ThreatQuotient

VirusTotal LiveHunt CDF Guide

Version 2.1.2

February 06, 2023

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	2.1.2
Compatible with ThreatQ Versions	>= 4.43.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/virustotal-livehunt-feed

Introduction

The VirusTotal LiveHunt CDF ingests and enriches Incident type Events and related indicators into your ThreatQ platform from your VirusTotal LiveHunt environment.

> ⚠ ThreatQ recommends using this integration in conjunction with VirusTotal LiveHunt Operation. The Operation will push YARA Signatures from ThreatQ to VirusTotal LiveHunt, and the CDF will ingest data related to each signature from VirusTotal LiveHunt back into ThreatQ.

The integration provides the following endpoint:

- **VirusTotal LiveHunt** - ingests incident type Events that can be enriched with attributes and related Indicators.

The integration ingests the following system object types:

- Events
  - Event Attributes
- Indicators

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 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

   > 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 integrations page.

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 integration-related credentials.

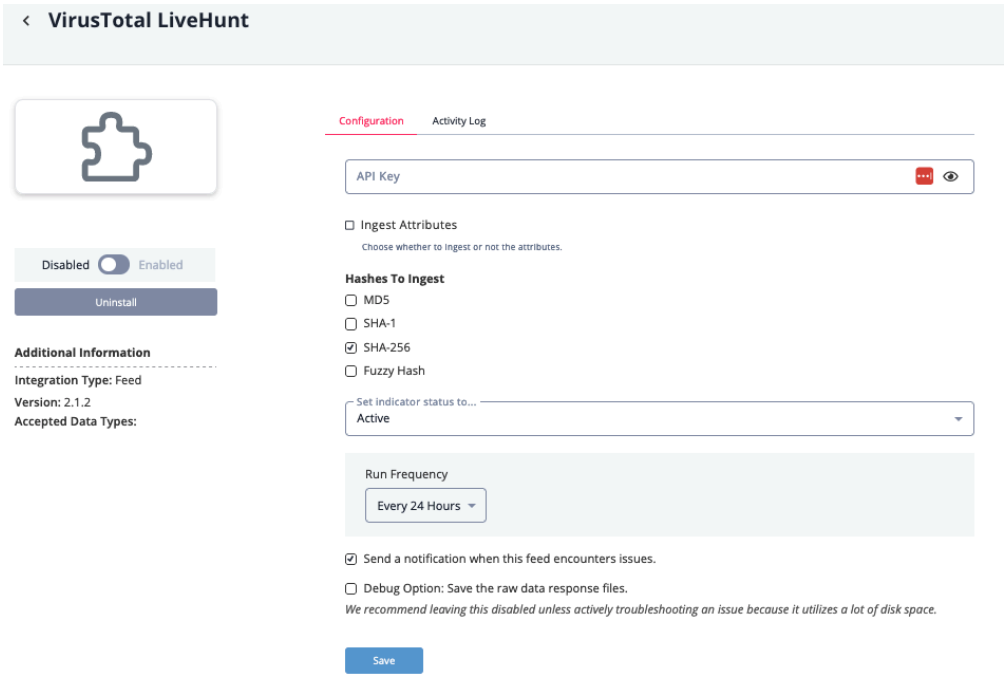
To configure the integration:

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 parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your VirusTotal LiveHunt API Key to be used in HTTP headers for accessing feed data.
Ingest Attributes	Enabling this parameter will result in the integration ingesting attributes.
Hashes to Ingest	Select which hashes to ingest. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256 (default) ◦ Fuzzy Hash



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

VirusTotal LiveHunt

The VirusTotal LiveHunt feed creates and enriches incident type events with attributes and related indicators.

```
GET https://www.virustotal.com/api/v3/intelligence/hunting_notification_files
```

