ReversingLabs Spectra Analyze for Anomali ThreatStream

Configuration and usage guide

Author: Mislav Sever

Proprietary and Confidential

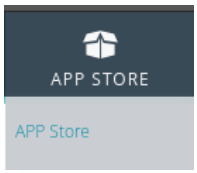
Table of Contents

Introduction

The ReversingLabs Spectra Analyze 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 Analyze, a powerful and versatile threat analysis platform, into Anomali ThreatStream.

Activating the app

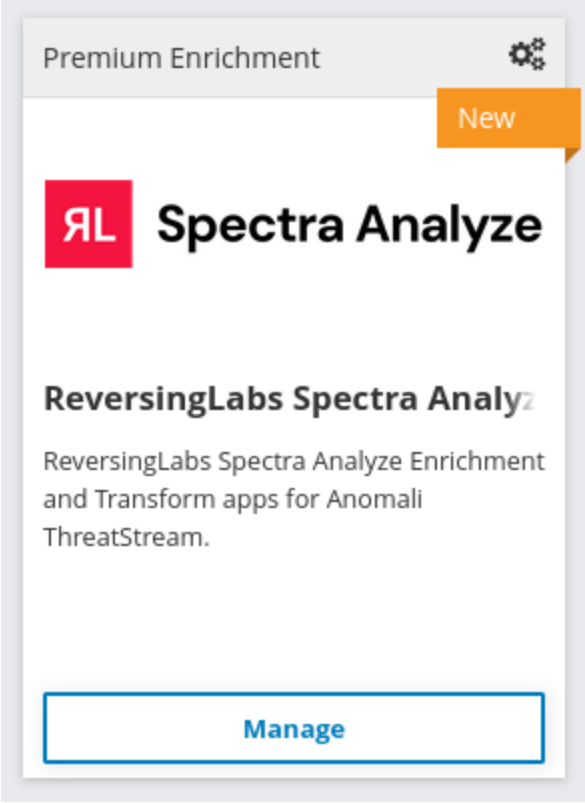


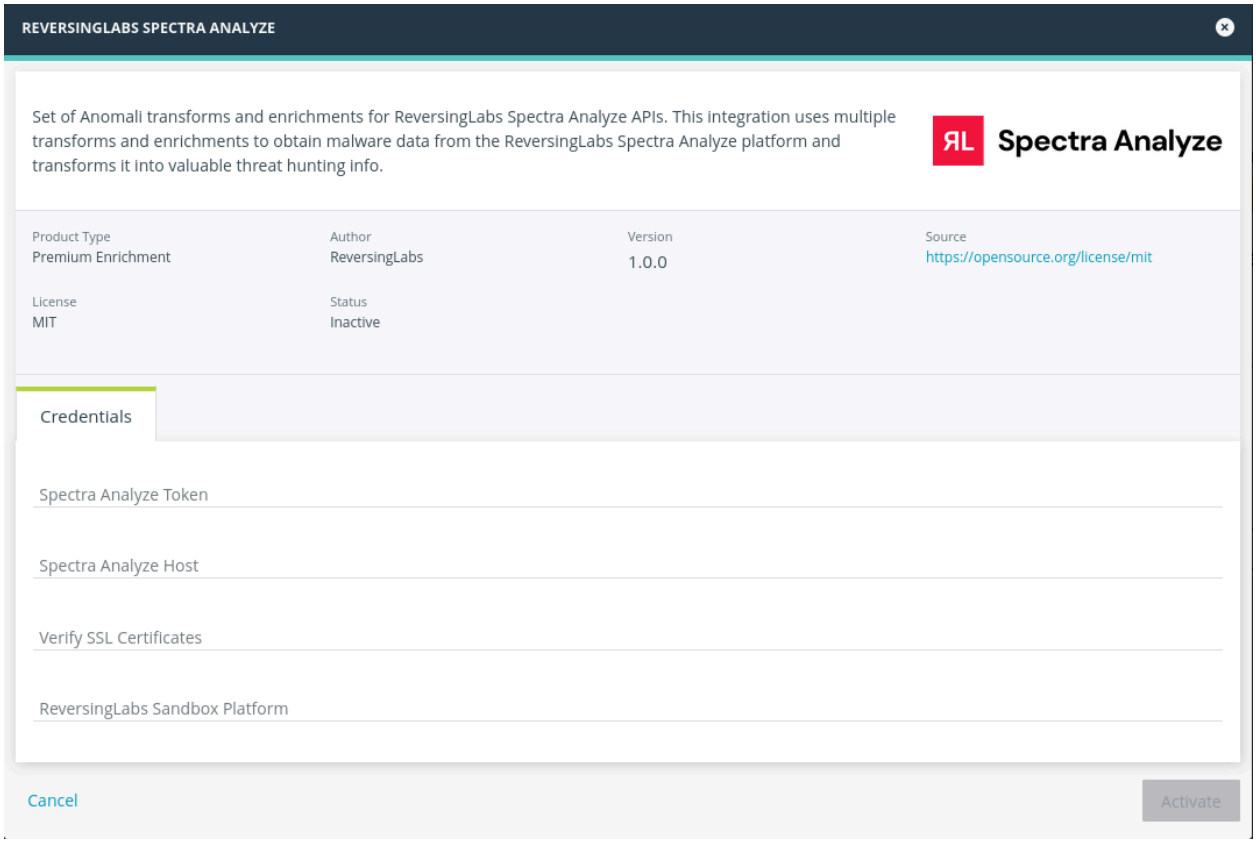
To activate the enrichment pack, click on the App Store in the ThreatStream top navigation bar and find the ReversingLabs Spectra Analyze app. After you do that, configure the app using your Spectra Analyze account credentials. For this app to work, you need an active instance of Spectra Analyze reachable from the Anomali cloud. In case you do not have such an instance, contact ReversingLabs using the links provided in the **ReversingLabs Contacts and Links** section.

