ThreatQuotient

HYAS Insight Action Bundle

Version 1.0.0

March 25, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.29.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The HYAS Insight Action Bundle for ThreatQ submits a data collection of indicator objects to HYAS to query for geo-location, alternative hashes, or HYAS' own verdicts. The integration returns related threat intelligence to be ingested into the ThreatQ library.

The integration provides the following actions:

- **HYAS - IP Lookup** - collects information about an IP address indicator, such as location, ASN, and related FQDNs.
- **HYAS - Get Hashes** - collects related hashes from an initial hash and add the Malware count.
- **HYAS - Get Verdict** - collects the HYAS verdict and verdict reason for IP and FQDN type indicators.

The actions are compatible with the following indicator types:

- FQDN (Get Verdict)
- IP Address (IP Lookup, Get Verdict)
- MD5 (Get Hashes)
- SHA-1 (Get Hashes)
- SHA-256 (Get Hashes)
- SHA-512 (Get Hashes)

The actions return the following enriched indicator object types:

- ASN
- FQDN
- IP Address
- MD5
- SHA-1
- SHA-256
- SHA-512

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A HYAS License and API Key.
- A data collection containing at least one of the following indicator types:
  - FQDN (Get Verdict)
  - IP Address (IP Lookup, Get Verdict)
  - MD5 (Get Hashes)
  - SHA-1 (Get Hashes)
  - SHA-256 (Get Hashes)
  - SHA-512 (Get Hashes)

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip file on your local machine
6. Select the actions to install, when prompted, and click on **Install**.

   > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

The action(s) will now be installed on your ThreatQ instance. You will still need to configure the action(s).

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

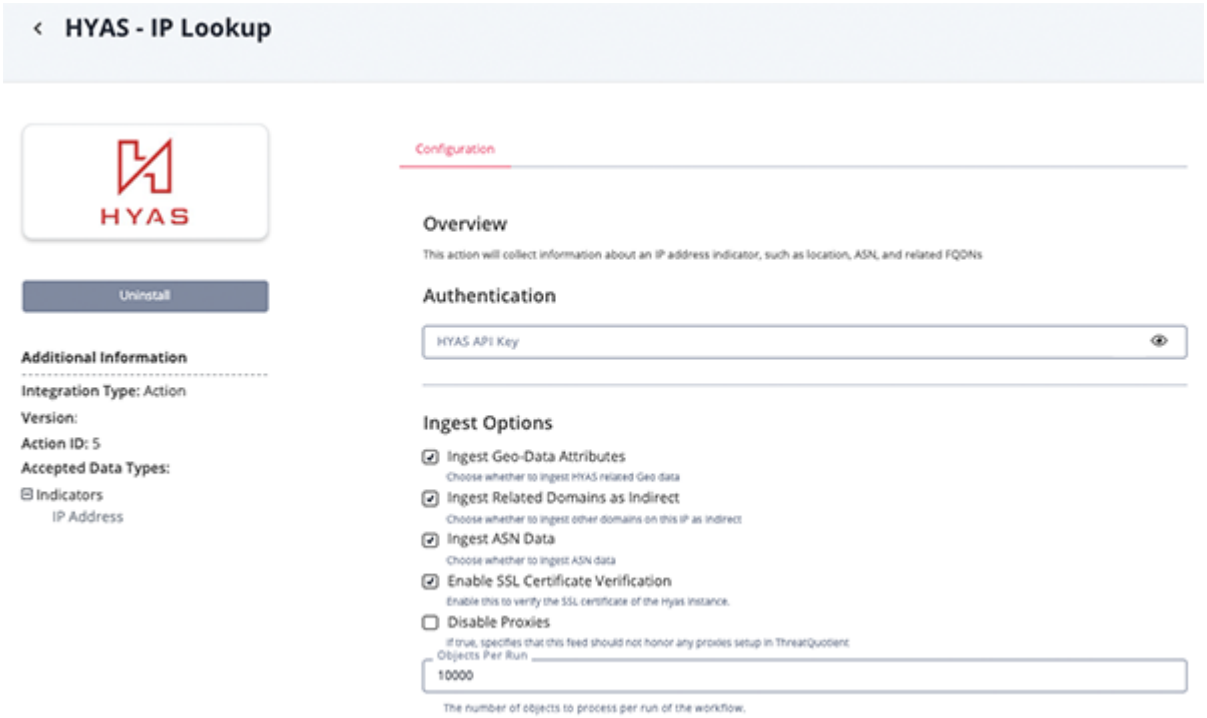
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

HYAS - IP Lookup Parameters

PARAMETER	DESCRIPTION
HYAS API Key	Enter your HYAS API Key.
Ingest Geo-Data Attributes	Enable this parameter to ingest Geolocation data for an IP. This parameter is enabled by default.
Ingest Related Domains as Indirect	Enable this parameter to ingest related FQDNs as "Indirect" rather than the default configured. This parameter is enabled by default.
Ingest ASN Data	Enable this parameter to ingest ASN Data. This parameter is enabled by default.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.

