ThreatQuotient

Project Hades Operation

Version 1.0.0

September 17, 2024

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	>= 4.57.2
Support Tier	ThreatQ Supported

Introduction

The Project Hades operation for ThreatQ provides actions that perform lookups of indicators of compromise, cryptocurrency hashes and onion sites in the Project Hades database.

The operation provides the following actions:

- **Search Project Hades (Indicators)** - queries the Project Hades database for indicators of compromise.
- **Search Project Hades (Cryptocurrency)** - queries the Project Hades database for cryptocurrency hashes.

The operation can query the following object types

- Indicators - Email Address, IP Address, Hashes (MD5, SHA-1, SHA-256)
- Cryptocurrency - Bitcoin, Ethereum

Prerequisites

The following is required install and use the integration:

- Project Hades API credentials
- Cryptocurrency and Onion custom objects. Review the steps below for details on installing the required custom objects and types.

Custom Objects

The integration requires the Cryptocurrency and Onion custom objects. Additionally, two Cryptocurrency types are required: Bitcoin and Ethereum. The custom object script provided with the integration files will install both the custom objects and the required Cryptocurrency types.

Use the steps provided to install the the custom objects.

> When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

ThreatQ V6 Steps

Use the following steps to install the custom objects in ThreatQ v6:

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.

   > The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Navigate to the following location:

   ```
   cd /var/lib/threatq/misc/
   ```

5. Upload the custom object files, including the images folder.

   The directory structure should be as the following:

   - misc
     - install.sh
     - <custom_object_name>.json
     - images (directory)
       - <custom_object_name>.svg

6. Run the following command:

```
kubectl exec -it deployment/api-schedule-run -n threatq -- sh /var/
lib/threatq/misc/install.sh /var/lib/threatq/misc
```

> The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

7. Delete the install.sh, definition json file, and images directory from the `misc` directory after the object has been installed as these files are no longer needed.

ThreatQ v5 Steps

Use the following steps to install the custom objects in ThreatQ v5:

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   cd /tmp/
   ```

4. Create a new directory:

   ```
   mkdir hades_op
   ```

5. Upload the **hades.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the hades_op directory.

   ```
   mkdir images
   ```

7. Upload the Cryptocurrency and Onion svg files.
8. Navigate to the **/tmp/hades_op**.

   The directory should resemble the following:

   - tmp
     - **hades_op**
       - **hades.json**
       - **install.sh**
       - **images**
         - **crypocurrency.svg**
         - **onion.svg**

9. Run the following command to ensure that you have the proper permissions to install the custom object:

   ```
   chmod +x install.sh
   ```

10. Run the following command:

    ```
    sudo ./install.sh
    ```

> You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf hades_op
```

Installation

> The operation requires the installation of custom objects before installing the actual operation. See the Prerequisites chapter for more details. The custom objects must be installed prior to installing the operation. Attempting to install the operation without the custom objects will cause the operation install process to fail.

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 integration zip file.
3. Extract and install the required custom objects listed in the Prerequisites chapter.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration .whl file using one of the following methods:
   - Drag and drop the .whl file into the dialog box
   - Select **Click to Browse** to locate the .whl file on your local machine

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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

