ThreatQuotient

Netskope CDF Guide

Version 1.0.0

June 10, 2025

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	>= 5.29.0
Third-Party Compatibility	Netskope Platform
Support Tier	ThreatQ Supported

Introduction

The Netskope CDF integration ingests Netskope alerts into the ThreatQ platform.

The integration provides the following feeds:

- **Netskope - Policy Alerts** - ingests Netskope alerts of type Policy.
- **Netskope - CTEP Alerts** - ingests Netskope alerts of type Client Traffic Exploitation Protection.
- **Netskope - DLP Alerts** - ingests Netskope alerts of type DLP.
- **Netskope - Malsite Alerts** - ingests Netskope alerts of type Malsite.
- **Netskope - UBA Alerts** - Ingests Netskope alerts of type User Behavior Analytics.
- **Netskope - Compromised Credential Alerts** - ingests Netskope alerts of type Compromised Credentials.
- **Netskope - Malware Alerts** - ingests Netskope alerts of type Malware.
- **Netskope - Quarantine Alerts** - ingests Netskope alerts of type Quarantine.
- **Netskope - Remediation Alerts** - ingests Netskope alerts of type Remediation.
- **Netskope - Security Assessment Alerts** - ingests Netskope alerts of type Security Assessment.
- **Netskope - Watchlist Alerts** - ingests Netskope alerts of type Watchlist.
- **Netskope - Content Alerts** - ingests Netskope alerts of type Content.
- **Netskope - Device Alerts** - ingests Netskope alerts of type Device.

The integration ingests the following object types:

- Events
- Identities
- Indicators
- Malware

Prerequisites

The integration requires the following:

- A Netskope instance.
- A Netskope API v2 token with read permissions for the following endpoints:
  - /api/v2/events/dataexport/alerts/policy
  - /api/v2/events/dataexport/alerts/ctep
  - /api/v2/events/dataexport/alerts/dlp
  - /api/v2/events/dataexport/alerts/malsite
  - /api/v2/events/dataexport/alerts/uba
  - /api/v2/events/dataexport/alerts/compromisedcredential
  - /api/v2/events/dataexport/alerts/malware
  - /api/v2/events/dataexport/alerts/quarantine
  - /api/v2/events/dataexport/alerts/remediation
  - /api/v2/events/dataexport/alerts/securityassessment
  - /api/v2/events/dataexport/alerts/watchlist
  - /api/v2/events/dataexport/alerts/content
  - /api/v2/events/dataexport/alerts/device

See the following Netskope topic for more information: https://docs.netskope.com/en/rest-api-v2-overview.

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**.

   > 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 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:

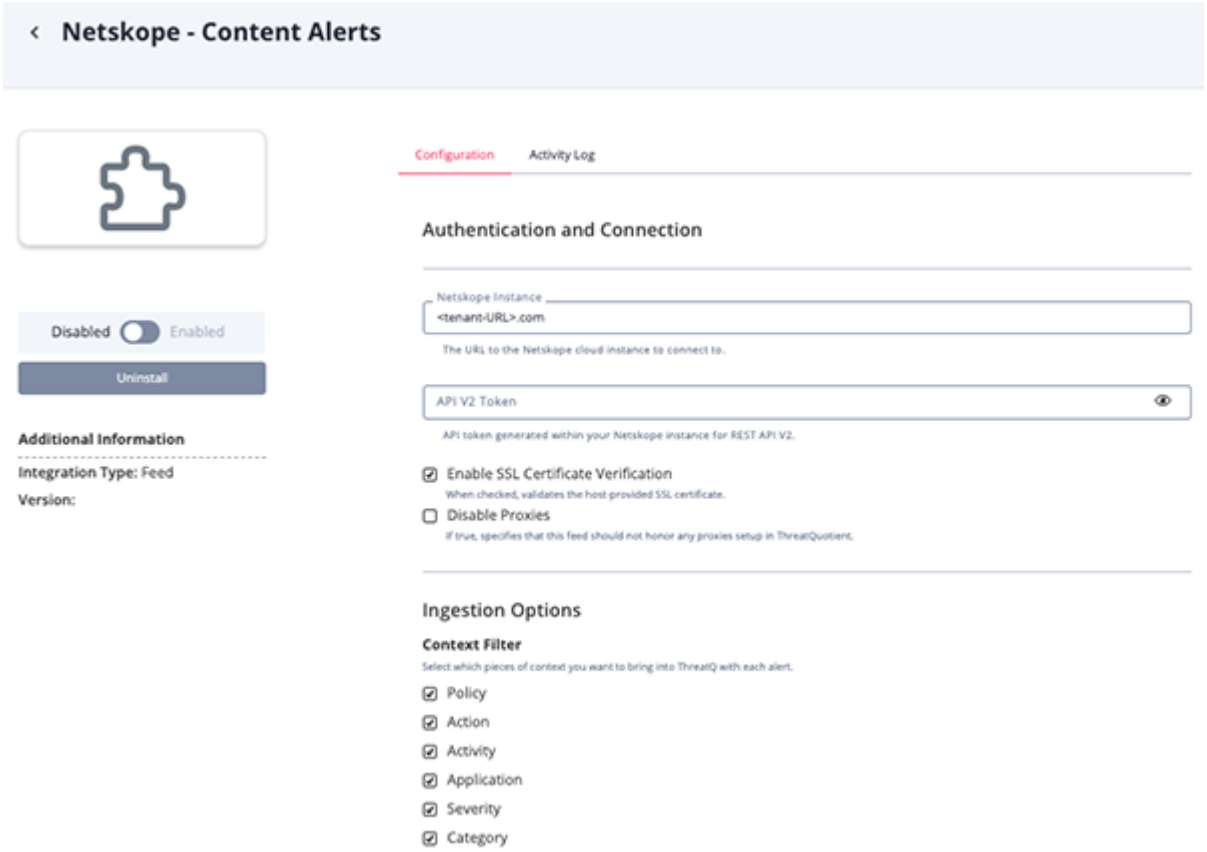
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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 parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Netskope Instance	Enter the URL to the Netskope cloud instance.
API v2 Token	Enter the API token generated within your Netskope instance for REST API V2. > Confirm that the token used in this field has the appropriate endpoint permissions. See the Prerequisites section for more details.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Context Filter	Select which pieces of context to bring into ThreatQ with each alert. Options include:

PARAMETER	DESCRIPTION
	◦ Policy *(Default)* ◦ Action *(Default)* ◦ Activity *(Default)* ◦ Application ◦ Severity *(Default)* ◦ Category *(Default)* ◦ Alert Type ◦ Attack Severity ◦ Impact Flag ◦ Service ◦ Type ◦ Browser ◦ Netskope Cloud Confidence Index ◦ Netskope Cloud Confidence Level ◦ Device ◦ Operating System ◦ Application Suite ◦ Access Method ◦ Traffic Type ◦ Application Category ◦ Total Events ◦ DLP Rule ◦ DLP Rule Severity ◦ Score ◦ Anomaly Type
Relationship Filter	Select the relationships to include with each event. Options include: ◦ Destination IP ◦ Source IP ◦ User ◦ File ◦ Malware



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

All Feeds

All the endpoints have a very similar responses.

Netskope - Policy Alerts

The Netskope - Policy Alerts feed ingests Netskope alerts of type Policy.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/policy`

Netskope - CTEP Alerts

The Netskope - CTEP Alerts feed ingests Netskope alerts of type Client Traffic Exploitation Protection.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/ctep`

Netskope - DLP Alerts

The Netskope - DLP Alerts feed ingests Netskope alerts of type DLP.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/dlp`

Netskope - Malsite Alerts

The Netskope - Malsite Alerts feed ingests Netskope alerts of type Malsite.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/malsite`

Netskope - UBA Alerts

The Netskope - UBA Alerts feed ingests Netskope alerts of type User Behavior Analytics.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/uba`

Netskope - Compromised Credential Alerts

The Netskope - Compromised Credential Alerts feed ingests Netskope alerts of type Compromised Credentials.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/compromisedcredential`

Netskope - Malware Alerts

The Netskope -Malware Alerts feed ingests Netskope alerts of type Malware.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/malware`

Netskope - Quarantine Alerts

The Netskope - Quarantine Alerts feed ingests Netskope alerts of type Quarantine.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/quarantine`