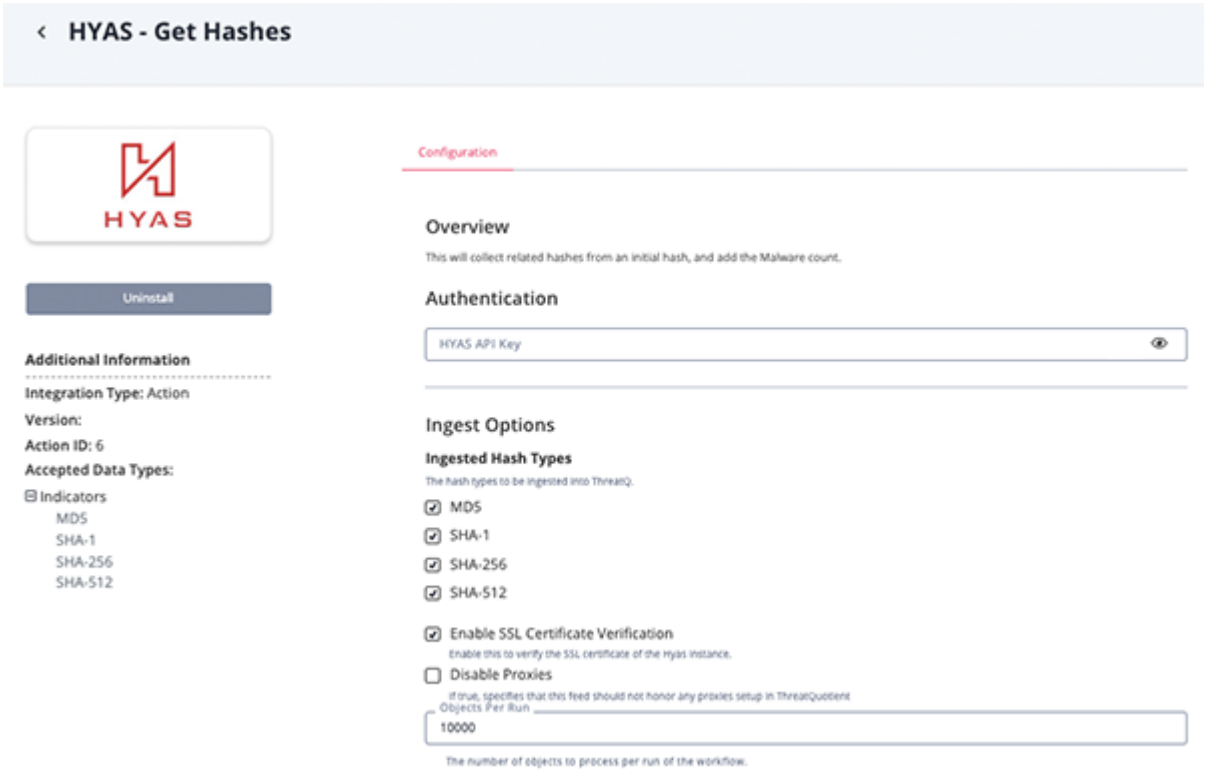
PARAMETER	DESCRIPTION
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	The number of objects to return with each run. The default value is 10,000. Any objects above this limit will be silently ignored.