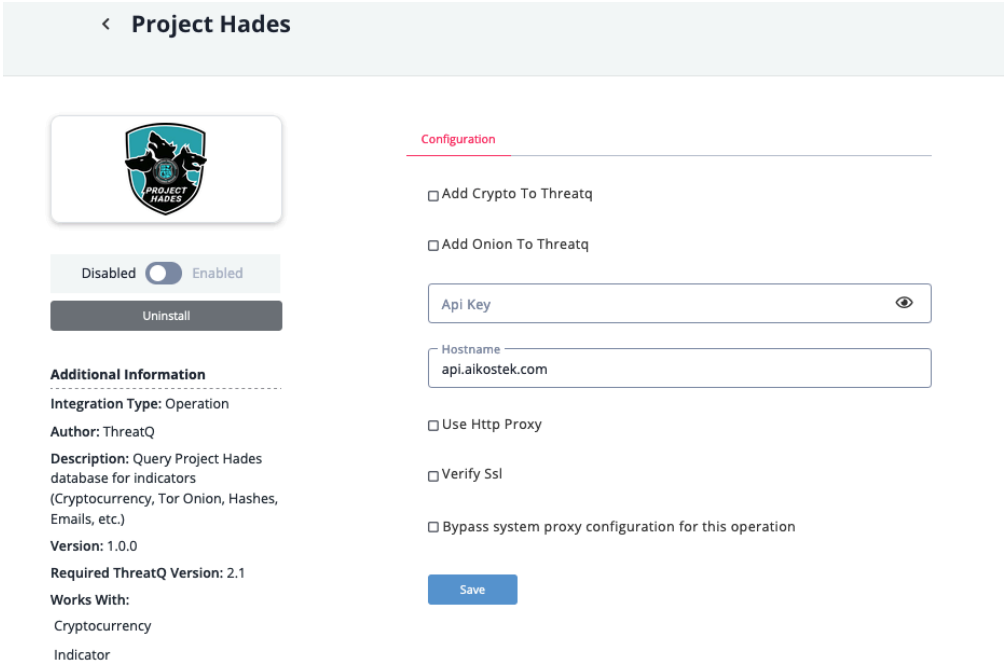
Configuration

> 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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Hostname	Your hostname or IP address of Project Hades API. The default is api.aikostek.com.
API Key	Your access token for authenticating with Project Hades API.
Add Onion Sites to ThreatQ	Enabling this option allows you to automatically add any discovered Onion sites to ThreatQ.
Add Cryptocurrency Hashes to ThreatQ	Enabling this option allows you to automatically add any discovered cryptocurrency hashes to ThreatQ.
Use HTTP Proxy	Enabling this option allows you to use the HTTP proxy configured in the ThreatQ System Configurations.
Verify SSL	Enabling this option allows you to verify SSL when connecting to Project Hades API.



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Search Project Hades	Query Project Hades database for indicators of compromise	Indicator	IP Address, Email Address, MD5, SHA-1, SHA-256
Search Project Hades	Query Project Hades database for cryptocurrency hashes	Cryptocurrency	Bitcoin, Ethereum

Search Project Hades (Indicators)

The Search Project Hades action, when performed on an indicator, queries the Project Hades database for indicators of compromise.

Email Address

`GET https://api.aikostek.com/v2/lookup/email`

Sample Response:


```
{
  "data": [
    {
      "appearances": [
        "pedohubd2zi7jv5e.onion",
        "pedohub755qxwt7mpcdq3tj455aum7ejwvca2nghmejbwldgizjn4oid.onion",
        "pedohubksclx37ve.onion",
        "pedohubhsrhqwbhh.onion",
        "pedohub6lyqy7pla.onion",
        "pedohubvqv5mnxazrhv6kqzrz6ezebkugt7daro7cfsum6zfrmdtgaqd.onion",
        "pedohub2jyt2rcucrbbmrvaxrfowvvueddilwaugkowxpt3t7tznpcqd.onion",
        "udp3dseyoyfk3n4oug2c4s63rqpyaczfii3ipwgdrxpdc4pouy4u3qyd.onion",
        "pedohubj4cx2xebrvcjt3b5eoae3lxme34fj6kmwblzr3wd6ria5gfid.onion",
        "pedohubbuiyyxxh5uodpcm4yhscm6nsl2ne2skcuiwoelbuav5rffgid.onion",
        "pedohubmq66kovax642xrpwajvq4wnz3zzkr6kp6frlcjxoz5mahgyqd.onion",
        "pedohubotw4vaob3jahhxmblg73mxf7uvhbkltnr4htzl2ezemsr36yd.onion",
        "pedohubk6dvg33wjtinp7dvszec4n6lyut4p2ay46ieulolseeboksyd.onion"
      ],
      "meta": "",
      "selector": "opva.access@secmail.pro",
      "source_url": [
        "http://pedohubotw4vaob3jahhxmblg73mxf7uvhbkltnr4htzl2ezemsr36yd.onion",
        "http://pedohubotw4vaob3jahhxmblg73mxf7uvhbkltnr4htzl2ezemsr36yd.onion/index.html",
        "http://pedohub2ffxswug6w2mczstmwgnwmfhp2cdrwcdelg3t5yvtnfjjdyqd.onion",
        "http://pedohub2ffxswug6w2mczstmwgnwmfhp2cdrwcdelg3t5yvtnfjjdyqd.onion/index.html",
        "http://sw7utj33cbpsw4pywco7c6ylhajcggt4fzmlxex32bxkn5c57zix42id.onion",
        "http://sw7utj33cbpsw4pywco7c6ylhajcggt4fzmlxex32bxkn5c57zix42id.onion/index.html",
        "http://pedohubmzbd7mkbv3alsflgcmuemzo2yufwqjvr2nsntdxdnzgnsc7id.onion",
        "http://pedohub5am7icvfpr3brn2eaaagv3vtyua3iex7gj7czfm3dvfhjrnad.onion",
        "http://pedohub5am7icvfpr3brn2eaaagv3vtyua3iex7gj7czfm3dvfhjrnad.onion/index.html"
      ],
      "type": "email"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].	Onion	Onion	Current Timestamp	pedohub6lyqy7pla.onion	The .onion nodes are automatically added to ThreatQ and related to the primary object

Hashes (MD5, SHA-1, SHA-256)

`GET https://api.aikostek.com/v2/lookup/hash`

Sample Response:


```
{
  "data": [
    {
      "appearances": [
        "22kx7cbfnz6cwhz2.onion",
        "2464b3fu462tx2en.onion",
        "24mtxzx54uexcnrs.onion",
        "25ijhvugmashun4x.onion",
        "2ba4l7ihpln5krxs.onion",
        "2cj2kjlxtwbfytbl.onion",
        "2deogh434fawggi7.onion",
        "2dlp7y6hz7s43haz.onion",
        "2k62gpuyurilf5fh.onion",
        "2splewjorncdtgls.onion",
        "2yafdfcfigpj2kd2.onion",
        "2z2kekl4xsry4fvi.onion",
        "2zdche5xwicvayv6.onion",
        "2zmicnxnb5324msg.onion",
        "34ljepgdnctyqndm.onion",
        "zzdcf3fpnfcn7l24.onion",
        "vbj36rtt5sdomdi7f6gy4y3sjot3z5dcm3pkofv3bujwvc7qv5q6wbyd.onion",
        "joyaqqqf3cs4koe6siz5ab3xx36ukbfuxxuew7mil55zs5r7ndnvycqd.onion",
        "iqxkqwppsnbxcd4tj7vlhyspvz2oy4id6znfmhthaq7wphaakjasr3id.onion",
        "f6ha7dpjcyi3ohrd3o3fqxmkjdvmkp6uuyvetiqlgnzxoeekcqhdudyd.onion"
      ],
      "filename": "4.png",
      "first_seen": "2021-06-17T10:01:12Z",
      "md5": "ef212899150c852b6677a0b8bbf113f3",
      "onion": "22kx7cbfnz6cwhz2.onion",
      "sha1": "a96549dd6cee4630ef9763f2988c445a98b5778e",
      "sha256": "2b0d7124e05dba6b5d0de095ca09f0781213939be0dcda3bd66dec49cab4d1b3",
      "source_url": "hXXp://22kx7cbfnz6cwhz2[.]onion/",
      "url": "hXXp://22kx7cbfnz6cwhz2[.]onion/CHILDPORNCENTER/4.png"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].	Onion	Onion	Current Timestamp	2z2kekl4xsry4fvi.onion	The .onion nodes are automatically added to ThreatQ and related to the primary object
.data[].	Indicator	Filename	Current Timestamp	4.png	
.data[].	Indicator	MD5	Current Timestamp	ef212899150c852b6677a0b8bbf113f3	
.data[].	Indicator	SHA-1	Current Timestamp	a96549dd6cee4630ef9763f2988c445a98b5778e	
.data[].	Indicator	SHA-256	Current Timestamp	2b0d7124e05dba6b5d0de095ca09f0781213939be0dcda3bd66dec49cab4d1b3	
.data[].	Indicator	URL	Current Timestamp	hXXp://22kx7cbfnz6cwhz2[.]onion/CHILDPORNCENTER/4.png	

