ThreatQuotient

A Securonix Company

ExtraHop RevealX CDF

Version 1.0.0

December 01, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
ThreatQ Mapping **13**
ExtraHop RevealX Detections 13
Category Mapping Table 22
Threat Type Mapping Table 24
Tactic Mapping Table 25
Average Feed Run **26**
Change Log **27**

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: tq-support@securonix.com
Support Web: https://ts.securonix.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	>= 6.6.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ExtraHop RevealX CDF enables ThreatQ to automatically ingest high-fidelity threat intelligence and telemetry generated by ExtraHop RevealX, an advanced Network Detection and Response (NDR) platform. ExtraHop RevealX provides deep, agent-less visibility into network traffic—including encrypted traffic—using cloud-scale machine learning to identify advanced threats, anomalous behavior, and security hygiene issues in real time. By integrating detections, assets, and indicators of compromise from RevealX directly into ThreatQ, this CDF empowers security teams to enhance triage, accelerate investigations, and strengthen their response to threats across hybrid and multi-cloud environments.

The integration provides the following feed:

- **ExtraHop RevealX Detections** - retrieves, parses, and ingests ExtraHop RevealX detections, including contextual information about malicious or suspicious network activity and anomalies.

The integration ingests the following object types:

- Incidents
- Events
- Assets
- Indicators
- Attack Patterns
- Tools
- Malware

Prerequisites

The following is required in order to install and run the integration:

- A valid ExtraHop RevealX API host.
- A valid ExtraHop RevealX API Client ID.
- A valid ExtraHop RevealX API Client Secret.
- A ThreatQ instance running version 6.6.0 or later.

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 ExtraHop RevealX 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.

   > 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 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 ExtraHop to obtain API credentials for this integration.

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 **ExtraHop RevealX** integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

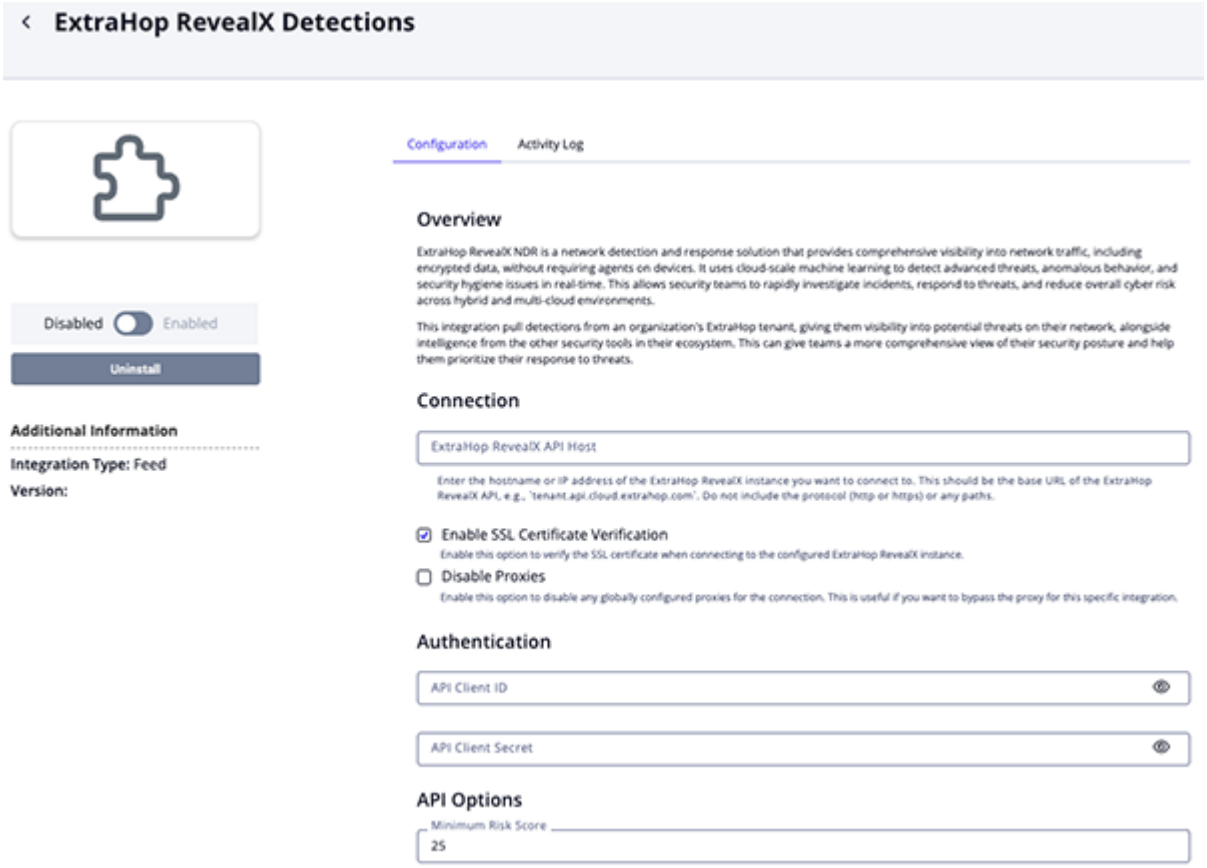
PARAMETER	DESCRIPTION
ExtraHop RevealX API Host	Enter the hostname or IP address of the ExtraHop RevealX instance to connect to with the integration. This should be the base host value only - example: `tenant.api.cloud.extrahop.com`). ⚠ Do not include the protocol (`http` or `https`) or any path segments.
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.
API Client ID	Enter the ExtraHop RevealX API Client ID used to authenticate to the ExtraHop RevealX API.
API Client Secret	Enter the ExtraHop RevealX API Client Secret associated with the configured Client ID.