Netskope - Remediation Alerts

The Netskope - Remediation Alerts feed ingests Netskope alerts of type Remediation.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/remediation`

Netskope - Security Assessment Alerts

The Netskope - Security Assessment Alerts feed ingests Netskope alerts of type Security Assessment.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/securityassessment`

Netskope - Watchlist Alerts

The Netskope - Watchlist Alerts feed ingests Netskope alerts of type Watchlist.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/watchlist`

Netskope - Content Alerts

The Netskope - Content Alerts feed ingests Netskope alerts of type Content.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/content`

Netskope - Device Alerts

The Netskope - Device Alerts feed ingests Netskope alerts of type Device.

`GET https://NETSKOPE_TENANT.com/api/v2/events/dataexport/alerts/device`

Sample Request Parameters:

```
{
  "operation": 1748260115000
}
```

Sample Response:


```
{
  "ok": 1,
  "result": [
    {
      "_id": "6300b28c9b30ed621169f103",
      "access_method": "Client",
      "acked": "false",
      "action": "block",
      "activity": "Browse",
      "alert": "yes",
      "alert_name": "Block All",
      "alert_type": "policy",
      "app": "Microsoft Bing",
      "app_session_id": 4091125200856892354,
      "appcategory": "Search Engines",
      "browser": "Edge",
      "browser_session_id": 2802715152225722581,
      "browser_version": "18.19045",
      "category": "Search Engines",
      "cci": 60,
      "ccl": "medium",
      "connection_id": 8004814100032082012,
      "count": 1,
      "device": "Windows Device",
      "device_classification": "not configured",
      "dst_country": "GB",
      "dst_latitude": 51.50852966308594,
      "dst_location": "London",
      "dst_longitude": -0.12574000656604767,
```

```
      "dst_region": "England",
      "dst_timezone": "Europe/London",
      "dst_zipcode": "N/A",
      "dstip": "150.171.30.10",
      "dstport": 443,
      "hostname": "nskp-bothusers",
      "incident_id": 2082914907519519230,
      "managed_app": "no",
      "notify_template": "block_page.html",
      "organization_unit": "",
      "os": "Windows 10",
      "os_version": "Windows NT 10.0",
      "other_categories": [
        "Search Engines"
      ],
      "page": "www.bing.com",
      "page_site": "Microsoft Bing",
      "policy": "Block All",
      "policy_id": "-5891596717689204243 2025-03-06 18:28:34.584609",
      "protocol": "HTTPS/1.1",
      "request_id": 3055797198798255872,
      "severity": "unknown",
      "site": "Microsoft Bing",
      "src_country": "US",
      "src_latitude": 39.0469,
      "src_location": "Ashburn",
      "src_longitude": -77.4903,
      "src_region": "Virginia",
      "src_time": "Thu Mar  6 15:09:00 2025",
      "src_timezone": "America/New_York",
      "src_zipcode": "20149",
      "srcip": "54.88.212.123",
      "telemetry_app": "",
      "timestamp": 1741291758,
      "traffic_type": "CloudApp",
      "transaction_id": 2082914907519519230,
      "type": "nspolicy",
      "ur_normalized": "lab-manager+joeschmo@attackiq.com",
      "url": "www.bing.com/client/config",
      "user": "lab-manager+joeschmo@attackiq.com",
      "useragent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; Cortana
1.14.17.19041; 10.0.0.0.19045.5487) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/70.0.3538.102 Safari/537.36 Edge/18.19045",
      "userip": "172.16.7.76",
      "record_type": "alert",
      "http_status": "",
      "modified": 0,
      "scan_type": "",
      "dlp_fail_reason": "",
      "external_collaborator_count": 0,
```

```
    "forward_to_proxy_xau": "",
    "malware_severity": "",
    "session_duration": 0,
    "q_instance": "",
