ThreatQuotient

Sixgill Darkfeed Implementation Guide

Version 1.0.0

Saturday, September 19, 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.

Last Updated: Saturday, September 19, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.34.0`

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 feed:

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

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **Sixgill Darkfeed** integration file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed file on your local machine

   

   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.

   The feeds will be added to the **Commercial** tab for Incoming Feeds. You will still need to configure and then enable the feed.

Configuration

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. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **Commercial** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
API ID	The Sixgill API ID.
API Key	The Sixgill API Key.

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

The connector is installed under the **Commercial** category.

ThreatQ Mapping

Sixgill Darkfeed

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

The end points used by this feed are as follows:

- POST `https://api.cybersixgill.com/auth/token` - returns the data about the authorization token.

```
{
    "access_token”: "123456789",
    "expires_in": 28800,
    "refresh_expires_in": 86400,
    "refresh_token": "123456789",
    "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` - returns a bundle of 2000 IOCs (indicators of compromise - darkfeed threat intelligence items)


```
{
    "created": "2020-05-15T12:10:28.942Z",
    "description": "Malware available for download from file-sharing sites",
    "external_reference": [
        {
                "positive_rate": "low",
                "source_name": "VirusTotal",
                "url": "https://virus-
total.com/#/file/923c0221f827c32a01a142b5ff68a90bbdf76226b8df7b02b72524e02a887635"
        },
        {
            "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--97e6f2f8-58f1-4b4c-bb8f-0bab1d65dbbe",
    "labels": [
        "malicious-activity",
        "malware",
        "Build Capabilities",
        "Obtain/re-use payloads"
    ],
    "lang": "en",
    "modified": "2020-05-15T12:10:28.942Z",
    "object_marking_refs": [
        "marking-definition--41eaaf7c-0bc0-4c56-abdf-d89a7f096ac4",
        "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
    ],
    "pattern": "[url:value = 'https://anonfile.com/bcqfn7ydoa/sqli_dumper_10.1_zip']",
    "sixgill_actor": "meisami2015",
    "sixgill_confidence": 80,
    "sixgill_feedid": "darkfeed_010",
    "sixgill_feedname": "malware_download_urls",
    "sixgill_post_virustotallink":
```

```
"https://virustotal.com/#/file/e436924a2fac62b5df8e77b588ce8e3f8c23075e1367c6c53fbca70ff3107e42",
    "sixgill_postid": "9528ffecd65e2a1ae9f5c3b1f5e6948e2353d620",
    "sixgill_posttitle": "sqli dumper 10.2 2020",
    "sixgill_severity": 80,
    "sixgill_source": "forum_demonforums",
    "spec_version": "2.0",
    "type": "indicator",
    "valid_from": "2020-05-11T18:40:00Z"
}
```

- 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
```

Default Mapping Table

ThreatQ provides the following default mapping for this feed:

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[].de-`	Indicator	N/A	N/A	'Malware available for download from file-sharing	N/A

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
`scription`	Description			sites'	
`.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
`.objects[].sixgill_postid`	Indicator Attribute	Sixgill Post ID	.objects[].valid_	'9528ffecd65e2a1ae9f5c3b1f5e6948e2353d620'	N/A

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
			from		
`.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_	'https://virustotal.com/#/file/e436924a2fac62b5d...'	N/A

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
			from		
`.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'
`.objects[].external_reference`	TTP Attribute	Technique ID	N/A	'T1346'	N/A

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
`[].mitre_attack_technique_id`					
`.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`	TTP Attribute	Tactic Name	N/A	'Build Capabilities'	N/A

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
`[].mitre_attack_tactic`					
`.objects[].external_reference[].mitre_attack_tactic_url`	TTP Attribute	Tactic External Reference	N/A	'https://attack.mitre.org/tactics/TA0024/'	N/A

Average Feed Run

Average Feed Run results for Sixgill Darkfeed:

Metric	Result
Run Time	7 minutes
Indicators	2,212
Indicator Attributes	28,198
Adversaries	635
TTPs	4
TTPs Attributes	21

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.

Change Log

- **Version 1.0.0**
  - Initial release