PARAMETER	DESCRIPTION
Minimum Risk Score	Specify the minimum risk score a detection must have to be retrieved from the ExtraHop RevealX API. Detections with a risk score below this threshold will not be returned and will not be ingested into ThreatQ. Set this to `0` to retrieve detections regardless of risk score.
Ingest Detections As	Select the ThreatQ object type into which detections should be ingested. This allows alignment with the organization's preferred data model. Options include: • **Events (Type: Detection)** (default) • **Incidents**
Ingest the Selected Detection Participants as Assets	Select which ExtraHop detection participants should be created as Asset objects in ThreatQ. This setting enables relationships between detections and involved assets. Options include: • Internal Victim Server Devices • Internal Victim Client Devices • Internal Offender Server Devices • Internal Offender Client Devices
Ingest Asset Tags	Enable this option to apply tags to ingested Assets based on the participant's role in the detection. Tags can include values such as *victim* or *offender*, and whether the device acted as a *client* or *server*.
Ingest Categories As	Configure how ExtraHop detection categories (for example, `sec.attack`, `sec.exploit`, `perf.network`) are ingested into ThreatQ. When ingested as Attributes, values are converted to human-readable labels. When ingested as Tags, values are preserved as returned by the API. Options include: • **Attributes** (default) • **Tags**
Ingest Recommendation Factors As	Configure how detection recommendation factors (for example, `top-offender`, `critical-asset`) are ingested. These factors indicate why a detection was marked as recommended and can be used in ThreatQ for filtering and prioritization. Options include: • **Attributes** (default)

PARAMETER	DESCRIPTION
	• **Tags** (default)
Ingest CVEs As	Select how CVEs parsed from detection titles should be stored in ThreatQ. By default, CVEs are stored as Vulnerability objects. To take advantage of ThreatQ Scoring Policy, CVEs can also be ingested as Indicators (which are scorable). Options include: • **Vulnerabilities** (default) • **Indicators**
Minimum Risk Score to Ingest IOCs as Active	Specify the minimum ExtraHop risk score required for associated indicators of compromise (IOCs) to be created with the **Active** status in ThreatQ. IOCs with a risk score below this threshold are ingested with the **Review** status. The default value is `60`.
Normalize Risk Score	Enable this option to normalize the numeric ExtraHop risk score (0–100) into a human-readable attribute (for example, Low, Medium, High, Critical). The normalized value is stored in the **Normalized Risk** attribute on the Incident and supporting Indicators, allowing ThreatQ Scoring Policy to evaluate the normalized score. This parameter is disabled by default.