After making sure that you have a Spectra Analyze instance with an active user account, select the “I have credentials” option and enter the following information:

- Spectra Analyze token - A token for using your Spectra Analyze instance’s API.
- Spectra Analyze host - The host of your Spectra Analyze instance.
- Verify SSL certificates - Set to “false” in case your Spectra Analyze instance does not have a valid SSL certificate.
- ReversingLabs sandbox platform - Set the desired sandbox platform that will be used in actions which utilize dynamic analysis. See the Spectra Analyze documentation for available options.

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


Premium Enrichment
New
Spectra Analyze
ReversingLabs Spectra Analyz
ReversingLabs Spectra Analyze Enrichment and Transform apps for Anomali ThreatStream.
Manage


REVERSINGLABS SPECTRA ANALYZE
Set of Anomali transforms and enrichments for ReversingLabs Spectra Analyze APIs. This integration uses multiple transforms and enrichments to obtain malware data from the ReversingLabs Spectra Analyze platform and transforms it into valuable threat hunting info.
Spectra Analyze
Product Type
Premium Enrichment
Author
ReversingLabs
Version
1.0.0
Source
https://opensource.org/license/mit
License
MIT
Status
Inactive
Credentials
Spectra Analyze Token
Spectra Analyze Host
Verify SSL Certificates
ReversingLabs Sandbox Platform
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:

Submit URL
- URL

List extracted files
- SHA-1 hash
- SHA-256 hash
- MD5 hash

Reanalyze a sample
- SHA-1 hash
- SHA-256 hash
- MD5 hash

Files found on IP address
- IPv4 address

IP to domain resolutions
- IPv4 address

URLs hosted on IP address
- IPv4 address

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

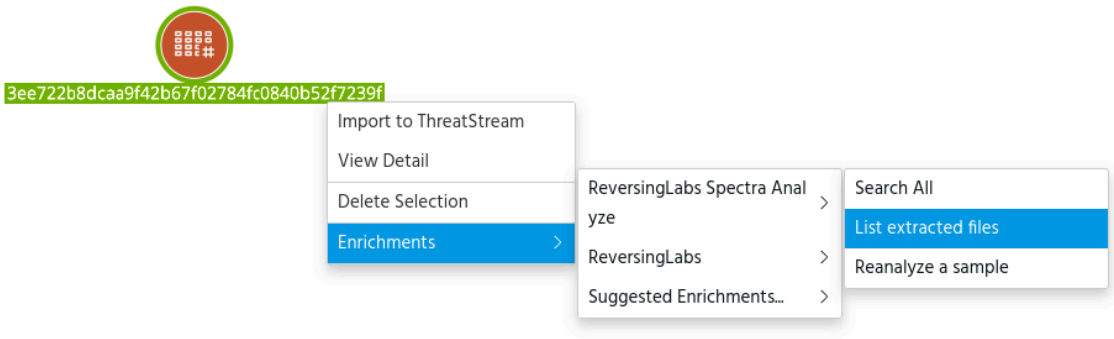
- Domain
- IPv4 address
- URL

Usage

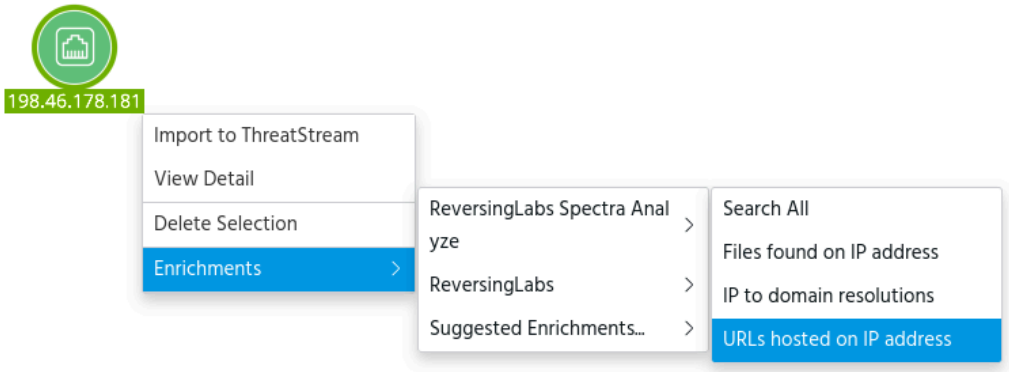
Pivot-Based Enrichments

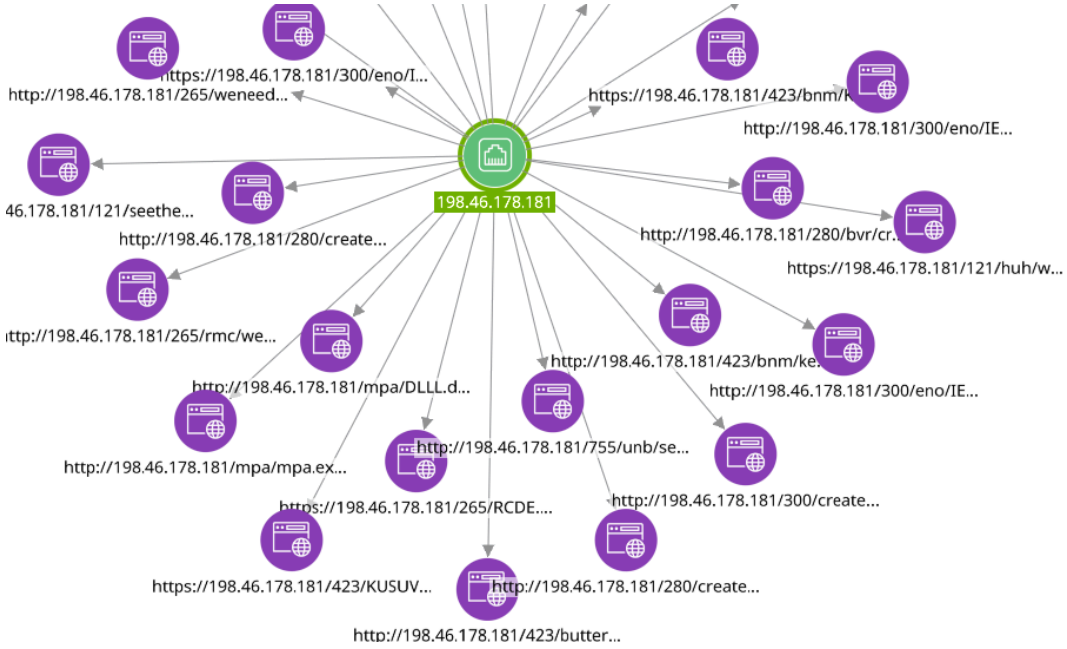
Pivot-based enrichments are used to dynamically trigger actions over various types of observables. Each type of observable displays only actions that were made for its specific type.