HYAS - Get Hashes Parameters

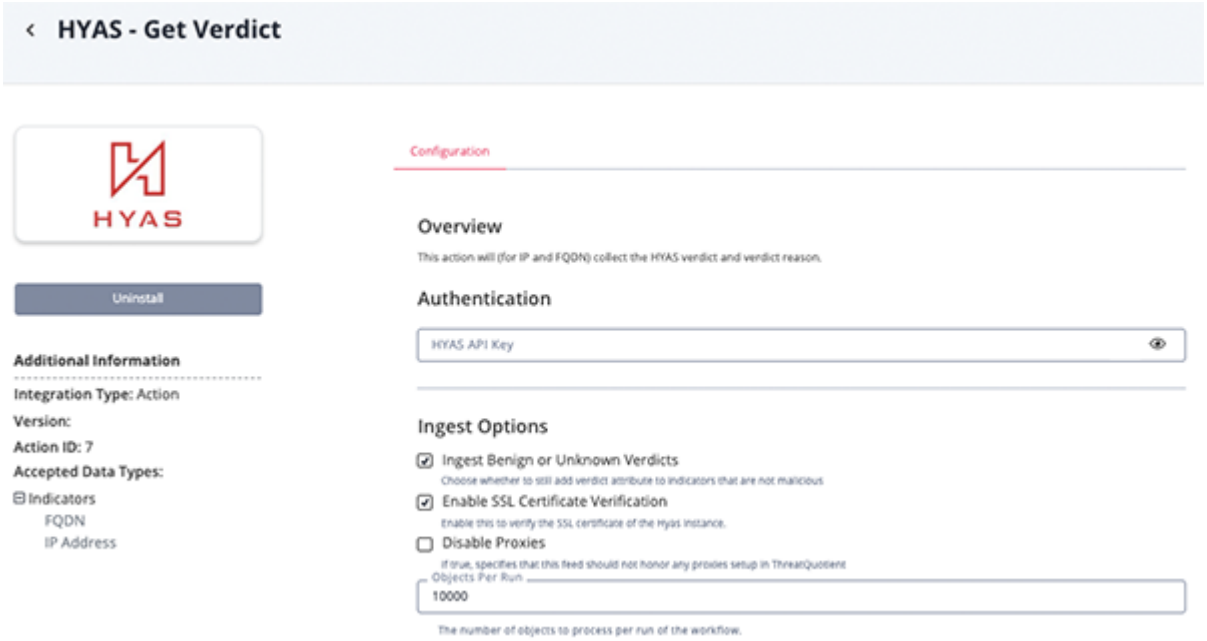
PARAMETER	DESCRIPTION
HYAS API Key	Enter your HYAS API Key.
Ingested Hash Types	Select one or more types of hashes to ingest based on the supplied hash. Options include: ◦ MD5

PARAMETER	DESCRIPTION
	◦ SHA-1 ◦ SHA-256 ◦ SHA-512
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	The number of objects to return with each run. The default value is 10,000. Any objects above this limit will be silently ignored.



HYAS - Get Verdict Parameters

PARAMETER	DESCRIPTION
HYAS API Key	Enter your HYAS API Key.
Ingest Benign or Unknown Verdicts	Select whether to add a Verdict attribute to indicators that are not malicious.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	The number of object to return with each run. The default value is 10,000. Any objects above this limit will be silently ignored.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
HYAS - IP Lookup	Collects information about an IP address, such as location, ASN, and related FQDNs	Indicator	IP Address
HYAS - Get Hashes	Queries a hash and finds alternative variants.	Indicator	MD5, SHA-1, SHA-256, SHA-512
HYAS - Get Verdict	Collects the HYAS verdict for existing IPs or FQDNs.	Indicator	IP Address, FQDN

HYAS - IP Lookup

The HYAS - IP Lookup action collects information about an IP address indicator, such as location, ASN, and related FQDNs.

`POST http://api.HYAS.com/ip/info/batch`

Sample Response:


```
{
  "153.141.243.214": {
    "ip": "153.141.243.214",
    "bogon": false,
    "hostname": "p56214-obmd01.osaka.ocn.ne.jp",
    "anycast": false,
    "city": "Tokyo",
    "region": "Tokyo",
    "latitude": "35.6895",
    "longitude": "139.6917",
    "postal": "101-8656",
    "timezone": "Asia/Tokyo",
    "asn": {
      "asn": "AS4713",
      "name": "NTT Communications Corporation",
      "domain": "ntt.com",
      "route": "153.128.0.0/10",
      "type": "isp"
    },
    "company": {
      "name": "Open Computer Network",
      "domain": "ocn.ne.jp",
      "type": "isp"
    },
    "abuse": {
      "address": "Uchikanda OS Bldg 4F, 2-12-6 Uchi-Kanda, Chiyoda-ku, Tokyo
101-0047, japan",
      "country": "JP",
      "email": "hostmaster@nic.ad.jp",
      "name": "",
      "network": "153.128.0.0-153.253.255.255",
      "phone": "+81-3-5297-2311"
    },
    "privacy": {
      "vpn": false,
      "proxy": false,
      "tor": false,
      "relay": false,
      "hosting": false,
      "service": ""
    },
```

```
    "domains": [
      "livets.ru",
      "fragsts.ru",
      "topts3.ru",
      "topts3.online"
    ],
    "country_code": "JP",
    "country_name": "Japan",
    "domains_total": 0,
    "private": false
  }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
{IP}.city	Indicator.Attribute	City	N/A	Tokyo	User-configurable.
{IP}.region	Indicator.Attribute	Region	N/A	Tokyo	User-configurable.
{IP}.latitude	Indicator.Attribute	Latitude	N/A	"35.6895"	User-configurable.
{IP}.longitude	Indicator.Attribute	Longitude	N/A	"139.6917"	User-configurable.
{IP}.postal	Indicator.Attribute	Postal Code	N/A	"101-8656"	User-configurable.
{IP}.timezone	Indicator.Attribute	Timezone	N/A	"Asia/Tokyo"	User-configurable.
{IP}.country_code	Indicator.Attribute	Country Code	N/A	JP	User-configurable.
{IP}.country_name	Indicator.Attribute	Country	N/A	Japan	User-configurable.
{IP}.asn.asn	Indicator	ASN	N/A	4713	User-configurable. Status set to Indirect
{IP}.asn.route	Indicator	CIDR Block	N/A	153.128.0.0/10	User-configurable. Status set to Indirect
{IP}.asn.name	Indicator.Attribute	Name	N/A	NTT Communications Corporation	Added to both ASN and CIDR
{IP}.asn.domain	Indicator.Attribute	ASN Owner Domain	N/A	ntt.com	Added to both ASN and CIDR
{IP}.domains[]	Indicator	FQDN	N/A	livets.ru	N/A
{IP}.ip	Indicator	IP Address	N/A	153.141.243.214	N/A

HYAS - Get Hashes

The HYAS - Get Hashes action collects related hashes from an initial hash, and add the Malware count.

`POST https://api.HYAS.com/malware/v2/information`

Sample Response:


```
{
    "items":
    [
        {
            "md5": "2781f23530d6a69824ab8f23ec40595d",
            "sha1": "95762c6bb48f4669c2d91bde8f4ee43cce0dbd5c",
            "sha256":
"11f4e9be4a633369d2dac63abff03111b576cbd4c3ca8a083a4343796fd2eed0",
            "sha512":
"6906bde845d2ca3577d72358cf8288d2956b839f0129d0b61dc5099d2814b9a6a75f92783a4095
17df5bb9fded1298ae798ebfff7f64d6a3629a80b79e7cc2dc",
            "scan_time": "2022-07-12T05:10:18Z",
            "avscan_score": "6/24",
            "scan_results":
            [
                {
                    "av_name": "Bitdefender",
                    "threat_found": "Trojan.GenericKD.39854339",
                    "def_time": "2022-06-24T09:16:11Z"
                },
                {
                    "av_name": "Cyren",
                    "threat_found": "W32/MSIL_Kryptik.GME.gen!Eldorado",
                    "def_time": "2022-06-24T10:24:00Z"
                },
                {
                    "av_name": "Emsisoft",
                    "threat_found": "Trojan.GenericKD.39854339 (B)",
                    "def_time": "2022-06-24T10:01:00Z"
                },
                {
                    "av_name": "IKARUS",
                    "threat_found": "Trojan-Spy.Vidar",
                    "def_time": "2022-06-24T07:41:38Z"
                },
                {
                    "av_name": "K7",
                    "threat_found": "Trojan-Downloader ( 00594af71 )",
                    "def_time": "2022-06-24T07:31:00Z"
                },
                {
                    "av_name": "Kaspersky",
```

```
                    "threat_found": "HEUR:Trojan.MSIL.Startun.gen",
                    "def_time": "2022-06-24T07:21:00Z"
                }
            ]
        }
    ]
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
items[].md5	Indicator	MD5	N/A	2781f23530d6a69824ab8f23ec40595d	N/A
items[].sha1	Indicator	SHA-1	N/A	95762c6bb48f4669c2d91bde8f4ee43cce0dbd5c	N/A
items[].sha256	Indicator	SHA-256	N/A	11f4e9be4a633369d2dac63abff03111b576cbd4c3ca8a083a4343796fd2eed0	N/A
items[].sha512	Indicator	SHA-512	N/A	6906bde845d2ca3577d72358cf8288d2956b839f0129d0b61dc5099d2814b9a6a75f92783a409517df5bb9fded1298ae798ebfff7f64d6a3629a80b79e7cc2dc	N/A
items[].avscan_score	Indicator.Attribute	AV Scan Score	N/A	"6/24"	

HYAS - Get Verdict

The HYAS - Get Verdict action collects the HYAS verdict and verdict reason for IP and FQDN type indicators.

```
GET https://api.HYAS.com/infrastructure-analyzer/ioc
```

Sample Response:

```
{
    "verdict": "Suspicious",
    "verdict_reason": "Domain Config/History",
    "verdict_reason_list":
    [
        "Domain Config/History"
    ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.verdict	Indicator.Attribute	Verdict	N/A	Suspicious	N/A
.verdict_reason	Indicator.Attribute	Verdict Reason	N/A	Domain Config/History	N/A

Enriched Data

> Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

HYAS - IP Lookup

METRIC	RESULT
Run Time	1m
Indicators	23
Indicator Attributes	89

HYAS - Get Hashes

METRIC	RESULT
Run Time	1m
Indicators	20
Indicator Attributes	20

HYAS - Get Verdict

METRIC	RESULT
Run Time	1m
Indicators	100
Indicator Attributes	102

Change Log

- **Version 1.0.0**
  - Initial release