IP Address

`GET https://api.aikostek.com/v2/lookup/ip`

Sample Response:


```
{
  "data": [
    {
      "appearances": [
        "hpf2suizq5llpg6b.onion",
        "kzuywmbp5vsd6a3h.onion",
        "ovnhblrjrpf3x5k4.onion",
        "e5kornfjykwb7jif.onion",
        "tubeabf4racapudw.onion",
        "2ytx47bzuorew4id.onion",
        "vp4egeld5gh3wny3.onion",
        "e464ynqdbn3wdzhr.onion",
        "a64azcam7zdkug5u.onion",
        "lz7yglodon4s4kpy.onion",
        "3lmt2qhh3kct3ocy.onion",
        "zg43cdq7r36zgmlwqie5ijcwg7v6fhry2hvmokuyzn6h743jvwq34sid.onion",
        "4four5xmolkr2yqqgxkqv2dpks4cghafyked555si3aktzrfsnl5pcyd.onion",
        "ryeuyd3sqpqrfczicvej2dcluu2rcob55hivengfwdec3bvbron2l7id.onion",
        "ig6tu53xl5s7wmwzbi3uvdyq3vntlb6czbalskbfg6cot6ybvnyafhyd.onion"
      ],
      "meta": {
        "city": "Yonkers",
        "country": "US",
        "hostname": "ool-182f2e3f.dyn.optonline.net",
        "loc": "40.9312,-73.8988",
        "org": "AS6128 Cablevision Systems Corp.",
        "postal": "10702",
        "region": "New York",
        "timezone": "America/New_York"
      },
      "selector": "1.1.57.69",
      "source_url": [
```

```
        "http://dqcdd6m64tte2nt3v5xwkyadakhougkhnsqkmloh2cfy44ne7wty23yd.onion/login"
      ],
      "type": "ip"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].	Onion	Onion	Current Timestamp	a64azcam7zdkug5u.onion	The .onion nodes are automatically added to ThreatQ and related to the primary object
.data[].	indicator.attribute	City	Current Timestamp	Yonkers	
.data[].	indicator.attribute	Country	Current Timestamp	US	
.data[].	indicator.attribute	Region	Current Timestamp	New York	
.data[].	indicator.attribute	Timezone	Current Timestamp	America/New_York	
.data[].	indicator.attribute	Geolocation	Current Timestamp	40.9312,-73.8988	
.data[].	indicator.attribute	Postal Code	Current Timestamp	10702	
.data[].	indicator.attribute	Organization	Current Timestamp	AS6128 Cablevision Systems Corp.	
.data[].	indicator.attribute	Hostname	Current Timestamp	ool-182f2e3f.dyn.optonline.net	

Search Project Hades (Cryptocurrency)

High-level summary of what info the action does

`GET https://api.aikostek.com/v2/lookup/crypto`

Sample Response:


```
{
  "data": [
    {
      "appearances": [
        "bngoskfo32g3mjzo.onion",
        "jjlcfbdzivju5bh2.onion",
        "tzcrbsdfetmohmms.onion",
        "skcnr65vumlo6eaz.onion",
        "5th3cqxt4jqjepdm.onion",
        "wvzb5aqijvbe7t7w.onion",
        "dsnrhcttjax66jzf.onion",
        "tajcpga3m7okprcw.onion",
        "wiukcn7en7itzqvu.onion",
        "eongxahzuxsganqo.onion",
        "oaiavbaamzwmc7sp.onion",
        "lotto3gggtl3lnldipcb3co5bc3rbpfxebdcuf3dild7llxv3cg3gtid.onion",
        "3c2xastt7ripfjjyr3iaalu2rhjsnspwnbjma2sf23ob2rruz6eviiid.onion"
      ],
      "meta": "",
      "selector": "3JgfqZmwGFseH7hpkmrejyoryUkXaXriyE",
      "type": "bitcoin"
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].	Onion	Onion	Current Timestamp	oaiavbaamzwmc7sp.onion	The .onion nodes are automatically added to ThreatQ and related to the primary object

Change Log

- **Version 1.0.0**
  - Initial release