Example 1:
Trigger **List extracted files** on a SHA-1 hash. The result will consist of multiple hash observables.



Example 2:
Trigger **URLs hosted on IP address** on an IPv4 observable. The result will be multiple URL observables.



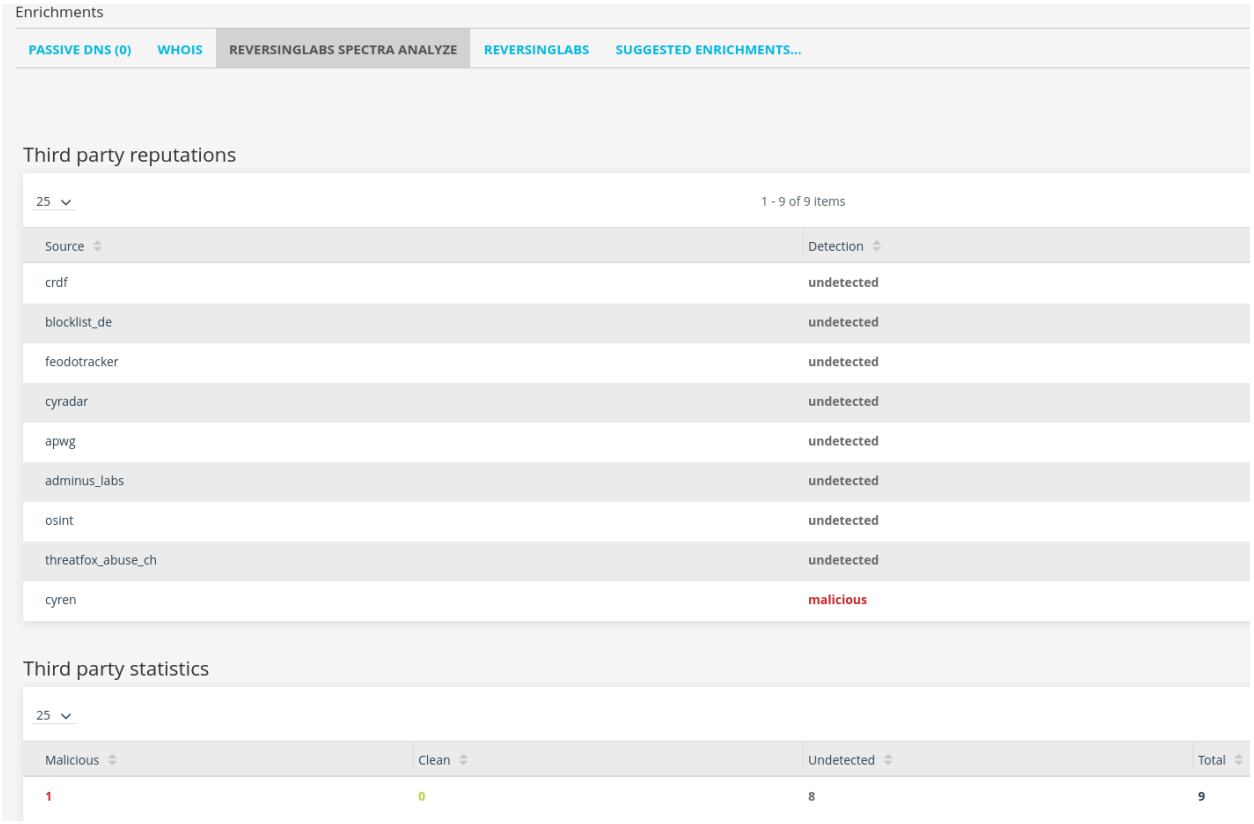


Context-Based Enrichments

