ThreatQuotient

Sixgill Darkfeed Guide

Version 1.0.2

Monday, November 9, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@cybersixgill.com

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.

Contents

Versioning

- Current integration version: 1.0.2
- Supported on ThreatQ versions: 4.34.0 or greater

Introduction

Delivering the next generation of deep & dark web threat intelligence feeds, Sixgill tailors threat intelligence to customers' intelligence needs, maximizing effective mitigation and remediation. Using an agile collection methodology and its proprietary collection automation algorithm, Sixgill provides broad coverage of exclusive-access deep and dark web sources, as well as relevant surface web sources. Sixgill harnesses artificial intelligence and machine learning to automate the production cycle of cyber intelligence from monitoring through extraction to production - unleashing both existing platforms' and teams' performance.

Leverage the power of Sixgill to supercharge ThreatQuotient with real-time Threat Intelligence indicators. Get IOCs such as domains, URLs, hashes, and IP addresses straight into the ThreatQuotient platform.

Installation

Perform the following steps to install the integration:

Note: *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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:

- Drag and drop the file into the dialog box
- Select **Click to Browse** to locate the integration file on your local machine

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

6. If prompted, select the individual feeds to install and click **Install**.

The feed will be added to the Commercial category for integrations. You will still need to configure and then enable the feed.

Configuration

Note: *ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other feed-related credentials.*

To configure the feed:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** tab (optional).
3. Click on the integration to open its details page.
4. Under the Connection tab, enter the following configuration parameters:

Parameter	Description
API ID	Your Sixgill API ID.
API Key	Your Sixgill API Key.
Add MITRE Tactics to Indicators	Toggle controlling whether MITRE Attack Patterns will be related to ingested indicators from Sixgill.

5. Click on **Save**.
6. Click on the toggle switch to the left of the integration name to enable it.

ThreatQ Mapping

The API ID and API Key User Fields are required in order to set the end points.

The endpoints used by this feed are as follows:

POST https://api.cybersixgill.com/auth/token

`POST https://api.cybersixgill.com/auth/token` - returns an OAuth2 token.


```
{
    "access_token":
"eyJhbGciOiJIUzUxMiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICIwODc2ZDU4My1lODI1LTRhNmEt
YTZiMC1iNDhiNjA2MGM5YmIifQ.eyJleHAiOjE1OTM0NDYwNjAsImlhdCI6MTU5MzQxNzI2MCwian
RpIjoiZjQ1YzgyNDYtNGU5OC00MzYwLTg2ODktNTNhZjU5YmMxNmRjIiwiaXNzIjoiaHR0cHM6Ly9
zZWN1cmVhY2Nlc3MuY3liZXJzaXhnaWxsLmNvbS9hdXRoL3JlYWxtcy9TaXhnaWxsIiwiYXVkIjoi
YWNjb3VudCIsInN1YiI6IjgxMTgwMjA0LTQ0YjEtNDgwNS04ZjJmLWNjZTQ4NTM3NDU1ZiIsInR5c
CI6IkJlYXJlciIsImF6cCI6ImxvZ2luc29mdCIsInNlc3Npb25fc3RhdGUiOiIxMWFiMzBjOS1kOT
Q3LTQ4NGEtOGU5Yi1hNTEwNzE3NjJjOWUiLCJhY3IiOiIxIiwicmVhbG1fYWNjZXNzIjp7InJvbGV
zIjpbIm9mZmxpbmVfYWNjZXNzIiwidW1hX2F1dGhvcml6YXRpb24iXX0sInJlc291cmNlX2FjY2Vz
cyI6eyJhY2NvdW50Ijp7InJvbGVzIjpbIm1hbmFnZS1hY2NvdW50IiwibWFuYWdlLWFjY291bnQtb
Glua3MiLCJ2aWV3LXByb2ZpbGUiXX19LCJzY29wZSI6ImVtYWlsIHByb2ZpbGUiLCJjbGllbnRIb3
N0IjoiMTgyLjc2LjE3NS4xMTgiLCJjbGllbnRJZCI6ImxvZ2luc29mdCIsImVtYWlsX3ZlcmlmaWV
kIjpmYWxzZSwicHJlZmVycmVkX3VzZXJuYW1lIjoic2VydmljZS1hY2NvdW50LWxvZ2luc29mdCIs
ImNsaWVudEFkZHJlc3MiOiIxODIuNzYuMTc1LjExOCIsIm9yZ0lkIjoiNWViOTc0ZjkxMzg3NzAwM
DEzZGY5YTM0In0.a7DHCtIUF2JVamI-
Don3_fsMLBe4kLKQUMICuen3aM43yqMG2t5nf4Q4dEV9sD86PjeOjPCIASSSpGJJb8n__A",
    "expires_in": 28800,
    "refresh_expires_in": 86400,
    "refresh_token":
"eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICI4NzczMmU4ZS0zNTU3LTRjMjEt
ODNiZS1hZWNhMzAzNTgyMjYifQ.eyJleHAiOjE1OTM1MDM2NjAsImlhdCI6MTU5MzQxNzI2MCwian
RpIjoiODg2ODM5ZTAtZGU0Ni00YjgzLWFkYTUtNDZhOWM4ODNhYzUwIiwiaXNzIjoiaHR0cHM6Ly9
zZWN1cmVhY2Nlc3MuY3liZXJzaXhnaWxsLmNvbS9hdXRoL3JlYWxtcy9TaXhnaWxsIiwiYXVkIjoi
aHR0cHM6Ly9zZWN1cmVhY2Nlc3MuY3liZXJzaXhnaWxsLmNvbS9hdXRoL3JlYWxtcy9TaXhnaWxsI
iwic3ViIjoiODExODAyMDQtNDRiMS00ODA1LThmMmYtY2NlNDg1Mzc0NTVmIiwidHlwIjoiUmVmcm
VzaCIsImF6cCI6ImxvZ2luc29mdCIsInNlc3Npb25fc3RhdGUiOiIxMWFiMzBjOS1kOTQ3LTQ4NGE
tOGU5Yi1hNTEwNzE3NjJjOWUiLCJzY29wZSI6ImVtYWlsIHByb2ZpbGUifQ.hlMFrFQJigxjU2Tli
DrYy26mU7dcanms94XgrobRUTI",
    "token_type": "bearer",
    "not-before-policy": 0,
    "session_state": "11ab30c9-d947-484a-8e9b-a51071762c9e",
    "scope": "email profile"
}
```