    "profile_emails": [],
    "threat_match_value": "",
    "act_user": "",
    "nsdeviceuid": "",
    "file_category": "",
    "malsite_category": [],
    "retro_scan_name": "",
    "TSS-scan": "",
    "all_policy_matches": [],
    "event_type": "",
    "mime_type": "",
    "quarantine_file_id": "",
    "sha256": "",
    "publisher_name": "",
    "client_bytes": 0,
    "file_type": "",
    "group": "",
    "threat_source_id": 0,
    "smtp_to": [],
    "server_bytes": 0,
    "num_sessions": 0,
    "cc": "",
    "manager": "",
    "object": "",
    "to_user": "",
    "malicious": "",
    "src_geoip_src": 0,
    "sfwder": "",
    "resp_cnt": 0,
    "Title": "",
    "quarantine_file_name": "",
    "tunnel_up_time": 0,
    "protocol_port": "",
    "division": "",
    "exposure": "",
    "tss_mode": "",
    "gateway": "",
    "last_name": "",
    "risk_level": "",
    "instance_id": "",
    "shared_with": "",
    "tunnel_id": "",
    "threat_match_field": "",
    "user_confidence_index": 0,
    "from_storage": "",
    "numbytes": 0,
```

```
    "malware_name": "",
    "ip_protocol": "",
    "justification_reason": "",
    "suppression_end_time": 0,
    "app_scopes": "",
    "metadata": {
      "attack-severity": [
        "high"
      ],
      "impact_flag": [
        "red"
      ],
      "policy": [
        "security-ips drop",
        "max-detect-ips drop",
        "balanced-ips drop"
      ],
      "service": [
        "http"
      ]
    },
    "file_size": 0,
    "userCountry": "",
    "bcc": "",
    "log_file_name": "",
    "object_id": "",
    "network": "",
    "dsthost": "",
    "trust_computer_checked": "",
    "total_collaborator_count": 0,
    "encrypt_failure": "",
    "activity_status": "",
    "to_storage": "",
    "data_type": "",
    "network_session_id": "",
    "serial": "",
    "start_time": "",
    "sender": "",
    "quarantine_profile": "",
    "shared_domains": "",
    "memberOf": "",
    "object_type": "",
    "access_key_id": "",
    "q_original_version": "",
    "tss_scan_failed": "",
    "conn_duration": 0,
    "publisher_cn": "",
    "server_packets": 0,
    "suppression_start_time": 0,
    "quarantine_profile_id": "",
```

```
    "total_packets": 0,
    "srcport": 0,
    "malware_id": "",
    "end_time": "",
    "owner": "",
    "q_original_filepath": "",
    "sanctioned_instance": "",
    "custom_connector": "",
    "ext_labels": [],
    "dynamic_classification": "",
    "dlp_profile": "",
    "from_object": "",
    "tunnel_type": "",
    "suppression_key": "",
    "file_id": "",
    "universal_connector": "",
    "to_object": "",
    "activity_type": "",
    "malware_type": "",
    "from_user": "",
    "dst_geoip_src": 0,
    "req_cnt": 0,
    "sessionid": "",
    "appsuite": "",
    "smtp_status": "",
    "user_tmp": "",
    "remediation_profile": "",
    "message_id": "",
    "two_factor_auth": "",
    "custom_attr": {},
    "client_packets": 0,
    "justification_type": "",
    "q_original_shared": "",
    "aggregated_user": "",
    "q_original_filename": "",
    "file_path": "",
    "parent_id": "",
    "org": "",
    "user_id": "",
    "displayName": "",
    "dlp_scan_failed": "",
    "internal_collaborator_count": 0,
    "q_admin": "",
    "sAMAccountName": "",
    "managementID": "",
    "q_app": "",
    "instance": "",
    "md5": "",
    "mail": "",
    "distinguishedName": "",
```

```
      "app_activity": "",
      "message_size": 0,
      "orignal_file_path": "",
      "referer": "",
      "sAMAccountType": "",
      "redirect_url": "",
      "object_count": 0,
      "tss-mode": "",
      "tss_fail_reason": ""
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

