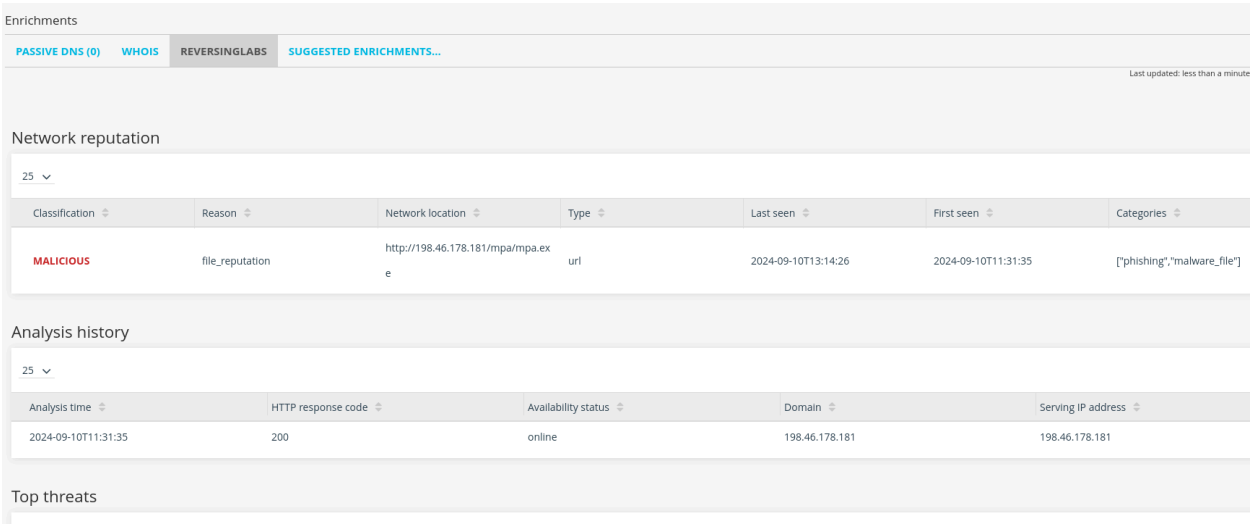
Context-based enrichments are displayed automatically when starting an observable investigation.
In the observable details page, click on the “REVERSINGLABS” tab to display them.

Depending on the observable type and the availability of threat intelligence for the given observable in the ReversingLabs Spectra Intelligence, different enrichment tabs will be shown additionally.

File hash:



URL:



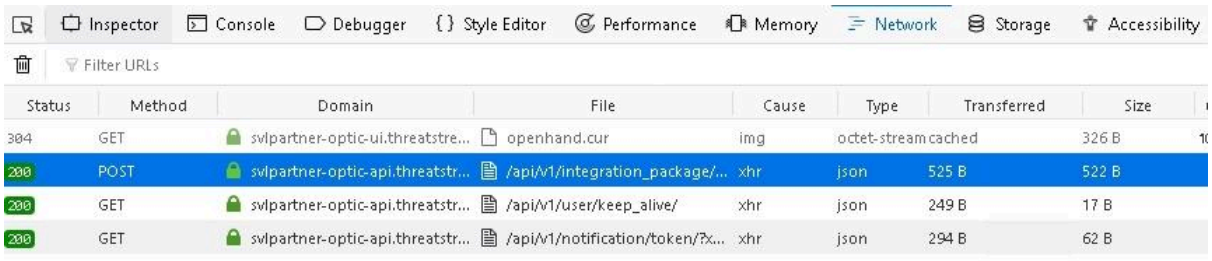
All context-based enrichments display static data formatted into multiple tables.