Sample Response:


```
{
  "meta": {
    "count": 200,
    "cursor": "CsABChEKBGRhdGUSCQjM15--
xoD9AhKmAWoRc352aXJ1c3RvdGFsY2xvdWRykAELEhNIdW50aW5nTm90aWZpY2F0aW9uInc4OTU5ODUyNzc2LTljZTQxM2RlYjcwNDJmZWRlMDgxNzk2M
GI5MzlmYTRiLTY2MWU0MDA4YzkyZTllYjI3ZTVlYmM3OTEyNDQzODBkZjFkZWY5ODBjNjE0Yzc0ZmIzOTkxNGE2YTgxMmJjMWYtMTY3NTY3NDQ1OAwYAC
AB"
  },
  "data": [
    {
      "attributes": {
        "type_description": "Android",
        "tlsh": "T19D472206B71C992EC873A0B25D5B22BA11591D51AE43FB97B809334C34F7BE44B4EBC9",
        "vhash": "d0720ca6cf2701b262b4f63438410e1e",
        "exiftool": {
          "ZipRequiredVersion": "0",
          "MIMEType": "application/zip",
          "ZipCRC": "0xa8a745df",
          "FileType": "ZIP",
          "ZipCompression": "Deflated",
          "ZipUncompressedSize": "95124",
          "ZipCompressedSize": "15413",
          "FileTypeExtension": "zip",
          "ZipFileName": "AndroidManifest.xml",
          "ZipBitFlag": "0",
          "ZipModifyDate": "1981:01:01 01:01:02"
        },
        "trid": [
          {
            "file_type": "Android Package",
            "probability": 45
          },
          {
            "file_type": "Java Archive",
            "probability": 15.7
          },
          {
            "file_type": "Pocket Code/Catroid Catrobat Project",
            "probability": 12.8
          },
          {
            "file_type": "Sweet Home 3D design (generic)",
```

```
            "probability": 12.2
          },
          {
            "file_type": "Mozilla Archive Format (gen)",
            "probability": 8.1
          }
        ],
        "names": [],
        "last_modification_date": 1675682579,
        "type_tag": "android",
        "times_submitted": 1,
        "total_votes": {
          "harmless": 0,
          "malicious": 0
        },
        "size": 25542461,
        "type_extension": "apk",
        "last_submission_date": 1675680601,
        "reputation": 0,
        "downloadable": true,
        "crowdsourced_ids_stats": {
          "high": 0,
          "info": 1,
          "medium": 0,
          "low": 1
        },
        "sha256": "21c5e05926f5507422018876605cedb94bc33985cdf71791c64fa6cbed76a688",
        "tags": [
          "apk",
          "android",
          "obfuscated",
          "runtime-modules",
          "reflection",
          "telephony",
          "detect-debug-environment",
          "checks-gps"
        ],
        "crowdsourced_ids_results": [
          {
            "rule_category": "protocol-command-decode",
            "alert_severity": "low",
            "rule_msg": "(stream_tcp) data sent on stream after TCP reset sent",
            "rule_raw": "alert ( gid:129; sid:8; rev:2; msg:\"(stream_tcp) data sent on stream after TCP reset
sent\"; metadata: policy max-detect-ips drop, rule-type preproc; classtype:protocol-command-decode;)",
            "alert_context": [
              {
                "src_ip": "31.13.71.1",
                "src_port": 443
              }
            ],
            "rule_url": "https://www.snort.org/downloads/#rule-downloads",
            "rule_source": "Snort registered user ruleset",
            "rule_id": "129:8"
          },
          {
            "rule_category": "Potential Corporate Privacy Violation",
            "alert_severity": "info",
            "rule_msg": "ET INFO Android Device Connectivity Check",
            "rule_raw": "alert http $HOME_NET any -> $EXTERNAL_NET any (msg:\"ET INFO Android Device Connectivity
Check\"; flow:established,to_server; urilen:13; http.method; content:\"GET\"; http.uri; content:\"/generate_204\";
fast_pattern; endswith; http.host; content:\"connectivitycheck.gstatic.com\"; http.accept_enc; content:\"gzip\";