Custom Score Mapping	Provide a line-separated, CSV-formatted mapping that defines how numeric ExtraHop risk scores are translated into normalized values stored in the **Normalized Risk** attribute. Each row must contain three columns: *Minimum*, *Maximum*, and *Normalized Value*.
	Example (default mapping):
	`0,25,Low`
	`26,59,Medium`
	`60,89,High`
	`90,100,Critical`
	  This field is only displayed when **Normalize Risk Score** is enabled. The original ExtraHop Risk Score is always ingested in addition to the normalized value.

PARAMETER	DESCRIPTION
Add Detected Tag	Enable this option to automatically add the **detected** tag to all ingested indicators derived from ExtraHop detections. This tag is useful for filtering and searching for indicators that have been observed in the environment. This parameter is enabled by default.



5. Review any additional settings, make any changes if needed, and click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the feed.

ThreatQ Mapping

ExtraHop RevealX Detections

The ExtraHop RevealX Detections feed queries the ExtraHop API for detections and ingests them into ThreatQ as Events or Incidents, along with related assets, indicators, attack patterns, malware, and tools. The feed supports flexible mapping of categories, recommendation factors, and CVEs to align with an organization's data model and scoring policies.

```
POST https://{{ host }}/api/v1/detections/search
```

Sample Response:


```
[
  {
    "appliance_id": 6,
    "assignee": null,
    "categories": [
      "sec",
      "sec.hardening"
    ],
    "create_time": 1741137367144,
    "description": "[db1\\.i\\.rx\\.tours](https://extrahop-
bd.cloud.extrahop.com#/metrics/devices/
71c6ffe3ae8548bbbb9bf279c912d3ae.0e5dcb05abfd0000/overview?
from=1741137361interval_type=DTuntil=1753378590) established an SSL/TLS
connection with a deprecated version of SSL/TLS. SSL 2.0, SSL 3.0, and TLS 1.0
are deprecated because they are vulnerable to attacks.",
    "id": 25769804021,
    "is_user_created": false,
    "mitre_tactics": [],
    "mitre_techniques": [],
    "mod_time": 1741137370145,
    "participants": [
      {
        "endpoint": "server",
        "external": false,
        "hostname": "db1.i.rx.tours",
        "id": 7387,
        "object_id": 25769803835,
        "object_type": "device",
        "object_value": "10.1.1.39",
        "role": "offender",
        "scanner_service": null,
        "username": null
      }
    ],
    "properties": {
```

```
      "version": "TLSv1.0"
    },
    "recommended": false,
    "recommended_factors": [],
    "resolution": null,
    "risk_score": 30,
    "start_time": 1741137361379,
    "status": "new",
    "ticket_id": null,
    "title": "Deprecated SSL/TLS Versions",
    "type": "deprecated_ssl_tls_individual",
    "update_time": 1753324263134,
    "url": "https://extrahop-bd.cloud.extrahop.com/extrahop/#/detections/
detail/25769804021/?from=1741136461until=1753325163interval_type=DT"
  },
  {
    "appliance_id": 6,
    "assignee": null,
    "categories": [
      "sec",
      "sec.action",
      "sec.ransomware",
      "sec.attack"
    ],
    "create_time": 1751912454611,
    "description": "[web3\\.i\\.rx\\.tours](https://extrahop-
bd.cloud.extrahop.com#/metrics/devices/
71c6ffe3ae8548bbbb9bf279c912d3ae.0ee8eb8bc6330000/overview?
from=1751908800interval_type=DTuntil=1751914800) added new file extensions to a
remote file share over the SMB protocol. These extensions are associated with
one or more ransomware families. The number of files that were modified was
unusually high compared to past behavior for this device. Check for unexpected
file modifications or encrypted files.\n\nRansomware families linked to this
detection:\n\n* ` WannaCry `\n",
    "end_time": 1751914800000,
    "id": 25769804202,
    "is_user_created": false,
    "mitre_tactics": [
      {
        "id": "TA0040",
        "name": "Impact",