> See the Event Description Key Additions section for keys added the descriptions based on the alert type.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.alert_name, alert_type`	Event.Title	Alert	`.timestamp`	`Block All (policy)`	Concatenated as in the example.
`.app`	Event.Attribute	Application	`.timestamp`	`Microsoft Bing`	User-configurable.
`.policy`	Event.Attribute	Policy	`.timestamp`	`Block All`	User-configurable.
`.action`	Event.Attribute	Action	`.timestamp`	`Block`	User-configurable. Title cased.
`.activity`	Event.Attribute	Activity	`.timestamp`	`Browse`	User-configurable.
`.browser`	Event.Attribute	Browser	`.timestamp`	`Edge`	User-configurable.
`.category`	Event.Attribute	Category	`.timestamp`	`Search Engines`	User-configurable.
`.other_categories[]`	Event.Attribute	Category	`.timestamp`	`Search Engines`	User-configurable.
`.malsite_category[]`	Event.Attribute	Category	`.timestamp`	N/A	User-configurable.
`.cci`	Event.Attribute	Netskope Cloud Confidence Index	`.timestamp`	`60`	User-configurable. Updatable.
`.ccl`	Event.Attribute	Netskope Cloud Confidence Level	`.timestamp`	`Medium`	User-configurable. Title cased. Updatable.
`.device`	Event.Attribute	Device	`.timestamp`	`Windows Device`	User-configurable.
`.os`	Event.Attribute	Operating System	`.timestamp`	`Windows 10`	User-configurable.
`.severity`	Event.Attribute	Severity	`.timestamp`	`N/A`	User-configurable. Updatable.
`.type`	Event.Attribute	Type	`.timestamp`	`nspolicy`	User-configurable. Updatable.
`.alert_type`	Event.Attribute	Alert Type	`.timestamp`	`policy`	User-configurable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.metadata.attack-severity`	Event.Attribute	Attack Severity	`.timestamp`	`high`	User-configurable. Updatable.
`.metadata.impact_flag`	Event.Attribute	Impact Flag	`.timestamp`	`red`	User-configurable. Updatable.
`.metadata.policy`	Event.Attribute	Policy	`.timestamp`	`security-ips drop`	User-configurable.
`.metadata.service`	Event.Attribute	Service	`.timestamp`	`http`	User-configurable.
`.appsuite`	Event.Attribute	Application Suite	`.timestamp`	`N/A`	User-configurable.
`.access_method`	Event.Attribute	Access Method	`.timestamp`	`Client`	User-configurable.
`.traffic_type`	Event.Attribute	Traffic Type	`.timestamp`	`CloudApp`	User-configurable.
`.appcategory`	Event.Attribute	Application Category	`.timestamp`	`Search Engines`	User-configurable.
`.count`	Event.Attribute	Total Events	`.timestamp`	`1`	User-configurable. Updatable.
`.dlp_rule`	Event.Attribute	DLP Rule	`.timestamp`	`N/A`	User-configurable.
`.dlp_rule_severity`	Event.Attribute	DLP Rule Severity	`.timestamp`	`N/A`	User-configurable. Updatable.
`.score`	Event.Attribute	Score	`.timestamp`	`N/A`	User-configurable. Updatable.
`.anomaly_type`	Event.Attribute	Anomaly Type	`.timestamp`	`N/A`	User-configurable. Updatable.
`.srcip`	Event.Related Indicator.Value	IP Address	`.timestamp`	`54.88.212.123`	User-configurable.
`.dstip`	Event.Related Indicator.Value	IP Address	`.timestamp`	`150.171.30.10`	User-configurable.
`.src_country`	Event.Related Indicator.Attribute	Country Code	`.timestamp`	`US`	Attribute of `srcip`.
`.src_location`	Event.Related Indicator.Attribute	Location	`.timestamp`	`Ashburn`	Attribute of `srcip`.
`.src_region`	Event.Related Indicator.Attribute	Region	`.timestamp`	`Virginia`	Attribute of `srcip`.
`.src_zipcode`	Event.Related Indicator.Attribute	Zip Code	`.timestamp`	`20149`	Attribute of `srcip`.
`.srcport`	Event.Related Indicator.Attribute	Port	`.timestamp`	`N/A`	Attribute of `srcip`.
`.dst_country`	Event.Related Indicator.Attribute	Country Code	`.timestamp`	`GB`	Attribute of `dstip`.
`.dst_location`	Event.Related Indicator.Attribute	Location	`.timestamp`	`London`	Attribute of `dstip`.
`.dst_region`	Event.Related Indicator.Attribute	Region	`.timestamp`	`England`	Attribute of `dstip`.
