ThreatQuotient

BitDefender Advanced Threat Intelligence CDF

Version 2.0.0

June 03, 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	2.0.0
Compatible with ThreatQ Versions	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

BitDefender Advanced Threat Intelligence is a security service that enables security professionals to make more informed decisions by providing real-time threat knowledge that can be easily integrated in their existing technology stack. The solution delivers up-to-date, contextual intelligence on URLs, IPs, domains, certificates, files, Command and Control servers and Advanced Persistent Threats to Security Operation Centers (SOCs), Managed Security Service Providers (MSSPs), Managed Detection & Response (MDR) companies, IT security and investigation consultancies and large enterprises that need to block ingenious threats.

The integration provides the following feeds:

- **BitDefender APTs** - ingests STIX 2.0 threat intelligence about APT.
- **BitDefender C2 Servers** - ingests STIX 2.0 threat intelligence about Command and Control servers.
- **BitDefender Phishing And Fraud** - ingests STIX 2.0 threat intelligence about phishing and frauds.
- **BitDefender Ransomware** - ingests STIX 2.0 threat intelligence about ransomware events.
- **BitDefender Mobile** - ingests STIX 2.0 threat intelligence about mobile malware.
- **BitDefender Malicious Domains** - ingests STIX 2.0 threat intelligence about domains associated with malware.
- **BitDefender Malicious IPs** - ingests STIX 2.0 threat intelligence about IPs associated with any threat.
- **BitDefender Malicious URLs** - ingests STIX 2.0 threat intelligence about URLs associated with any threat.
- **BitDefender Malicious Filehashes** - ingests STIX 2.0 threat intelligence about file hashes associated with any threat.
- **BitDefender File Reputations** - ingests real-time reputation information on malicious file hashes captured from the live sensors.
- **BitDefender Web Reputations** - ingests real-time reputation information on malicious URLs and domains captured from the live sensors.
- **BitDefender IP Reputations** - ingests real-time reputation information on malicious IPs captured from the live sensors.
- **BitDefender Vulnerability Extended Reputations** - ingests information about known vulnerabilities and CVEs along with real world sensor data, such as associated vulnerable files and exploits.

The integration ingests the following system objects:

- Adversary
- Identity
- Indicators
- Malware
- Report
- Signatures
- Vulnerabilities

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 integration yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the file on your local machine
6. Select the individual feeds to install, when prompted, and click **Install**.

The feed(s) will be added to the integrations page. You will still need to configure and then enable the feed(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 **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	The API key to be used when authenticating to BitDefender Threat Intelligence service.
Timespan	The time frame for which content will be ingested. Options include: ◦ Latest day of data in the feed ◦ Latest 18 hours of data in the feed ◦ Latest 12 hours of data in the feed ◦ Latest 6 hours of data in the feed
Include Aggressive Detection *BitDefender File Reputations feed only*	Enable this parameter to include additional entries that resulted from processes known to have a higher rate of false positive.
Related IoCs Filter *BitDefender File Reputations, Web Reputations, and IP Reputations feeds only*	Select which related IoCs should be ingested into ThreatQ.
Ingest CVEs As *BitDefender Vulnerability*	Select the entity type you'd like CVEs ingested as. Options include Vulnerabilities or Indicators.

PARAMETER	DESCRIPTION
Extended Reputations feed only	
Related File Hashes Filter *BitDefender Vulnerability Extended Reputations feed only*	Select which file hash types should be ingested into ThreatQ. Options include: ◦ Vulnerable file hashes associated with the vulnerability ◦ File hashes associated with files seen exploiting this vulnerability in the wild

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.

ThreatQ Mapping

BitDefender APTs

The BitDefender APTs feed ingests STIX 2.0 threat intelligence about APT.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=APTs
```

Sample Request Parameters

```
{
  "timespan": "1d",
  "format": "STIX2.0"
}
```

Sample Response:


```
{"type":"bundle","id":"bundle--f9525f38-a1b8-446a-
b2ce-483ccb128f72","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--5ff3b043-73f9-4584-
bc8b-1e5b11d63676","created":"2019-12-17T21:49:47.000Z","modified":"2024-05-15T
03:32:08.000Z","labels":["malicious-activity"],"name":"file-
e186e7d3cd02842...","pattern":"[file:hashes.MD5 =
'891b6298656d2806622aee050006d2ce'] OR [file:hashes.'SHA-1' =
'7567e3bc659dc66ce29915ce8e2b0e6ef6e9dff5'] OR [file:hashes.'SHA-256' =
'e186e7d3cd028420d8da6e46785cc13bb7d26544eba8e23d40a23b2886b5a7cd']","valid_fro
m":"2024-05-15T03:32:08.000Z","valid_until":"2124-04-21T03:32:08.000Z","kill_ch
ain_phases":[{"kill_chain_name":"mitre-attack","phase_name":"defense-evasion"},
{"kill_chain_name":"mitre-
attack","phase_name":"discovery"}],"x_popularity":2}]}
{"type":"bundle","id":"bundle--87cb7269-715c-44b9-
acf5-96cd15360057","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--b3e4493c-a75a-40f4-
a270-1821a23dd53e","created":"2018-02-24T14:23:12.000Z","modified":"2024-04-30T
22:35:37.000Z","labels":["malicious-
activity"],"name":"file-32b2a1bbfbcac53...","pattern":"[file:hashes.MD5 =
'a882db04c4a75aaff220ffedb23e0f39'] OR [file:hashes.'SHA-1' =
'67b076b2e5c67f69b5a536f23721d8461974b2d7'] OR [file:hashes.'SHA-256' =
'32b2a1bbfbcac53cb6b10c6b05ec2996834da6f3b2d149ebeaca92936383dd85']","valid_fro
m":"2024-04-30T22:35:37.000Z","valid_until":"2124-04-06T22:35:37.000Z","kill_ch
ain_phases":[{"kill_chain_name":"mitre-attack","phase_name":"defense-
evasion"}]}]}
```


The mapping for this feed is handled by the native ThreatQ STIX 2 parser. Attributes: `Valid Until`, `Valid From` and `Modified At` are updated at ingestion.

BitDefender C2 Servers

The BitDefender C2 Servers feed ingests STIX 2.0 threat intelligence about Command and Control servers.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=C2-servers
```