        "url": "https://attack.mitre.org/tactics/TA0040"
      }
    ],
    "mitre_techniques": [
      {
        "id": "T1486",
        "legacy_ids": [
          "T1486"
        ],
```

```
        "name": "Data Encrypted for Impact",
        "url": "https://attack.mitre.org/techniques/T1486"
      }
    ],
    "mod_time": 1751914861361,
    "participants": [
      {
        "endpoint": "client",
        "external": false,
        "id": 7665,
        "object_id": 25769803834,
        "object_type": "device",
        "role": "offender",
        "scanner_service": null,
        "username": null
      },
      {
        "endpoint": "server",
        "external": false,
        "id": 7195,
        "object_id": 25769803790,
        "object_type": "device",
        "object_value": "10.1.0.151",
        "role": "victim",
        "scanner_service": null,
        "username": null
      }
    ],
    "properties": {
      "variant": [
        "WannaCry"
      ]
    },
    "recommended": true,
    "recommended_factors": [
      "rare_type",
      "top_offender"
    ],
    "resolution": null,
    "risk_score": 83,
    "start_time": 1751908800001,
    "status": null,
    "ticket_id": null,
    "title": "Ransomware Activity",
    "type": "ransomware_activity",
    "update_time": 1751914800000,
    "url": "https://extrahop-bd.cloud.extrahop.com/extrahop/#/detections/
detail/25769804202/?from=1751907900until=1751915700interval_type=DT"
  },
  {
```

```
    "appliance_id": 6,
    "assignee": null,
    "categories": [
      "sec",
      "sec.command",
      "sec.attack"
    ],
    "create_time": 1751912996509,
    "description": "[pc1\\.i\\.rx\\.tours](https://extrahop-
bd.cloud.extrahop.com#/metrics/devices/
71c6ffe3ae8548bbbb9bf279c912d3ae.0e83fdcab6ad0000/overview?
from=1751912989interval_type=DTuntil=1751912989) sent SMB traffic that contains
a filename matching a named pipe associated with malware, attack tools, or
software that enables attacks. An attacker can hide command-and-control (C&C)
traffic within named pipes.\n\nNamed pipe linked to this detection:\n*
remcom\n\nMalware, attack tools, or software linked to this detection:\n*
RemCom",
    "end_time": 1751912989718,
    "id": 25769804210,
    "is_user_created": false,
    "mitre_tactics": [
      {
        "id": "TA0002",
        "name": "Execution",
        "url": "https://attack.mitre.org/tactics/TA0002"
      },
      {
        "id": "TA0011",
        "name": "Command and Control",
        "url": "https://attack.mitre.org/tactics/TA0011"
      }
    ],
    "mitre_techniques": [
      {
        "id": "T1071",
        "legacy_ids": [
          "T1071"
        ],
        "name": "Application Layer Protocol",
        "url": "https://attack.mitre.org/techniques/T1071"
      },
      {
        "id": "T1559",
        "name": "Inter-Process Communication",
        "url": "https://attack.mitre.org/techniques/T1559"
      }
    ],
    "mod_time": 1751916626047,
    "participants": [
      {
```

```
        "endpoint": "client",
        "external": false,
        "hostname": "pc1.i.rx.tours",
        "id": 7243,
        "object_id": 25769803786,
        "object_type": "device",
        "object_value": "10.1.0.146",
        "role": "offender",
        "scanner_service": null,
        "username": "administrator@ATTACK.LOCAL"
      },
      {
        "endpoint": "server",
        "external": false,
        "hostname": "dc1.attack.local",
        "id": 7601,
        "object_id": 25769803777,
        "object_type": "device",
        "object_value": "10.1.1.10",
        "role": "victim",
        "scanner_service": null,
        "username": null
      }
    ],
    "properties": {
      "association": "RemCom",
      "category": "Malware",
      "client_port": 53284,
      "named_pipe": "remcom",
      "server_port": 445
    },
    "recommended": true,
    "recommended_factors": [