`.dst_zipcode`	Event.Related Indicator.Attribute	Zip Code	`.timestamp`	`N/A`	Attribute of `dstip`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.dstport`	Event.Related Indicator.Attribute	Port	`.timestamp`	`443`	Attribute of `dstip`.
`.user`	Event.Related Identity.Value	Identity	`.timestamp`	`lab-manager+joeschmo@attackiq.com`	User-configurable.
`.sha256`	Event.Related Indicator.Value	SHA-256	`.timestamp`	`N/A`	User-configurable.
`.file_path`	Event.Related Indicator.Value	File Path	`.timestamp`	`N/A`	User-configurable.
`.file_type`	Event.Related Indicator.Attribute	File Type	`.timestamp`	`N/A`	Attribute of `.sha256` and `file_path`.
`.file_size`	Event.Related Indicator.Attribute	File Size	`.timestamp`	`N/A`	Attribute of `.sha256` and `file_path`.
`.md5`	Event.Related Indicator.Value	MD5	`.timestamp`	`N/A`	User-configurable.
`.quarantine_file_name`	Event.Related Indicator.Value	Filename	`.timestamp`	`N/A`	User-configurable.
`.destination_file_name`	Event.Related Indicator.Value	Filename	`.timestamp`	`N/A`	User-configurable.
`.destination_file_path`	Event.Related Indicator.Value	File Path	`.timestamp`	`N/A`	User-configurable.
`.malware_name`	Event.Related Malware.Value	Malware	`.timestamp`	`N/A`	User-configurable.
`.malware_severity`	Event.Related Malware.Attribute	Severity	`.timestamp`	`N/A`	Attribute of `.malware_name`.
`.malware_type`	Event.Related Malware.Attribute	Type	`.timestamp`	`N/A`	Attribute of `.malware_name`.

Event Description Key Additions

All Alert Types

The following keys are added to the event description for all alert types:

- General:
  - `.incident_id`
  - `.appsuite`
  - `.page_site`
  - `.protocol`
  - `.src_time`
  - `.type`
  - `.useragent`
  - `access_method`
  - `.traffic_type`
  - `referer`
- Application:
  - `.app`
  - `.url`
  - `.site`
  - `.page`
  - `.activity`
- User:
  - `.user`
  - `.userip`
  - `.os`
  - `.browser`
  - `.device`
  - `.from_user`
- Source (Egress):
  - `.srcip`
  - `.src_location`
  - `.src_country`
- Destination:
  - `.dstip`
  - `.dst_location`
  - `.dst_country`

DLP Type Alerts

The following keys are added to the event description for alerts of type DLP:

- `.dlp_profile`
- `.dlp_rule`
- `.dlp_rule_count`
- `.dlp_unique_count`
- `.dlp_rule_severity`
- `.dlp_file`

- `.dlp_incident_id`.

Compromised Credential Type Alerts

The following keys are added to the event description for alerts of type Compromised Credential:

- `.breach_description`
- `.matched_username`
- `.breach_date`

Malware Type Alerts

The following keys are added to the event description for alerts of type Malware:

- `.malware_name`
- `.detection_engine`

Quarantine Type Alerts

The following keys are added to the event description for alerts of type Quarantine:

- `.quarantine_file_name`
- `.owner`
- `.q_original_filename`

Remediation Type Alerts

The following keys are added to the event description for alerts of type Remediation:

- `.remediation_profile`

Content Type Alerts

The following keys are added to the event description for alerts of type Content:

- `.process_name`
- `.process_path`
- `.process_cert_subject`

Device Type Alerts

The following keys are added to the event description for alerts of type Device:

- `usb_device_name`
- `usb_device_type`
- `usb_vendor_id`

.srcip Indicator description

The following fields are added to the .srcip indicator description:

- `src_location`
- `src_region`
- `src_country`
- `src_latitude`
- `src_longitude`
- `src_timezone`

.dstip Indicator description

The following fields are added to the .dstip indicator description:

- `dst_location`
- `dst_region`
- `dst_country`

- `dst_latitude`
- `dst_longitude`
- `dst_timezone`

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.

METRIC	RESULT
Run Time	2 minutes
Indicators	56
Indicator Attributes	300
Events	168
Event Attributes	2,300
identities	1

Change Log

- **Version 1.0.0**
  - Initial release