```

```
depth:4; endswith; http.header_names; content:!\"Cache\"; content:!\"Referer\"; classtype:policy-violation;
sid:2036220; rev:3; metadata:affected_product Android, attack_target Mobile_Client, created_at 2018_09_14, deployment
Perimeter, deployment Internal, former_category POLICY, performance_impact Low, signature_severity Minor, tag
Connectivity_Check, updated_at 2020_09_16;)",
            "alert_context": [
              {
                "url": "http://connectivitycheck.gstatic.com/generate_204",
                "hostname": "connectivitycheck.gstatic.com",
                "dest_ip": "108.177.119.94",
                "dest_port": 80
              }
            ],
            "rule_url": "https://rules.emergingthreats.net/",
            "rule_source": "Proofpoint Emerging Threats Open",
            "rule_id": "1:2036220"
          }
        ],
        "last_analysis_date": 1675680601,
        "unique_sources": 1,
        "first_submission_date": 1675680601,
        "sha1": "92c0302fb0b3b8f38ea672abf21edc0cc884fa0d",
        "ssdeep": "393216:6qQ+ijgqrnblIt72MfGKPWL6VLy1beU8N2tY/dNyRM/EyZj/wQLQUwc:6qQ+sgWnCQM9UimbY2u/dNyR4EyBoQ02",
        "bundle_info": {
          "highest_datetime": "1981-01-01 01:01:02",
          "lowest_datetime": "1981-01-01 01:01:02",
          "num_children": 2971,
          "extensions": {
            "xml": 605,
            "bin": 1,
            "p0": 1,
            "b": 1,
            "gif": 2,
            "j0": 1,
            "gz": 1,
            "jks": 1,
            "dex": 5,
            "s": 1,
            "w0": 1,
            "txt": 131,
            "ttf": 4,
            "png": 13
          },
          "file_types": {
            "XML": 605,
            "DEX": 5,
            "unknown": 356,
            "Java Bytecode": 1,
            "GIF": 2,
            "JSON": 17,
            "HTML": 1,
            "PNG": 13
          },
          "type": "APK",
          "uncompressed_size": 40792067
        },
        "md5": "53ce73d40657f9b10733b3125c99218d",
        "androguard": {
          "VTAndroidInfo": 2,
          "Libraries": [
            "org.apache.http.legacy",
            "androidx.window.extensions",
            "androidx.window.sidecar"
```

```
  ],
  "AndroidApplicationError": false,
  "MinSdkVersion": "21",
  "AndroguardVersion": "4.0",
  "Activities": [
    "br.com.mobills.splash.SplashScreenActivity",
    "br.com.mobills.onboarding.OnboardingWelcomeActivity",
    "br.com.mobills.onboarding.gympass.GympassOnboardingActivity",
    "br.com.mobills.onboarding.goal.OnboardingGoalActivity",
    "br.com.mobills.onboarding.signup.OnboardingSignUpActivity",
    "br.com.mobills.onboarding.signup.OnboardingSignUpSuccessActivity"
  ],
  "certificate": {
    "Subject": {
      "DN": "CN:Carlos Batista",
      "CN": "Carlos Batista"
    },
    "validto": "3011-03-09 20:45:47",
    "serialnumber": "13ebabb1",
    "thumbprint": "abb62a825040a153fb7c59cfcba8a3ee3082626d",
    "validfrom": "2012-11-05 20:45:47",
    "Issuer": {
      "DN": "CN:Carlos Batista",
      "CN": "Carlos Batista"
    }
  },
  "AndroidApplication": 1,
  "RiskIndicator": {
    "APK": {
      "DEX": 5
    },
    "PERM": {
      "INTERNET": 1,
      "INSTANT": 3,
      "NORMAL": 9,
      "PRIVACY": 3,
      "GPS": 2
    }
  },
  "Services": [
    "com.google.android.play.core.assetpacks.AssetPackExtractionService"
  ],
  "AndroidVersionCode": "783",
  "main_activity": "br.com.mobills.splash.SplashScreenActivity",
  "Package": "br.com.gerenciadorfinanceiro.controller",
  "intent_filters": {
    "Services": {
      "br.com.mobills.services.FCMService": {
        "action": [
          "com.google.firebase.MESSAGING_EVENT"