Sample Request Parameters

```
{
  "timespan": "1d",
  "format": "STIX2.0"
}
```

Sample Response:


```
{"type":"bundle","id":"bundle--49fa6c62-d1f6-4b4b-
acf0-8066a90bb632","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--787ec721-b03d-4a51-ae63-
d540656ce6cd","created":"2022-05-04T13:30:21.000Z","modified":"2024-05-17T11:28
:11.000Z","labels":["malicious-
activity"],"name":"ip-104.255.152.61","pattern":"[ipv4-addr:value =
'104.255.152.61']","valid_from":"2024-05-17T11:28:11.000Z","valid_until":"2024-
06-10T11:28:11.000Z","kill_chain_phases":[{"kill_chain_name":"mitre-
attack","phase_name":"impact"}],"x_popularity":1}]}
{"type":"bundle","id":"bundle--1c7104f5-4a84-4403-87ac-
ec0a25621594","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--a0e79f7b-
c0b8-4601-9a00-56b73112fe00","created":"2023-12-18T08:44:50.000Z","modified":"2
024-05-17T11:28:09.000Z","labels":["malicious-
activity"],"name":"domain-0djedia.duckd...","pattern":"[domain-name:value =
'0djedia.duckdns.org']","valid_from":"2024-05-17T11:28:09.000Z","valid_until":"
2024-06-10T11:28:09.000Z","kill_chain_phases":[{"kill_chain_name":"mitre-
attack","phase_name":"impact"}],"x_popularity":1}]}
```


The mapping for this feed is handled by the native ThreatQ STIX 2 parser. Attributes: `Valid Until`, `Valid From` and `Modified At` are updated at ingestion.

BitDefender Phishing and Fraud

The BitDefender Phishing and Fraud feed ingests STIX 2.0 threat intelligence about phishing and frauds.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=Phishing-and-Fraud
```

Sample Request parameters:

```
{
  "timespan": "1d",
  "format": "STIX2.0"
}
```

Sample Response:


```
{"type":"bundle","id":"bundle--78167e5f-9172-428e-8298-
e04ed76d9539","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--a32ea428-0df0-43e5-ab87-
ea335ee0a446","created":"2024-04-30T22:37:25.000Z","modified":"2024-04-30T22:37
:25.000Z","labels":["malicious-activity"],"name":"file-
ca586a07743e210...","pattern":"[file:hashes.MD5 =
'5db1aa94d1f984d7cf70530340087a76'] OR [file:hashes.'SHA-1' =
'7aa0c053668f7cdac690f87deb3bb8f7f1440543'] OR [file:hashes.'SHA-256' =
'ca586a07743e210e2326c2fec2ef6526ca7046ea9f4fa7edd2e14916e6315cc8']","valid_fro
m":"2024-04-30T22:37:25.000Z","valid_until":"2124-04-06T22:37:25.000Z"}]}
{"type":"bundle","id":"bundle--0357da6a-c7d7-472c-a90c-
f78ef475b62d","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--87a9e7b0-6203-4da2-
b7e2-411e525df580","created":"2024-05-17T11:57:18.000Z","modified":"2024-05-17T
11:57:18.000Z","labels":["malicious-activity"],"name":"domain-
c2x9y3.broked...","pattern":"[domain-name:value =
'c2x9y3.brokedownbodymoshpitmind.com']","valid_from":"2024-05-17T11:57:18.000Z"
,"valid_until":"2024-05-19T11:57:18.000Z"}]}
```


The mapping for this feed is handled by the native ThreatQ STIX 2 parser. Attributes: `Valid Until`, `Valid From` and `Modified At` are updated at ingestion.

BitDefender Ransomware

The BitDefender Ransomware feed ingests STIX 2.0 threat intelligence about ransomware events.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=Ransomware
```

Sample Request Parameters:

```
{
  "timespan": "1d",
  "format": "STIX2.0"
}
```