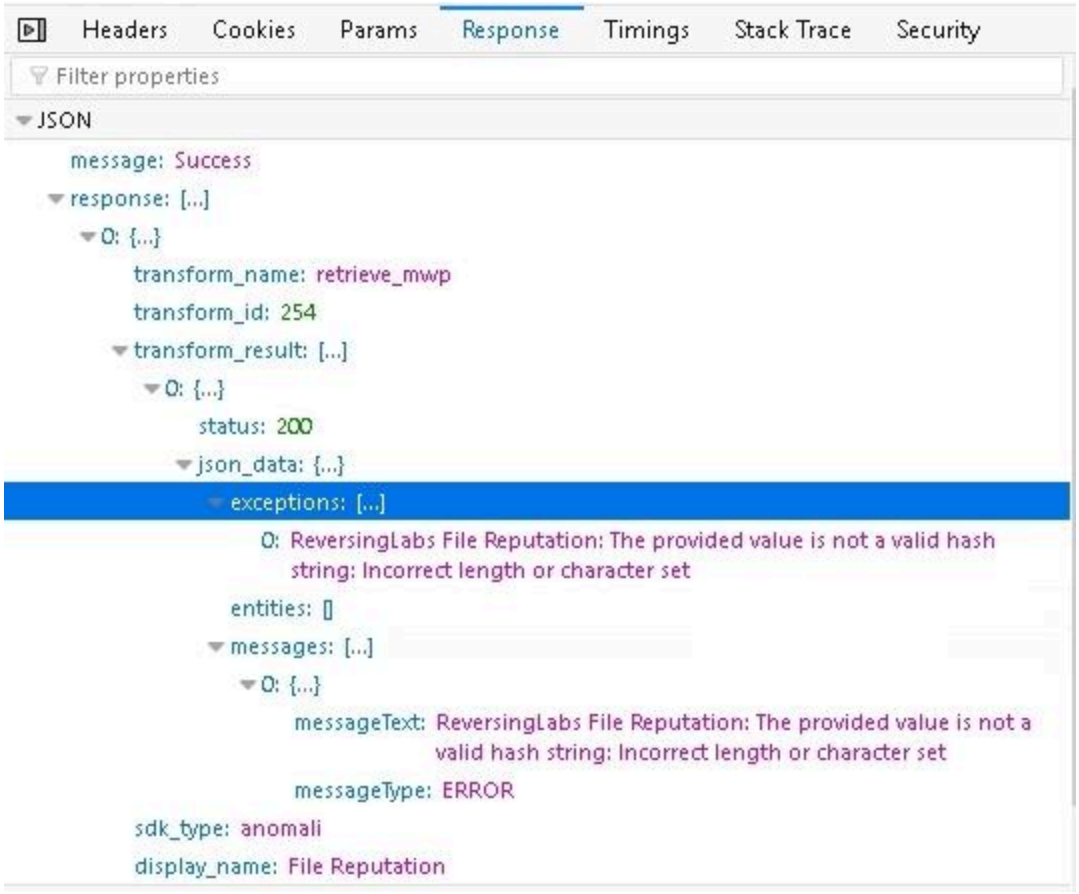
Additional Debugging

To find additional and descriptive error messages for unsuccessful actions, open the web browser's development tools by pressing F12 on the keyboard.

Navigate to the Network tab and view the Response section.

After performing an enrichment action, check the logged POST request JSON response and look for the "exceptions" and "messages" objects to see what went wrong in more detail.





ReversingLabs Contacts and Links

To request the credentials for the ReversingLabs web services and any other product information, contact your ReversingLabs account manager or the sales department.

Useful links	
Contact form	https://www.reversinglabs.com/contact-us
Other ReversingLabs integrations	https://www.reversinglabs.com/integrations
Spectra Intelligence	https://www.reversinglabs.com/products/spectra-intelligence

Version History

Date	Version	Author	Comment
2019-02-28	1.0.0	Mislav Sever	Created the initial version
2019-11-22	2.0.2	Mislav Sever	Version 2.0.2 update
2020-05-26	2.0.2	Kristijan Puljek	Proofreading and editing
2021-02-08	2.0.3	Mislav Sever	Version 2.0.3 update
2021-08-10	2.0.4	Mislav Sever	Version 2.0.4 update The integration was ported to Python 3
2024-09-09	3.0.0	Mislav Sever	App renamed to ReversingLabs Spectra Intelligence. App version updated to 3.0.0