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

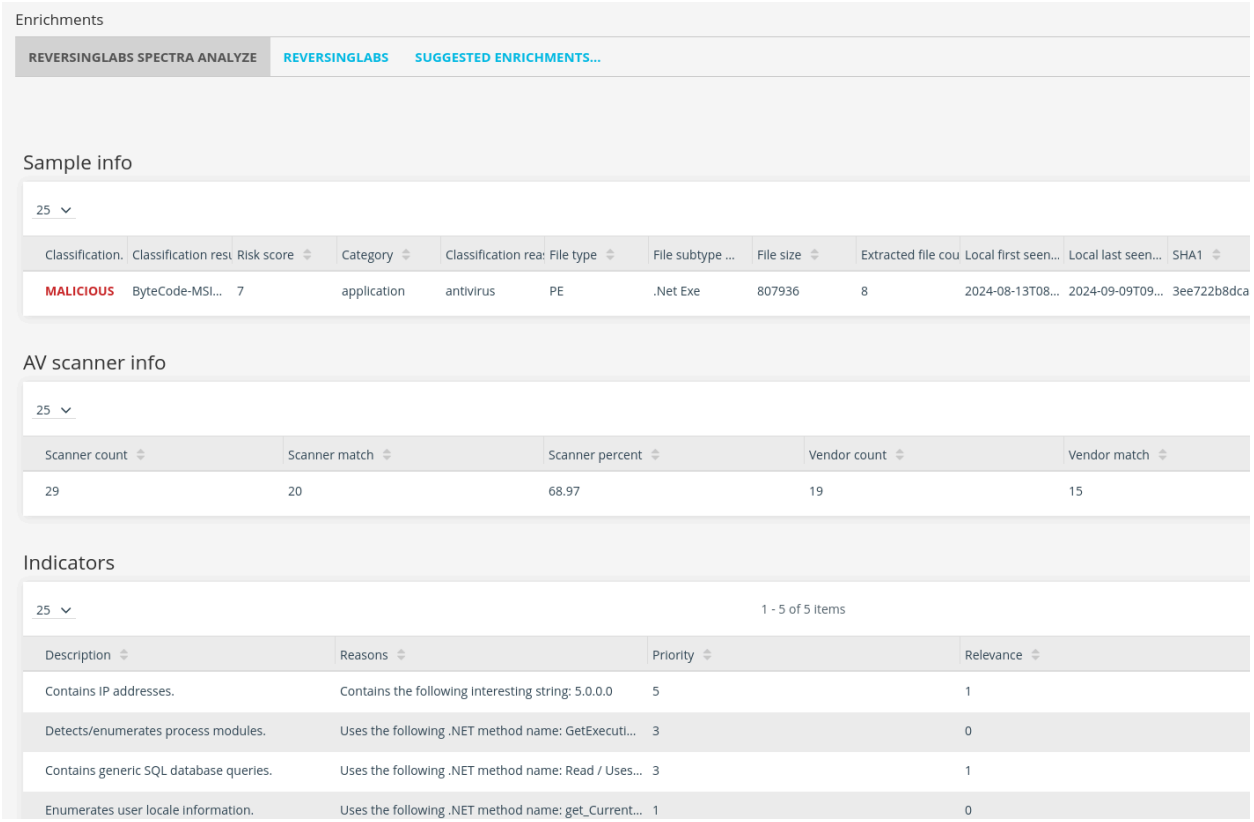
Depending on the observable type and the availability of threat intelligence for the given observable in the ReversingLabs Spectra Analyze, different enrichment tabs will be shown additionally.

IPv4 address:

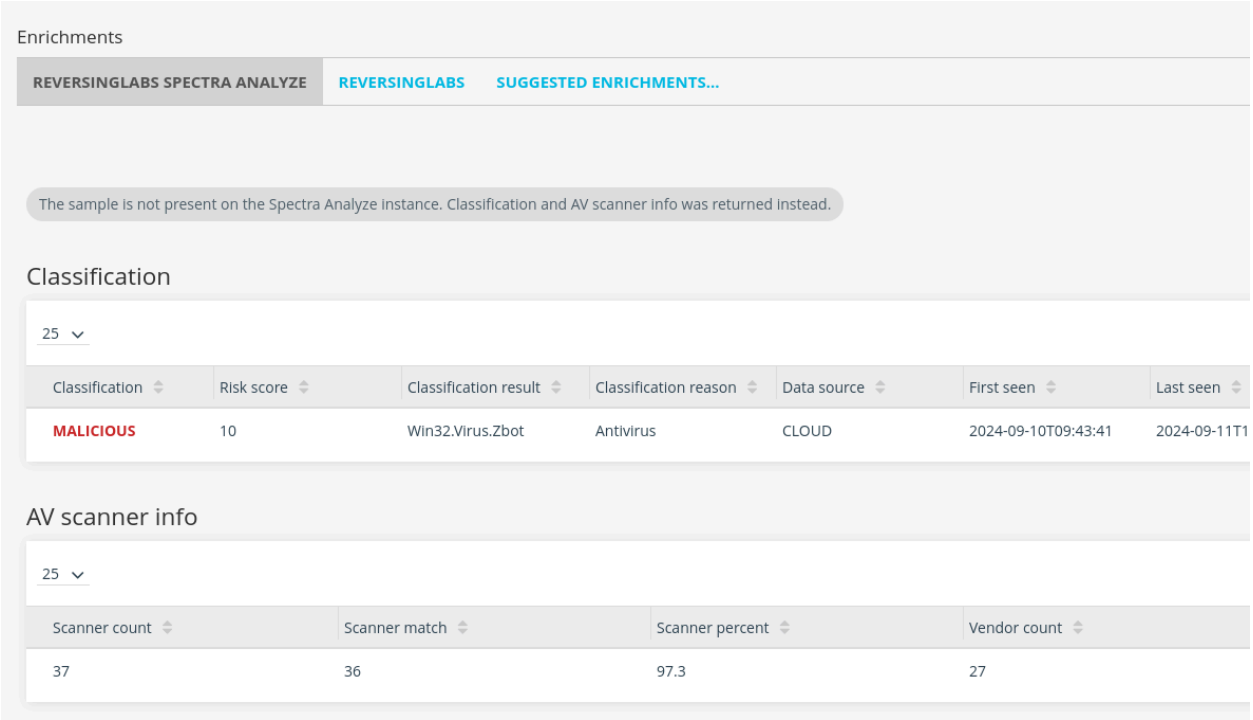


File hash:

In case the sample is **present** on your configured Spectra Analyze instance, the enrichment will display a **detailed sample analysis report**:



In case the sample is **not present** on your configured Spectra Analyze instance, the enrichment will display a **classification report**:



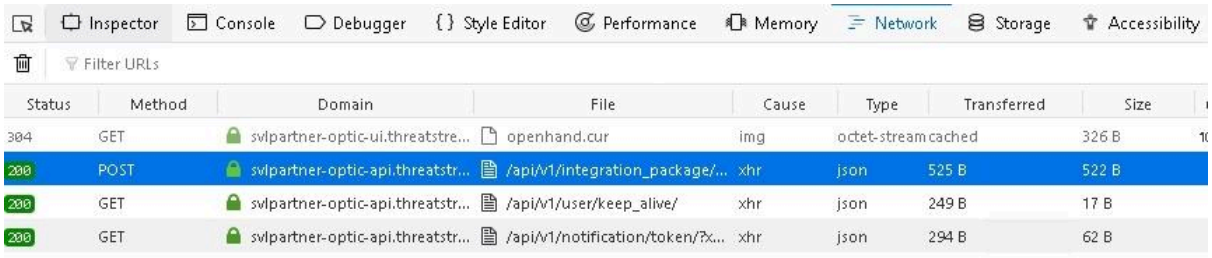
All context-based enrichments display static data formatted into multiple tables.