Sample Response:


```
{"type":"bundle","id":"bundle--515eabaa-b66c-4777-
bbfe-1c2e9db174c8","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--d406a921-3503-4e4c-99c6-
a568948032d6","created":"2023-08-24T13:57:29.000Z","modified":"2024-05-17T11:58
:26.000Z","labels":["malicious-
activity"],"name":"ip-181.119.125.226","pattern":"[ipv4-addr:value =
'181.119.125.226']","valid_from":"2024-05-17T11:58:26.000Z","valid_until":"2024
-05-24T11:58:26.000Z"},{"type":"report","id":"report--c48ad3ae-cc18-4a98-b794-
e29ba9955bda","name":"BDk22jxk6r","x_threat_version":1,"x_threat_confidence":85
,"labels":["threat-report","severity-
critical"],"created":"2023-08-30T21:26:31.000Z","modified":"2023-08-30T21:26:31
.000Z","published":"2023-08-30T21:26:31.000Z","object_refs":["indicator--
d406a921-3503-4e4c-99c6-a568948032d6"]}]}
{"type":"bundle","id":"bundle--
fea6c3bb-1b18-4833-9337-07013b53fbb1","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--a70a0fd4-6f0e-4372-
b761-4e98c5666864","created":"2023-12-06T13:35:26.000Z","modified":"2024-05-17T
11:18:06.000Z","labels":["malicious-
activity"],"name":"ip-200.111.8.30","pattern":"[ipv4-addr:value =
'200.111.8.30']","valid_from":"2024-05-17T11:18:06.000Z","valid_until":"2024-05
-24T11:18:06.000Z"},{"type":"report","id":"report--380b61f8-9acd-4b59-9aec-
e6ad25b9d5d6","name":"BDmr5r7kdd","x_threat_version":1,"x_threat_confidence":85
,"labels":["threat-report","severity-
critical"],"created":"2023-12-06T13:35:26.000Z","modified":"2023-12-06T13:35:26
.000Z","published":"2023-12-06T13:35:26.000Z","object_refs":["indicator--
a70a0fd4-6f0e-4372-b761-4e98c5666864"]}]}
```


The mapping for this feed is handled by the native ThreatQ STIX 2 parser. Attributes: `Valid Until`, `Valid From` and `Modified At` are updated at ingestion.

BitDefender Mobile

The BitDefender Mobile feed ingests STIX 2.0 threat intelligence about mobile malware.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=Mobile
```

Sample Request Parameters:

```
{
  "timespan": "1d",
  "format": "STIX2.0"
}
```

Sample Response:


```
{"type":"bundle","id":"bundle--3810d753-
a604-45de-8d20-825a7d553ca1","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--fcc8b7fa-28d2-40e7-8e4f-
fce6d2748414","created":"2024-05-17T11:49:53.000Z","modified":"2024-05-17T11:49
:53.000Z","labels":["malicious-activity"],"name":"file-
a242afc9e107388...","pattern":"[file:hashes.MD5 =
'cc212953d6f34b587a13024e84556ae6'] OR [file:hashes.'SHA-1' =
'8b0e300f437940f939977a1a28360c354a2b343e'] OR [file:hashes.'SHA-256' =
'a242afc9e107388cdfe8c1788d291e44d3a876c2ee12128d0fd2b197bfc14bc0']","valid_fro
m":"2024-05-17T11:49:53.000Z","valid_until":"2124-04-23T11:49:53.000Z","kill_ch
ain_phases":[{"kill_chain_name":"mitre-attack","phase_name":"execution"},
{"kill_chain_name":"mitre-attack","phase_name":"defense-
evasion"}],"x_popularity":1}]}
{"type":"bundle","id":"bundle--3fd0a001-7b25-46e8-bf72-
a310903a8df6","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--e5a72b89-d44b-4a64-9ea0-
f87b20902ea4","created":"2024-05-17T11:50:06.000Z","modified":"2024-05-17T11:50
:06.000Z","labels":["malicious-activity"],"name":"file-
ed1d745a15d6dd2...","pattern":"[file:hashes.MD5 =
'82d984ceb3369faaca25ac42e740acb6'] OR [file:hashes.'SHA-1' =
'416c1846d74b81ff3b979216fe364ba3851acb09'] OR [file:hashes.'SHA-256' =
'ed1d745a15d6dd22fc446d1420a6c0376a577f025c094c979ca25aee668a9fd4']","valid_fro
m":"2024-05-17T11:50:06.000Z","valid_until":"2124-04-23T11:50:06.000Z","kill_ch
ain_phases":[{"kill_chain_name":"mitre-attack","phase_name":"execution"},
{"kill_chain_name":"mitre-attack","phase_name":"defense-
evasion"}],"x_popularity":1}]}
```


The mapping for this feed is handled by the native ThreatQ STIX 2 parser. Attributes: `Valid Until`, `Valid From` and `Modified At` are updated at ingestion.

BitDefender Malicious Domains

The BitDefender Malicious Domains feed ingests STIX 2.0 threat intelligence about domains associated with malware.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=Malicious-domains
```

Sample Request Parameters:

```
{
  "timespan": "1d",
  "format": "STIX2.0"
}
```