      "critical_asset",
      "top_offender"
    ],
    "resolution": null,
    "risk_score": 65,
    "start_time": 1751912989096,
    "status": null,
    "ticket_id": null,
    "title": "Suspicious SMB Named Pipe",
    "type": "suspicious_smb_named_pipe",
    "update_time": 1751912989718,
    "url": "https://extrahop-bd.cloud.extrahop.com/extrahop/#/detections/
detail/25769804210/?from=1751912089until=1751913889interval_type=DT"
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`, `.type`, `.risk_score`, `.id`	Event.Title, Incident.Value	Detection	`.create_time`	`Kerberos Golden Ticket Attack | kerberos_golden_ticket_attack | Risk Score: 90 | ID: 25769804247`	Fields concatenated together to build the detection title.
`.description`, `.properties.*`, `.participants[]`	Event.Description, Incident.Description	N/A	N/A	N/A	Fields concatenated together to build the HTML description.
`.ticket_id`	Event.Attribute, Incident.Attribute	Ticket ID	`.create_time`	`1412`	N/A
`.type`	Event.Attribute, Incident.Attribute, Indicator.Attribute	Detection Type	`.create_time`	`malicious_file_hash_transfer`	See Category mapping table.
`.categories[]`	Event.Attribute/Tag, Incident.Attribute/Tag	Primary Category, Category	`.create_time`	`Exfiltration`	Attribute is named **Primary Category** with value **Security** or **Performance** if `.categories` contains `sec` or `perf`. For the rest, values are mapped using the Category mapping table and the attribute name is **Category**.
`.risk_score`	Event.Attribute, Incident.Attribute, Indicator.Attribute	Risk Score	`.create_time`	`61`	Updatable.
`.risk_score`	Event.Attribute, Incident.Attribute, Indicator.Attribute	Normalized Risk	`.create_time`	`High`	Updatable. User-configurable. Value based on the **Custom Score Mapping** user field.
`.recommended`	Event.Attribute, Incident.Attribute	Is Recommended	`.create_time`	`true`	Updatable.
`.status`	Event.Attribute, Incident.Attribute	Status	`.create_time`	`new`	Updatable.
`.mitre_tactics[].name`	Event.Attribute, Incident.Attribute	Tactic	`.create_time`	`Reconnaissance`	See Tactic mapping table.
`.resolution`	Event.Attribute, Incident.Attribute	Resolution	`.create_time`	N/A	Updatable.
`.assignee`	Event.Attribute, Incident.Attribute	Assignee	`.create_time`	N/A	N/A
`.recommended_factors[]`	Event.Attribute/Tag, Incident.Attribute/Tag	Recommendation Factor	`.create_time`	`top-offender`	User-configurable.
`.end_time`	Event.Attribute, Incident.Attribute	Ended At	`.create_time`	`2025-07-24 05:01:23`	User-configurable. Used when **Ingest Detections As** is set to **Event**.
`.properties.service_names`	Event.Attribute, Incident.Attribute	Service Name	`.create_time`	`Google (DoH)`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.properties.client_port`	Event.Attribute, Incident.Attribute	Client Port	`.create_time`	`80`	N/A
`.properties.server_port`	Event.Attribute, Incident.Attribute	Server Port	`.create_time`	`443`	N/A
`.properties.exec_file_types`	Event.Attribute, Incident.Attribute	Executable File Type	`.create_time`	`PE`	N/A
`.properties.collector`	Event.Attribute, Incident.Attribute	Ticket ID	`.create_time`	`Empire BloodHound.ps1`	N/A
`.properties.protocol`	Event.Attribute, Incident.Attribute	Protocol	`.create_time`	`HTTP`	N/A
`.properties.user`	Event.Attribute, Incident.Attribute	User	`.create_time`	`admin`	N/A
`.properties.version`	Event.Attribute, Incident.Attribute	TLS Version	`.create_time`	`TLS 1.2`	N/A
`.properties.certificate`	Event.Attribute, Incident.Attribute	Certificate	`.create_time`	`dc1.attack.local:RSA_2048:3e426a1a3b2c2cae4cb51ec46b6c8a88`	N/A
`.properties.named_pipe`	Event.Attribute, Incident.Attribute	Named Pipe	`.create_time`	`remcom`	N/A
`.ticket_id`	Event.Attribute, Incident.Attribute	Ticket ID	`.create_time`	`1412`	N/A
`.mitre_techniques[].id - .mitre_techniques[].name`	AttackPattern.Value	N/A	`.create_time`	`T1559 - Inter-Process Communication`	Mapped to existing MITRE Techniques in ThreatQ.