GET https://api.cybersixgill.com/darkfeed/ioc?limit=2000

GET https://api.cybersixgill.com/darkfeed/ioc?limit=2000 - returns 2000 Darkfeed threat intelligence IOCs.

```
GET https://panacea.threatgrid.com/api/v2/search/submissions
```


```
{
  "id": "bundle--318ed832-2b1c-4d3d-8b9f-6b4b8ef628ad",
  "objects": [
    {
      "created": "2017-01-20T00:00:00.000Z",
      "definition": {
        "tlp": "amber"
      },
      "definition_type": "tlp",
      "id": "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82",
      "type": "marking-definition"
    },
    {
      "created": "2019-12-26T00:00:00Z",
      "definition": {
        "statement": "Copyright Sixgill 2020. All rights reserved."
      },
      "definition_type": "statement",
      "id": "marking-definition--41eaaf7c-0bc0-4c56-abdf-d89a7f096ac4",
      "type": "marking-definition"
    },
    {
      "created": "2020-05-12T15:38:42.969Z",
      "description": "Malware available for download from file-sharing
sites",
      "external_reference": [
        {
          "description": "Mitre attack tactics and technique reference",
          "mitre_attack_tactic": "Build Capabilities",
          "mitre_attack_tactic_id": "TA0024",
          "mitre_attack_tactic_url":
"https://attack.mitre.org/tactics/TA0024/",
          "mitre_attack_technique": "Obtain/re-use payloads",
          "mitre_attack_technique_id": "T1346",
          "mitre_attack_technique_url":
"https://attack.mitre.org/techniques/T1346/",
          "source_name": "mitre-attack"
        }
      ],
      "id": "indicator--4bf4b89b-1115-40d1-9f6c-a70405d49141",
      "labels": [
        "malicious-activity",
        "malware",
        "Build Capabilities",
        "Obtain/re-use payloads"
      ],
      "lang": "en",
      "modified": "2020-05-12T15:38:42.969Z",
      "object_marking_refs": [
```

```
        "marking-definition--41eaaf7c-0bc0-4c56-abdf-d89a7f096ac4",
        "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
      ],
      "pattern": "[url:value =
'https://anonfile.com/te7aYaw7o9/Leeched_Combo_464705_txt']",
      "sixgill_actor": "h4ckcr4ck",
      "sixgill_confidence": 80,
      "sixgill_feedid": "darkfeed_010",
      "sixgill_feedname": "malware_download_urls",
      "sixgill_postid": "bded5cfcb05b917ac80c7a0aaac45a2fffb26ce4",
      "sixgill_posttitle": "464705 - HQ Combolist Mega, File-upload,
Mediafire, 4shared",
      "sixgill_severity": 80,
      "sixgill_source": "forum_nulled",
      "spec_version": "2.0",
      "type": "indicator",
      "valid_from": "2020-05-08T05:53:26Z"
    }
  ],
  "spec_version": "2.0",
  "type": "bundle"
}
```