Sample Response:


```
{"type":"bundle","id":"bundle--54958a9f-5505-4618-9f4d-
a29642631eb6","spec_version":"2.0","objects":
[{"type":"identity","id":"identity--4fd65920-ae6e-419f-86c5-
a9130e2ed678","created":"2019-07-23T02:57:11.000Z","modified":"2019-07-23T02:57
:11.000Z","labels":["country"],"identity_class":"class","name":"FR"},
{"type":"identity","id":"identity--484bab16-920e-4fac-a22e-
f07769034882","created":"2019-07-23T02:57:11.000Z","modified":"2019-07-23T02:57
:11.000Z","labels":["country"],"identity_class":"class","name":"RO"}]}
{"type":"bundle","id":"bundle--c329030c-
a34e-45c2-85c1-811eccff9de3","spec_version":"2.0","objects":
[{"type":"report","id":"report--46ca8b74-32bc-4021-
a395-7b72f84e3961","name":"BD8aikgw4h","x_threat_version":1,"x_threat_confidenc
e":97,"labels":["threat-report","severity-
dangerous"],"created":"2024-05-17T05:59:38.000Z","modified":"2024-05-17T05:59:3
8.000Z","published":"2024-05-17T05:59:38.000Z","object_refs":["indicator--
b23be89b-5b6c-4549-9831-7d24bd66b405"]}]}
```


The mapping for this feed is handled by the native ThreatQ STIX 2 parser. Attributes: `Valid Until`, `Valid From` and `Modified At` are updated at ingestion.

BitDefender Malicious IPs

The BitDefender Malicious IPs feed ingests STIX 2.0 threat intelligence about IPs associated with any threat.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=Malicious-IPs
```

Sample Request Parameters:

```
{
  "timespan": "1d",
  "format": "STIX2.0"
}
```

Sample Response:


```
{"type":"bundle","id":"bundle--cdcdf7b9-87ef-4dce-a75e-
efbf18392d78","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--25ba73f6-e608-4922-b51d-
f8d712808d1e","created":"2024-02-07T18:26:53.000Z","modified":"2024-05-17T08:59
:48.000Z","labels":["malicious-
activity"],"name":"ip-79.110.62.75","pattern":"[ipv4-addr:value =
'79.110.62.75']","valid_from":"2024-05-17T08:59:48.000Z","valid_until":"2024-05
-24T08:59:48.000Z","x_popularity":5},
{"type":"report","id":"report--55015568-82db-49c0-8f9b-
c9d22dddebe9","name":"BDnnfs4gt5","x_threat_version":1,"x_threat_confidence":81
,"labels":["threat-report","severity-
critical"],"created":"2024-02-12T15:08:55.000Z","modified":"2024-02-12T15:08:55
.000Z","published":"2024-02-12T15:08:55.000Z","object_refs":
["indicator--25ba73f6-e608-4922-b51d-f8d712808d1e"]}]}
{"type":"bundle","id":"bundle--4d3a583e-
a5e5-4d17-91e0-546e9aef4b70","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--c6a63e1c-8486-4d5e-97e2-
a1d6c1e2183a","created":"2023-01-03T17:17:06.000Z","modified":"2024-05-17T08:59
:48.000Z","labels":["malicious-
activity"],"name":"ip-147.78.47.8","pattern":"[ipv4-addr:value =
'147.78.47.8']","valid_from":"2024-05-17T08:59:48.000Z","valid_until":"2024-05-
24T08:59:48.000Z","x_popularity":5},{"type":"report","id":"report--
d4db76d3-9443-4b6d-8e00-4ce332a05bee","name":"BDv358yolf","x_threat_version":24
,"x_threat_confidence":81,"labels":["threat-report","severity-
critical"],"created":"2023-01-04T06:56:45.000Z","modified":"2023-01-04T06:56:45
.000Z","published":"2023-01-04T06:56:45.000Z","object_refs":["indicator--
c6a63e1c-8486-4d5e-97e2-a1d6c1e2183a"]}]}
```


The mapping for this feed is handled by the native ThreatQ STIX 2 parser. Attributes: `Valid Until`, `Valid From` and `Modified At` are updated at ingestion.

BitDefender Malicious URLs

The BitDefender Malicious URLs feed ingests STIX 2.0 threat intelligence about URLs associated with any threat.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=Malicious-URLs
```

Sample Request Parameters:

```
{
  "timespan": "1d",
  "format": "STIX2.0"
}
```

Sample Response:


```
{"type":"bundle","id":"bundle--c7a8891e-1128-49f2-
ad13-7f67eb4b9cb7","spec_version":"2.0","objects":
[{"type":"indicator","id":"indicator--f1491df5-799a-4e4a-
ad3c-29ab84a7c6d9","created":"2024-05-17T11:57:12.000Z","modified":"2024-05-17T
11:57:12.000Z","labels":["malicious-activity"],"name":"url-crm.ipaqme.com/
a...","pattern":"[url:value = 'crm.ipaqme.com/admin/
authentication']","valid_from":"2024-05-17T11:57:12.000Z","valid_until":"2024-0
5-19T11:57:12.000Z"}]}
{"type":"bundle","id":"bundle--43140a8c-a3b1-4643-9870-
e12ea4430759","spec_version":"2.0","objects":
[{"type":"report","id":"report--02a33064-aae6-46f8-9f88-
e89e3c2b6fb5","name":"BDdm6oxg74","x_threat_version":1,"x_threat_confidence":99
,"labels":["threat-report","severity-
suspicious"],"created":"2024-05-17T11:55:52.000Z","modified":"2024-05-17T11:55:
52.000Z","published":"2024-05-17T11:55:52.000Z","object_refs":
["indicator--8683544e-88f2-492d-89cf-a772eda8b7e5"]}]}
```


The mapping for this feed is handled by the native ThreatQ STIX 2 parser. Attributes: `Valid Until`, `Valid From` and `Modified At` are updated at ingestion.