        ]
      }
    },
    "Activities": {
      "br.com.mobills.views.activities.MainActivity": {
        "action": [
          "action.mobills.main.open"
        ],
        "category": [
          "android.intent.category.DEFAULT"
        ]
```

```
        }
      },
      "Receivers": {
        "androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryNotLowProxy": {
          "action": [
            "android.intent.action.BATTERY_OKAY",
            "android.intent.action.BATTERY_LOW"
          ]
        }
    },
    "AndroidVersionName": "5.82.3",
    "TargetSdkVersion": "33",
    "AndroidApplicationInfo": "APK",
    "Providers": [
      "androidx.core.content.FileProvider",
      "com.salesforce.marketingcloud.MCInitContentProvider",
    ],
    "permission_details": {
      "android.permission.POST_NOTIFICATIONS": {
        "short_description": "Unknown permission from android reference",
        "full_description": "Unknown permission from android reference",
        "permission_type": "normal"
      }
    },
    "Receivers": [
      "br.com.mobills.services.widgets.WidgetValueBroadcast",
      "br.com.mobills.services.widgets.WidgetWithTransactionsListService",
      "br.com.mobills.services.widgets.WidgetWithoutTransactionsListService",
      "br.com.mobills.views.activities.WidgetShortcutProvider"
    ],
    "StringsInformation": [
      "http://ns.adobe.com/xap/1.0/\u0000",
      "http://schemas.android.com/apk/res/android",
    ]
  },
  "magic": "Zip archive data",
  "main_icon": {
    "raw_md5": "b0c61ce5b07caa60f5771e49ba2d34b5",
    "dhash": "d488f6e0e8e8e0c4"
  },
  "last_analysis_stats": {
    "harmless": 0,
    "type-unsupported": 10,
    "suspicious": 0,
    "confirmed-timeout": 0,
    "timeout": 1,
    "failure": 0,
    "malicious": 0,
    "undetected": 63
  },
  "last_analysis_results": {
    "Bkav": {
      "category": "undetected",
      "engine_name": "Bkav",
      "engine_version": "1.3.0.9899",
      "result": null,
      "method": "blacklist",
      "engine_update": "20230206"
    },
    "Lionic": {
      "category": "undetected",
```

```
            "engine_name": "Lionic",
            "engine_version": "7.5",
            "result": null,
            "method": "blacklist",
            "engine_update": "20230206"
          },
          "Elastic": {
            "category": "type-unsupported",
            "engine_name": "Elastic",
            "engine_version": "4.0.77",
            "result": null,
            "method": "blacklist",
            "engine_update": "20230203"
          }
        }
      },
      "type": "file",
      "id": "21c5e05926f5507422018876605cedb94bc33985cdf71791c64fa6cbed76a688",
      "links": {
        "self": "https://www.virustotal.com/api/v3/files/
21c5e05926f5507422018876605cedb94bc33985cdf71791c64fa6cbed76a688"
      },
      "context_attributes": {
        "notification_id":
"8959852776-9ce413deb7042fede0817960b939fa4b-21c5e05926f5507422018876605cedb94bc33985cdf71791c64fa6cbed76a688-1675680
601",
        "notification_source_key": "62e613b2",
        "notification_tags": [
          "banbra",
          "21c5e05926f5507422018876605cedb94bc33985cdf71791c64fa6cbed76a688",
          "banker"
        ],
        "ruleset_name": "banbra",
        "notification_source_country": "AR",
        "rule_name": "banbra",
        "notification_snippet": "00 00 72 65 73 2F 6C 61 79 6F 75 74 2F 61 63 74  ..res/layout/act\n69 76 69 74 79 5F
*begin_highlight*73 65 6E 68 61 *end_highlight*2E 78 6D 6C C5  ivity_*begin_highlight*senha*end_highlight*.xml.\n98
4F 6C 14 55 1C C7 DF CC 6E B7 BB FD BB 5B 4A  .Ol.U....n....[J\n00 00 1D 00 00 00 72 65 73 2F 6C 61 79 6F 75