POST https://api.cybersixgill.com/darkfeed/ioc/ack

Acknowledges that you consumed a batch of IOC items after running the ioc endpoint. The next time you run the ioc endpoint, you will receive the next bundle of IOCs.


```
{
  2000
}
```

The following table shows the mapping for the analysis results:

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.objects[].pattern	Indicator Value	Extracted from .objects[].pattern	.objects[].valid_from	url:value = 'https://anonfile.com/bcqfn7ydoa/sqli_dumper_10.1_zip']	Both value and type are extracted from .pattern
.objects[].modified	Indicator Modified At	N/A	N/A	2020-05-15T12:10:28.942Z	N/A
.objects[].revoked	Indicator Status	N/A	N/A	False	'Active' if .revoked is False else 'Whitelisted'
.objects[].description	Indicator Description	N/A	N/A	Malware available for download from file-sharing sites	N/A
.objects[].sixgill_confidence	Indicator Attribute	Confidence	.objects[].valid_from	80	N/A
.objects[].sixgill_severity	Indicator Attribute	Severity	.objects[].valid_from	80	N/A
.objects[].sixgill_feedname	Indicator Attribute	Sixgill Feed Name	.objects[].valid_from	malware_download_urls	N/A
.objects[].sixgill_feedid	Indicator Attribute	Sixgill Feed ID	.objects[].valid_from	darkfeed_010	N/A

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.objects[].sixgill_postid	Indicator Attribute	Sixgill Post ID	.objects[].valid_from	9528ffecd65e2a1ae9f5c3b1f5e6948e2353d620	N/A
.objects[].sixgill_posttitle	Indicator Attribute	Sixgill Post Title	.objects[].valid_from	sqli dumper 10.2 2020	N/A
.objects[].sixgill_source	Indicator Attribute	Sixgill Source	.objects[].valid_from	forum_demonforums	N/A
.objects[].revoked	Indicator Attribute	False Positive	.objects[].valid_from	Flase	N/A
.objects[].labels[]	Indicator Attribute	Label	.objects[].valid_from	malware	N/A
.objects[].sixgill_post_virustotallink	Indicator Attribute	VirusTotal Link	.objects[].valid_from	https://virustotal.com/#/file/e436924a2fac62b5d...	N/A
.objects[].external_reference[].positive_rate	Indicator Attribute	VirusTotal Positive Rate	.objects[].valid_from	low	Applicable only when .source_name is 'VirusTotal'
.objects[].sixgill_actor	Adversary Name	N/A	.objects[].valid_from	meisami2015	N/A
.objects[].external_reference[].mitre_attack_tactic_id + mitre_attack_tactic	TTP Value	N/A	N/A	TA0024 - Build Capabilities	Applicable only when .source_name is 'mitre-attack'

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.objects[].external_reference[].mitre_attack_technique_id	TTP Attribute	Technique ID	N/A	T1346	N/A
.objects[].external_reference[].mitre_attack_technique	TTP Attribute	Technique Name	N/A	Obtain/re-use payloads	N/A
.objects[].external_reference[].mitre_attack_technique_url	TTP Attribute	Technique External Reference	N/A	https://attack.mitre.org/techniques/T1346/	N/A
.objects[].external_reference[].mitre_attack_tactic_id	TTP Attribute	Tactic ID	N/A	TA0024	N/A
.objects[].external_reference[].mitre_attack_tactic	TTP Attribute	Tactic Name	N/A	Build Capabilities	N/A
.objects[].external_reference[].mitre_attack_tactic_url	TTP Attribute	Tactic External Reference	N/A	https://attack.mitre.org/tactics/TA0024/	N/A

Average Run Time

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

Metric	Result
Run Time	7 minutes
Indicators	2,001
Indicator Attributes	30,248
Adversaries	65
Attack Patterns	2
TTP Attributes	21

Change Log

Version	Details
1.0.2	Update support for MITRE Attack Patterns.
1.0.1	Fixed filter error during ingestion
1.0.0	Initial Release