BitDefender Malicious Filehashes

The BitDefender Malicious Filehashes feed ingests STIX 2.0 threat intelligence about file hashes associated with any threat.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=Malicious-filehashes
```

Sample Request Parameters:

```
{
  "timespan": "1d",
  "format": "STIX2.0"
}
```

Sample Response:


```
{"id":"bundle--94a68b7a-9534-4048-bcfd-1d42afc8a787","objects":
[{"created":"2024-04-30T22:37:51.000Z","id":"indicator--19c4ba4e-6ee8-46fa-83a3
-583c90f9e1f8","labels":["malicious-
activity"],"modified":"2024-04-30T22:37:51.000Z","name":"file-112cdcf377715d8..
.","pattern":"[file:hashes.MD5 = '5b3b6aaeaab771f115c7d7780f713416'] OR
[file:hashes.'SHA-1' = 'e048cc40ef7282968a7ce2ad4c7e1de7db50c232'] OR
[file:hashes.'SHA-256' =
'112cdcf377715d86e41c3f8bf3ec362f913fd0e04dab964293b209f53cf95380']","type":"in
dicator","valid_from":"2024-04-30T22:37:51.000Z","valid_until":"2124-04-06T22:3
7:51.000Z"}],"spec_version":"2.0","type":"bundle"}
{"id":"bundle--66f4d067-05fe-4e2d-b24d-1191e845ed6d","objects":
[{"created":"2024-04-22T05:32:20.000Z","id":"indicator--f84dd1c9-
f684-4b73-83e1-f5d2be7d5851","kill_chain_phases":[{"kill_chain_name":"mitre-
attack","phase_name":"discovery"}],"labels":["malicious-
activity"],"modified":"2024-04-30T22:35:13.000Z","name":"file-817795232683c57..
.","pattern":"[file:hashes.MD5 = 'ceea1f2b4b862defa976354cc7e20c4d'] OR
[file:hashes.'SHA-1' = 'fecf2f2ff42d6354b3617786ad6c39481aa8e9e0'] OR
[file:hashes.'SHA-256' =
'817795232683c5775e4067256de2697db9835d249bf28e8dc3329e28e1eb375c']","type":"in
dicator","valid_from":"2024-04-30T22:35:13.000Z","valid_until":"2124-04-06T22:3
5:13.000Z"}],"spec_version":"2.0","type":"bundle"}
```


The mapping for this feed is handled by the native ThreatQ STIX 2 parser. Attributes: `Valid Until`, `Valid From` and `Modified At` are updated at ingestion.

BitDefender File Reputations

The BitDefender File Reputations feed ingests real-time reputation information on malicious file hashes captured from the live sensors.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=file-reputation
```

Sample Request Parameters:

```
{
  "from": 1715212800,
  "to": 1715277600,
  "include_aggressive_detection": "true"}
```

Sample Response:


```
{"sha256":"6e0d3fa93de6df3f76df54f053ecfb11b60d0649c6db056c9a60a31d82519ad5","m
d5":"246d8882ba03ad85152d86b6540b0112","sha1":"4067515bd5b97332870355b925671c47
ae57a94a","file_format":"Windows
executable","file_size":3584,"popularity":3,"confidence":80,"file_names":
[],"threat_name":"Gen:Trojan.Heur.DLP.aq4@aGBltti","threat_family":"Malware","f
irst_seen":1507600762,"timestamp":1715644803,"TTL":94608000}
{"sha256":"c140c00c02e112777b9d5bf896728a8a7d9309074a5a9839750b8af1902f7464","m
d5":"2ab887c902b2b4649e75a2695135a7f5","sha1":"4c30433872462a433070c8f90c8a1e87
d20e5db2","file_format":"Windows
executable","file_size":3584,"popularity":3,"confidence":80,"file_names":
[],"threat_name":"Gen:Trojan.Heur.DLP.aq4@aOrBuoo","threat_family":"Malware","f
irst_seen":1521081707,"timestamp":1715644803,"TTL":94608000}
{"sha256":"1371c603eea2638d995d381e0b54a7ec09072d55d29e791fb1ee0f0b936bbedc","m
d5":"2fc64a102ec39d23d53d9add8810c89f","sha1":"775f8f9157b0b89524f40fd6dda72296
93e2cbdb","file_format":"Windows
shortcut","file_size":187,"popularity":3,"confidence":65,"file_names":
["pureleadssvc.exe"],"threat_name":"Trojan.LNK.Gen.4","threat_family":"Malware"
,"first_seen":1713454775,"timestamp":1715644804,"TTL":94608000}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.sha256	Indicator.Value	SHA-256	.first_seen	6e0d3fa93de6df3f76df54f053ecfb11b60d0649c6db056c9a60a31d82519ad5	N/A
.sha1	Indicator.Value	SHA-1	.first_seen	4067515bd5b97332870355b925671c47ae57a94a	N/A
.md5	Indicator.Value	MD5	.first_seen	2fc64a102ec39d23d53d9add8810c89f	N/A
.popularity	Indicator.Attribute	Popularity	.first_seen	3	Updated at ingestion
.TTL	Indicator.Attribute	Time to live (seconds)	.first_seen	94608000	Updated at ingestion
.confidence	Indicator.Attribute	Confidence	.first_seen	80	Updated at ingestion
.threat_name	Indicator.Attribute	Threat Name	.first_seen	Gen:Trojan.Heur.DLP.aq4@aGBltti	N/A
.file_size	Indicator.Attribute	File Size	.first_seen	3584	N/A
.file_format	Indicator.Attribute	File Format	.first_seen	Windows executable	N/A
.threat_family	Indicator.Attribute	Threat Family	.first_seen	Malware	N/A
.file_names	Related Indicator.Value	Filename	.first_seen	pureleadssvc.exe	If enabled in `Related IoCs Filter`

BitDefender Web Reputation

The BitDefender Web Reputation feed ingests real-time reputation information on malicious URLs and domains captured from the live sensors.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=web-reputation
```