74  ......res/layout\n2F 63 61 64 61 73 74 72 6F 5F *begin_highlight*73 65 6E 68 61 *end_highlight*2E  /
cadastro_*begin_highlight*senha*end_highlight*.\n78 6D 6C AD 92 3D 6F D4 30 18 C7 1F 5F AE BD 24  xml..=o.0..._..$
\n00 9C 04 00 00 1B 00 00 00 72 65 73 2F 6C 61 79  .........res/lay\n6F 75 74 2F 64 69 67 69 74 65 5F
*begin_highlight*73 65 6E 68 61*end_highlight*  out/digite_*begin_highlight*senha*end_highlight*\n2E 78 6D 6C 95 93
3D 6B 14 41 18 C7 9F B9 DD BB  .xml..=k.A......\n72 2E 78 6D 6C 00 1D 1D 72 65 73 2F 6C 61 79 6F  r.xml...res/
layo\n75 74 2F 61 63 74 69 76 69 74 79 5F *begin_highlight*73 65 6E 68*end_highlight*  ut/
activity_*begin_highlight*senh*end_highlight*\n*begin_highlight*61 *end_highlight*2E 78 6D 6C 00 20 20 72 65 73 2F 6C
61 79 6F  *begin_highlight*a*end_highlight*.xml.  res/layo\n6D 6C 00 1D 1D 72 65 73 2F 6C 61 79 6F 75 74 2F
ml...res/layout/\n63 61 64 61 73 74 72 6F 5F *begin_highlight*73 65 6E 68 61 *end_highlight*2E 78
cadastro_*begin_highlight*senha*end_highlight*.x\n6D 6C 00 1E 1E 72 65 73 2F 6C 61 79 6F 75 74 2F  ml...res/layout/
\n72 65 73 2F 6C 61 79 6F 75 74 2F 64 69 67 69 74  res/layout/digit\n65 5F *begin_highlight*73 65 6E 68 61
*end_highlight*2E 78 6D 6C 00 26 26 72 65  e_*begin_highlight*senha*end_highlight*.xml.&&re\n73 2F 6C 61 79 6F 75 74
2F 64 72 61 67 5F 69 74  s/layout/drag_it\n43 56 56 00 13 13 43 61 64 61 73 74 72 61 72 20  CVV...Cadastrar \n73 75
61 20 *begin_highlight*73 65 6E 68 61 *end_highlight*00 19 19 43 61 69 78  sua
*begin_highlight*senha*end_highlight*...Caix\n61 20 61 70 70 20 6F 72 20 77 65 62 73 69 74 65  a app or website\n69
74 69 65 73 00 19 19 43 6F 6D 6F 20 63 61 64  ities...Como cad\n61 73 74 72 61 72 20 75 6D 61 20 *begin_highlight*73
65 6E 68 61*end_highlight*  astrar uma *begin_highlight*senha*end_highlight*\n3F 00 1C 1D 43 6F 6D 6F 20 66 61 7A 65
72 20 75  ?...Como fazer u\n6D 65 20 64 6F 20 6F 62 6A 65 74 69 76 6F 00 1F  me do objetivo..\n1F 44 69 67 69 74 65
20 73 75 61 20 *begin_highlight*73 65 6E 68*end_highlight*  .Digite sua
*begin_highlight*senh*end_highlight*\n*begin_highlight*61 *end_highlight*20 70 61 72 61 20 63 6F 6E 74 69 6E 75 61 72
*begin_highlight*a*end_highlight* para continuar\n07 07 4C 65 69 73 75 72 65 00 0D 0D 4C 65 6D
62  ..Leisure...Lemb\n72 61 72 20 *begin_highlight*73 65 6E 68 61 *end_highlight*00 47 47 4C 65 6D 62  rar
*begin_highlight*senha*end_highlight*.GGLemb\n72 65 2D 73 65 20 64 65 20 72 65 67 69 73 74 72  re-se de
```

```
registr\n\n...",
        "ruleset_id": "8959852776",
        "rule_tags": [
          "banker"
        ],
        "notification_date": 1675684215,
        "match_in_subfile": false
      }
    }
  ]
  "links": {
    "self": "https://www.virustotal.com/api/v3/users/EnglishLFC/hunting_notification_files?count_limit=200&limit=10",
    "next": "https://www.virustotal.com/api/v3/users/EnglishLFC/hunting_notification_files?
cursor=CsABChEKBGRhdGUSCQjM15--
xoD9AhKmAWoRc352aXJ1c3RvdGFsY2xvdWRykAELEhNIdW50aW5nTm90aWZpY2F0aW9uInc4OTU5ODUyNzc2LTljZTQxM2RlYjcwNDJmZWRlMDgxNzk2M
GI5MzlmYTRiLTY2MWU0MDA4YzkyZTllYjI3ZTVlYmM3OTEyNDQzODBkZjFkZWY5ODBjNjE0Yzc0ZmIzOTkxNGE2YTgxMmJjMWYtMTY3NTY3NDQ1OAwYAC
AB&count_limit=200&limit=10"
  }
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].context_attributes.ruleset_name	Event.Attribute	Ruleset Name	.data[].attributes.first_submission_date	'banker'	The attributes will only be ingested if the user select this option
.data[].context_attributes.notification_source_country	Event.Attribute	Source Country	.data[].attributes.first_submission_date	'US'	The attributes will only be ingested if the user select this option
.data[].attributes.magic	Event.Attribute	Magic	.data[].attributes.first_submission_date	'Dalvik dex file version 035'	The attributes will only be ingested if the user select this option