`.properties.association`	Malware.Value	N/A	`.create_time`	`RemCom`	Used when `.properties.category` is **Malware**.
`.properties.variant`	Malware.Value	N/A	`.create_time`	`WannaCry`	N/A
`.properties.association`	Adversary.Name	N/A	`.create_time`	N/A	Used when `.properties.category` is one of **Actor**, **Threat Actor**, or **Adversary**.
`.properties.software`	Tool.Value	N/A	`.create_time`	`sqlmap`	N/A
`.properties.hackin`	Tool.Value	N/A	`.create_time`	`Kali Linux`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`g_tool_name`					
`.properties.tool`	Tool.Value	N/A	`.create_time`	`Impacket's GetUserSPNs.py`	N/A
`.participants[].object_value`	Asset.Value	N/A	`.create_time`	`10.13.0.115`	User-configurable. Applied when `.object_type` is **device**.
`.participants[].role`	Asset.Tag	N/A	N/A	`victim`	User-configurable.
`.participants[].endpoint`	Asset.Tag	N/A	N/A	`server`	User-configurable.
`.participants[].hostname`	Asset.Attribute	Hostname	`.create_time`	N/A	N/A
`.properties.registered_domain_name`	Indicator.Value	FQDN	`.create_time`	N/A	N/A
`.properties.registered_domain_names`	Indicator.Value	FQDN	`.create_time`	N/A	N/A
`.properties.domain`	Indicator.Value	FQDN	`.create_time`	N/A	N/A
`.properties.host`	Indicator.Value	FQDN	`.create_time`	N/A	N/A
`.properties.query`	Indicator.Value	FQDN	`.create_time`	N/A	N/A
`.properties.rdn`	Indicator.Value	FQDN	`.create_time`	N/A	N/A
`.properties.server_ipaddr`	Indicator.Value	IP Address	`.create_time`	N/A	N/A
`.title`	Indicator.Value, Vulnerability.Value	CVE	`.create_time`	`CVE-2025-12345`	User-configurable. CVE ID is parsed from the detection title.
`.properties.filename`	Indicator.Value	File Name	`.create_time`	`H0d0r.exe`	N/A
`.properties.file_sha256`	Indicator.Value	SHA-256	`.create_time`	`178ba564b39bd07577e974a9b677dfd86ffa1f1d0299dfd958eb883c5ef6c3e1`	N/A
N/A	Indicator.Tag	N/A	N/A	`detected`	Automatically added to ingested indicators when enabled in the user fields.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Indicator.Attribute	Disposition	`.create_time`	`Malicious`	Disposition parsed from the detection title when available.
`.categories[]`	Indicator.Attribute	Threat Type	`.create_time`	`Ransomware`	Threat Type parsed from categories when available. See Threat Type mapping table.
`.categories[]`	Indicator.Attribute	Tactic	`.create_time`	`Command and Control`	Tactic parsed from categories when available.
`.properties.file_paths[]`	Event.Attribute, Incident.Attribute, Indicator.Attribute	File Path	`.create_time`	`ADMIN$\xxFDMxx.exe`	N/A

Category Mapping Table

EXTRAHOP VALUE	THREATQ VALUE
`sec.action`	Actions on Objective
`sec.attack`	Attack
`sec.botnet`	Botnet
`sec.caution`	Caution
`sec.command`	Command & Control
`sec.cryptomining`	Cryptomining
`sec.dos`	Denial of Service
`sec.exfil`	Exfiltration
`sec.exploit`	Exploitation
`sec.hardening`	Hardening
`sec.lateral`	Lateral Movement
`sec.ransomware`	Ransomware
`sec.recon`	Reconnaissance
`perf.auth`	Authorization & Access Control
`perf.db`	Database
`perf.network`	Network Infrastructure

EXTRAHOP VALUE	THREATQ VALUE
`perf.service`	Service Degradation
`perf.storage`	Storage
`perf.virtual`	Desktop & App Virtualization
`perf.web`	Web Application

Threat Type Mapping Table

EXTRAHOP VALUE	THREATQ VALUE
`sec.attack`	Attack
`sec.botnet`	Botnet
`sec.cryptomining`	Cryptomining
`sec.dos`	Denial of Service
`sec.exfil`	Exfiltration
`sec.exploit`	Exploitation
`sec.ransomware`	Ransomware

Tactic Mapping Table

EXTRAHOP VALUE	THREATQ VALUE
`sec.command`	Command and Control
`sec.lateral`	Lateral Movement
`sec.exfil`	Exfiltration
`sec.recon`	Reconnaissance

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	1 minute
Assets	13
Asset Attributes	12
Attack Patterns	51
Events	126
Event Attributes	1,500
Indicators	41
Indicator Attributes	190
Malware	2
Tools	5

Change Log

- **Version 1.0.0**
  - Initial release.