Sample Request parameters:

```
{
  "from": 1715212800,
  "to": 1715277600
  }
```

Sample Response:


```
{"url":"ehhai.info","type":"domain","first_seen":1715644800,"host_ips":
[],"countries":[],"timestamp":1715644800,"TTL":172800,"threat_types":
["phishing"],"popularity":1,"flags":["website_unreachable"]}
{"url":"restore4uads.com","type":"domain","first_seen":1705630336,"host_ips":
[],"countries":[],"timestamp":1715644800,"TTL":172800,"threat_types":
["phishing"],"popularity":1}
{"url":"guidebyexpert.com/best-telescopes/
0.5882180688110357","type":"url","first_seen":1715644801,"host_ips":
["172.67.209.62","104.21.93.110","167.206.37.137","136.226.19.151","2606:4700:3
032::ac43:a621"],"countries":
["US"],"timestamp":1715644801,"TTL":1209600,"threat_types":
["malware"],"popularity":1}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.url	Indicator.Value	URL/FQDN	.first_seen	ehhai.info	N/A
.popularity	Indicator.Attribute	Popularity	.first_seen	1	Updated at ingestion
.TTL	Indicator.Attribute	Time to live (seconds)	.first_seen	172800	Updated at ingestion
.threat_types	Indicator.Attribute	Threat Type	.first_seen	Phishing	Title cased
.countries	Indicator.Attribute	Country Code	.first_seen	US	N/A
.flags	Indicator.Attribute	Website Unreachable	.first_seen	True	True if `website_unreachable` in `.flags` else False
.host_ips	Related Indicator.Value	IP Address/IPv6 Address	.first_seen	172.67.209.62	If enabled in `Related IoCs Filter`

BitDefender IP Reputations

The BitDefender IP Reputations feed ingests real-time reputation information on malicious IPs captured from the live sensors.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=ip-reputation
```

Sample Request Parameters:

```
{
  "from": 1715212800,
  "to": 1715277600
}
```

Sample Response:

```
{"ip":"2a02:4780:1e:3d64:7ced:5a7c:4f73:e03d","first_seen":1715450400,"timestamp":1715450401,"TTL":604800,"severity":30,"confidence":30,"type":"ipv6","asn":47583,"countries":["US"],"domains":["crackwatcher.com"],"flags":["indirect_verdict"],"popularity":1}
{"ip":"154.220.96.215","first_seen":1715450408,"timestamp":1715450408,"TTL":604800,"severity":30,"confidence":30,"type":"ipv4","popularity":1,"flags":["indirect_verdict","cloud_provider"]}
{"ip":"154.220.96.214","first_seen":1715450410,"timestamp":1715450411,"TTL":604800,"severity":40,"confidence":50,"type":"ipv4","popularity":1,"ports":["80","1880"],"protocols":["HTTP"],"tags":["Malware"]}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip	Indicator.Value	IP Address/IPv6 Address	.first_seen	2a02:4780:1e:3d64 :7ced:5a7c:4f73:e03d	N/A
.popularity	Indicator.Attribute	Popularity	.first_seen	1	Updated at ingestion
.severity	Indicator.Attribute	Severity	.first_seen	30	Updated at ingestion
.confidence	Indicator.Attribute	Confidence	.first_seen	30	Updated at ingestion
.TTL	Indicator.Attribute	Time to live (seconds)	.first_seen	604800	Updated at ingestion
.ports	Indicator.Attribute	Port	.first_seen	80	N/A
.protocols	Indicator.Attribute	Protocol	.first_seen	HTTP	N/A
.countries	Indicator.Attribute	Country Code	.first_seen	US	N/A
.flags	Indicator.Attribute	Is Cloud Provider	.first_seen	True	Always True. Present only if `cloud_provider` in `.flags`.
.flags	Indicator.Attribute	Indirect Verdict	.first_seen	True	True if `indirect_verdict` in `.flags` else False. Updated at ingestion
.domains	Related Indicator.Value	FQDN	.first_seen	crackwatcher.com	If enabled in `Related IoCs Filter`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.asn	Related Indicator.Value	ASN	.first_seen	47583	If enabled in `Related IoCs Filter`

BitDefender Vulnerability Extended Reputations

The BitDefender Vulnerability Extended Reputations feed ingests information about known vulnerabilities and CVEs along with real world sensor data, such as associated vulnerable files and exploits.