.data[].attributes.meaningful_name	Event.Attribute	Meaningful Name	.data[].attributes.first_submission_date	'classes.dex'	The attributes will only be ingested if the user select this option
.data[].attributes.reputation	Event.Attribute	Reputation	.data[].attributes.first_submission_date	'0'	The attributes will only be ingested if the user select this option
.data[].attributes.trid.file_type	Event.Attribute	File Type	.data[].attributes.first_submission_date	'Dalvik Dex class'	The attributes will only be ingested if the user select this option
.data[].attributes.trid.probability	Event.Attribute	Probability	.data[].attributes.first_submission_date	'100'	The attributes will only be ingested if the user select this option
.data[].attributes.type_description	Event.Attribute	Description Type	.data[].attributes.first_submission_date	'Android'	The attributes will only be ingested if the user select this option
.data[].attributes.type_tag	Event.Attribute	Tag Type	.data[].attributes.first_submission_date	'android'	The attributes will only be ingested if the user select this option
.data[].attributes.exiftool.FileTypeExtension	Event.Attribute	File Extension	.data[].attributes.first_submission_date	'DEX'	The attributes will only be ingested if the user select this option

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.last_analysis_results.(key).result	Event.Attribute	(key) Analysis Result	.data[].attributes.first_submission_date	'Unsafe'	The name of this attribute is dynamically set with the value found on (key). We only add this attribute if the value is not null.
.data[].attributes.md5	Related.Indicator	MD5	.data[].attributes.first_submission_date	'52c5d34ffcf797f5d8de9fb8ae9120c8'	N/A
.data[].attributes.sha1	Related.Indicator	SHA-1	.data[].attributes.first_submission_date	'552eb372553ee115b88714180513da44cce748da'	N/A
.data[].attributes.sha256	Related.Indicator	SHA-256	.data[].attributes.first_submission_date	'8775216e22c6501fc65042c8c3a984fce0c20b27bdd17c28493c2318d7bb5cc9'	N/A
.data[].attributes.ssdeep	Related.Indicator	Fuzzy Hash	.data[].attributes.first_submission_date	'49152:vaMqTZeWWZsKWQfg+sbwUt1pdV/eTETEmvHNgyjkGKeQU6/7knE5KS:iMooTsAmMoHe7beQES'	N/A
.data[].context_attributes.rule_name	Event.Type	Incident	.data[].attributes.first_submission_date	'banbra'	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.

VirusTotal LiveHunt

METRIC	RESULT
Run Time	2 minutes
Events	1
Event Attributes	333
Indicators	6

Known Issues / Limitations

- Due to the limitation in the API, the manual run will fetch all the data - not just the one for the selected interval.

Change Log

- **Version 2.1.2**
  - Added a new configuration parameter, **Hashes to Ingest**, that allows you to filter which hashes to ingest into the ThreatQ platform.
- **Version 2.1.1**
  - Added data ingestion safeguards. The integration will now check if certain data is present in the JSON response before processing it in order to prevent errors if the feed data is not present.
- **Version 2.1.0**
  - Added the ability to perform a manual run.
  - Added new issue to Known Issues / Limitations chapter.
- **Version 2.0.1**
  - Fixed an issue where indicators were not ingested into the ThreatQ platform.
- **Version 2.0.0**
  - The integration now ingests Incident type Events objects instead of Signatures. The ingestion of Malware types has also been removed from the integration.
  - Added a new configuration parameter that allows users to select whether or not to ingest attributes.
- **Version 1.1.0**
  - Fixed issue for objects that were not being ingested.
- **Version 1.0.0**
  - Initial release