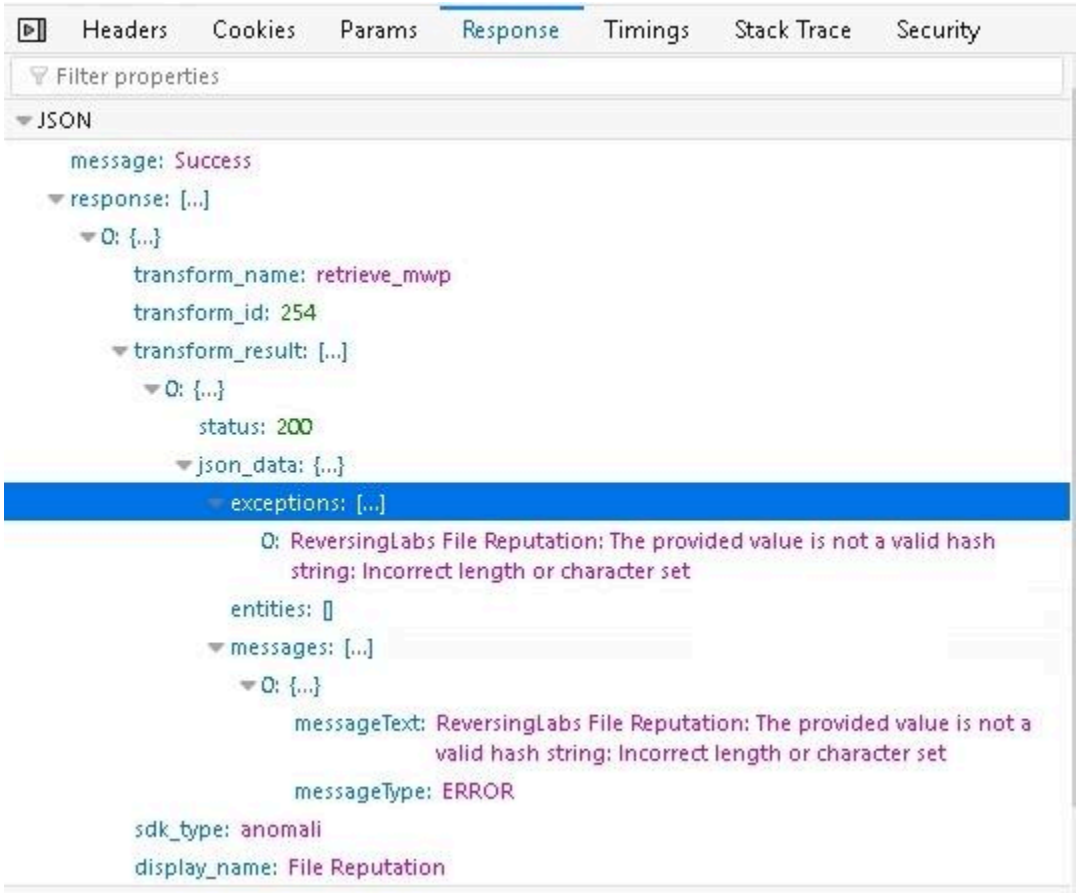
Additional Debugging

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.


Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
Accessibility
Filter URLs
Status
Method
Domain
File
Cause
Type
Transferred
Size
304 GET svlpartner-optic-ui.threatstre... openhand.cur img octet-stream cached 326 B
200 POST svlpartner-optic-api.threatstr... /api/v1/integration_package/... xhr json 525 B 522 B
200 GET svlpartner-optic-api.threatstr... /api/v1/user/keep_alive/ xhr json 249 B 17 B
200 GET svlpartner-optic-api.threatstr... /api/v1/notification/token/?x... xhr json 294 B 62 B


Headers
Cookies
Params
Response
Timings
Stack Trace
Security
Filter properties
JSON
message: Success
response: [...]
0: {...}
transform_name: retrieve_mwp
transform_id: 254
transform_result: [...]
0: {...}
status: 200
json_data: {...}
exceptions: [...]
0: ReversingLabs File Reputation: The provided value is not a valid hash string: Incorrect length or character set
entities: []
messages: [...]
0: {...}
messageText: ReversingLabs File Reputation: The provided value is not a valid hash string: Incorrect length or character set
messageType: ERROR
sdk_type: anomali
display_name: File Reputation

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 Analyze	https://www.reversinglabs.com/products/spectra-analyze

Version History

Date	Version	Author	Comment
2024-09-10	1.0.0	Mislav Sever	Initial document created.