```
GET https://feeds.ti.bitdefender.com/reputation?feed_name=vulnerabilities-extended
```

Sample Request Parameters:

```
{
  "from": 1715212800,
  "to": 1715277600
}
```

Sample Response:


```
{"cve":"CVE-2012-1723","publish_datetime":"2012-06-16 21:55:00","product_name":
["Jdk","Jre"],"product_category":"Application","vendor_name":
["Oracle"],"description":"Unspecified vulnerability in the Java Runtime
Environment (JRE)...","CVSS_score":{"v3":10.0},"CPE_list":
["cpe:2.3:a:oracle:jre:*:update4:*:*:*:*:*:*","cpe:2.3:a:sun:jre:*:update35:*:*
:*:*:*:*"],"references":[{"url":"http://www.oracle.com/technetwork/topics/
security/javacpujun2012-1515912.html","name":"http://www.oracle.com/
technetwork/topics/security/
javacpujun2012-1515912.html","refsource":"CONFIRM","tags":["Vendor
Advisory"]}],"vulnerable_file_hashes":
[{"md5":"232a562b71fb17c06bbe72c11181e7d4","sha256":"9476fe1896669163248747785f
a053aca7284949945abd37c59dae4184760d58","sha1":"4a8ba46820a4e36e77eccebf13b7fed
a833f5681"},"exploit_file_hashes":
[{"threat_name":"Java.Exploit.CVE-2012-1723.S","last_seen":1715180417,"md5":"9e
024c00aa43eec5d937334652656eb4","sha256":"8562865c9d3ef2fefd9b5b00364fcc161141c
aa9c315a62610b09dc76bd733f6","sha1":"5c968e8aeb2d9eda8ad7b5b11365e7a822d169af",
"popularity":1}],"solution_description":"It is recommended to update the
software to the newest version available"}
{"cve":"CVE-2012-0158","publish_datetime":"2012-04-10 21:55:00","product_name":
["Sql_Server","Visual_Foxpro"],"product_category":"Application","vendor_name":
["Microsoft"],"description":"The (1) ListView, (2) ListView2, (3) TreeView, and
(4) TreeView2 ActiveX controls ...","security_risks":["Execute Unauthorized
Code or Commands"],"CVSS_score":{"v2":9.3},"CPE_list":
["cpe:2.3:a:microsoft:visual_basic:6.0:*:runtime_extended_files:*:*:*:*:*"],"re
ferences":[{"url":"http://www.securitytracker.com/id?
1026902","name":"1026902","refsource":"SECTRACK","tags":
[]}],"vulnerable_file_hashes":[],"exploit_file_hashes":
[],"solution_description":"It is recommended to update the software to the
newest version available"}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.cve	Indicator/ Vulnerability.Value	CVE	.publish_datetime	CVE-2012-1723	Depends on user config `Ingest CVEs As`
.description, .solution_ description, .CPE_list, references	Indicator/ Vulnerability.Description	N/A	.publish_datetime	Unspecified vulnerability...	Fields are concatenated
.product_name	Indicator/ Vulnerability.Attribute	Affected Product	.publish_datetime	Jdk	All _ are removed
.product_category	Indicator/ Vulnerability.Attribute	Affected Product Category	.publish_datetime	Application	N/A
.vendor_name	Indicator/ Vulnerability.Attribute	Affected Vendor	.publish_datetime	Oracle	N/A
.CVSS_score.v2	Indicator/ Vulnerability.Attribute	CVSSv2 Base Score	.publish_datetime	9.3	Updated at ingestion
.CVSS_score.v3	Indicator/ Vulnerability.Attribute	CVSSv30 Base Score	.publish_datetime	10.0	Updated at ingestion
.references[].url	Indicator/ Vulnerability.Attribute	External Reference	.publish_datetime	http://www.oracle.com/ technetwork/topics/secu rity/javacpujun2012-151 5912.html	N/A
.security_risks[]	Indicator/ Vulnerability.Attribute	Security Risk	.publish_datetime	Execute Unauthorized Code or Commands	N/A
.vulnerable_file_ hashes[].md5	Related Indicator.Value	MD5	.last_seen	232a562b71fb17c06bbe 72c11181e7d4	If enabled in `Related File Hashes Filter`
.vulnerable_file_ hashes[].sha1	Related Indicator.Value	SHA-1	.last_seen	4a8ba46820a4e36e77ecce bf13b7feda833f5681	If enabled in `Related File Hashes Filter`
.vulnerable_file_ hashes[].sha256	Related Indicator.Value	SHA-256	.last_seen	9476fe189666916324874 7785fa053aca7284949945 abd37c59dae4184760d58	If enabled in `Related File Hashes Filter`
.exploit_file_ hashes[].md5	Related Indicator.Value	MD5	.last_seen	9e024c00aa43eec5d9373 34652656eb4	If enabled in `Related File Hashes Filter`
.exploit_file_ hashes[].sha1	Related Indicator.Value	SHA-1	.last_seen	5c968e8aeb2d9eda8ad7b5 b11365e7a822d169af	If enabled in `Related File Hashes Filter`
.exploit_file_ hashes[].sha256	Related Indicator.Value	SHA-256	.last_seen	8562865c9d3ef2fefd9b5b00 364fcc161141caa9c315a626 10b09dc76bd733f6	If enabled in `Related File Hashes Filter`
.exploit_file_ hashes[].popularity	Related Indicator.Attribute	Popularity	.last_seen	1	Updated at ingestion
.exploit_file_ hashes[].threat_name	Related Indicator.Attribute	Threat Name	.last_seen	Java.Exploit.CVE-2012-1723.S	N/A

Average Feed Run

> 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.

BitDefender APTs

METRIC	RESULT
Run Time	1 hour 55 minutes
Indicators	16,800
Indicator Attributes	76,525
Adversaries	450
Adversary Attributes	6,805
Identity	231
Identity Attributes	6,709
Malware	825
Malware Attributes	5,710
Report	1,633
Report Attributes	4,812
Signatures	5,727

METRIC	RESULT
Signature Attributes	26,017

BitDefender C2 Servers

METRIC	RESULT
Run Time	3 minutes
Indicators	1,110
Indicator Attributes	6,352
Adversaries	104
Adversary Attributes	455
Identity	27
Identity Attributes	465
Malware	39
Malware Attributes	467
Report	340
Report Attributes	1,020
Signatures	423
Signature Attributes	2,390

BitDefender Phishing and Fraud

METRIC	RESULT
Run Time	1 hour 8 minutes
Indicators	11,530
Indicator Attributes	48,073
Adversaries	84
Adversary Attributes	255
Identity	148
Identity Attributes	1,431
Malware	208
Malware Attributes	1,210
Report	370
Report Attributes	1,110
Signatures	4,044
Signature Attributes	16,827

BitDefender Ransomware

METRIC	RESULT
Run Time	2 minutes
Indicators	803
Indicator Attributes	3,974
Adversaries	56
Adversary Attributes	605
Identity	85
Identity Attributes	520
Malware	87
Malware Attributes	464
Report	94
Report Attributes	282
Signatures	289
Signature Attributes	1,410

BitDefender Mobile

METRIC	RESULT
Run Time	8 minutes
Indicators	3,980
Indicator Attributes	22,790
Adversaries	104
Adversary Attributes	455
Identity	113
Identity Attributes	2,424
Malware	273
Malware Attributes	2,005
Report	1,264
Report Attributes	3,790
Signatures	1,400
Signature Attributes	7,995

BitDefender Malicious Domains

METRIC	RESULT
Run Time	5 minutes
Indicators	590
Indicator Attributes	2,423
Adversaries	93
Adversary Attributes	468
Identity	176
Identity Attributes	2,583
Malware	11
Malware Attributes	200
Report	538
Report Attributes	1,595
Signatures	590
Signature Attributes	2,423

BitDefender Malicious IPs

METRIC	RESULT
Run Time	3 minutes
Indicators	635
Indicator Attributes	2,580
Adversaries	104
Adversary Attributes	455
Identity	28
Identity Attributes	235
Malware	20
Malware Attributes	180
Report	745
Report Attributes	2,210
Signatures	635
Signature Attributes	2,581

BitDefender Malicious URLs

METRIC	RESULT
Run Time	2 minutes
Indicators	70
Indicator Attributes	280
Adversaries	104
Adversary Attributes	455
Identity	10
Identity Attributes	32
Malware	13
Malware Attributes	60
Report	54
Report Attributes	162
Signatures	70
Signature Attributes	280

BitDefender Malicious Filehashes

METRIC	RESULT
Run Time	2 minutes
Indicators	70
Indicator Attributes	280
Adversaries	104
Adversary Attributes	455
Identity	10
Identity Attributes	32
Malware	13
Malware Attributes	60
Report	54
Report Attributes	162
Signatures	70
Signature Attributes	280

BitDefender File Reputations

METRIC	RESULT
Run Time	1 hour
Indicators	55,300
Indicator Attributes	350,500

BitDefender Web Reputations

METRIC	RESULT
Run Time	20 minutes
Indicators	40,200
Indicator Attributes	114,000

BitDefender IP Reputations

METRIC	RESULT
Run Time	1 hour 20 minutes
Indicators	165,100
Indicator Attributes	478,900

BitDefender Vulnerability Extended Reputations

METRIC	RESULT
Run Time	2 minutes
Indicators	803
Indicator Attributes	3,974
Adversaries	56
Adversary Attributes	605
Identity	85
Identity Attributes	520
Malware	87
Malware Attributes	464
Report	94
Report Attributes	282
Signatures	289
Signature Attributes	1,410

Known Issues / Limitations

- The API Endpoint used by the reputation feeds (`BitDefender Vulnerability Extended Reputations`, `BitDefender File Reputations`, `BitDefender Web Reputations`, `BitDefender IP Reputations`) allows only timestamps aligned to 6h timeframes for up to 24h for every request. Additionally, timestamps older than 7 days are not allowed. Due to this API limitation the feeds will only use the end date of the feed run and request data from the last 24/18/12/6 hours (depending on the user field `Timespan`). The since date of the feed run is not used at all.

Change Log

- **Version 2.0.0**
  - Updated the integration to use ThreatQ Intelligence API v3.8 endpoints. These endpoints replace the previous endpoints used by the integration.
  - The integration can now ingest signatures, identities, reports, adversaries and malware in addition to indicators and vulnerabilities.
  - Added a new entry to the Known Issues / Limitations chapter regarding API timeframe limitations.
  - Updated the minimum ThreatQ version to 5.12.0
  - Updated the support tier to ThreatQ Supported.
- **Version 1.0.0**
  - Initial release