ThreatQuotient

A Securonix Company

Intel 471 Hunter Action

Version 1.0.0

September 28, 2026

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

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	>= 5.29.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Intel 471 Hunter Action enriches Malware and Adversary objects in a ThreatQ Data Collection with contextual intelligence from Intel 471. It uses the same search capabilities and object mappings as the Intel 471 Hunter Operation.

The integration provides the following action:

- **Intel 471 Hunter - Search** - searches Intel 471 for contextual intelligence related to Malware and Adversary objects in a ThreatQ Data Collection, returning associated threat objects and indicators.

The integration is compatible with the following object types:

- Adversaries
- Malware

The integration enriches the following object types:

- Adversaries
- Attack Patterns
- Campaigns
- Indicators
- Malware
- Tools

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- An Intel 471 Developer Portal Application Client ID and Client Secret.
- A data collection containing at least one adversary or malware object.
- MITRE ATT&CK Attack Pattern objects must be present in ThreatQ before Hunter technique IDs can be mapped to their corresponding ATT&CK records. Ingest these objects using the MITRE Enterprise ATT&CK, MITRE Mobile ATT&CK, or MITRE ICS ATT&CK feeds from the MITRE ATT&CK integration.

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip file on your local machine

   > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

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 **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

   The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Client ID	Enter your Intel 471 Developer Portal application client ID.
Client Secret	Enter your Intel 471 Developer Portal application client secret.
Days For Querying	Enter the number of previous days included in the search. The default value is `7`.
Intel 471 Search Indexes	Select the Hunter indexes to be queried by the action. Options include: ◦ Cyborg Use Cases ◦ Cyborg Collections ◦ Cyborg Threat Profile

PARAMETER	DESCRIPTION
Threat Categories	Optional - Enter one or more Hunter threat categories to filter the search results.
Threat Types	Optional - Enter one or more Hunter threat types to filter the search results.
MITRE Tactic Names	Optional - Enter one or more MITRE ATT&CK tactics to filter the search results.
MITRE Technique IDs	Optional - Enter one or more MITRE ATT&CK technique IDs to filter the search results.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	Enter the maximum number of objects to process per run.

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Intel 471 Hunter - Search	Enriches submitted objects with contextual data from Intel 471.	Adversary, Malware	N/A

Intel 471 Hunter - Search

The Intel 471 Hunter - Search action enriches Malware and Adversary objects with contextual data from Intel 471.

```
GET https://api.intel471.cloud/integrations/hunter/v1/es/query
```

Sample Parameters:

```
{
  "term": "APT15",
  "days": "7",
  "size": 10,
  "indexes": "cyborg_usecases",
  "indexes": "cyborg_collections",
  "indexes": "cyborg_threat_profiles"
}
```

Sample Response (truncated):

```
{
  "total": 3,
  "results": [
    {
      "index": "cyborg_usecases",
      "id": "e1650196-ebc1-4dee-a65e-2fcaacf5255e",
      "score": 2,
      "title": "Suspicious SOCKS Proxy Process Creation",
      "UUID": "e1650196-ebc1-4dee-a65e-2fcaacf5255e",
      "status": "Complete",
```

```
      "severity": "Medium",
      "community": false,
      "description": "This hunt package identifies processes creating
a SOCKS proxy (ssh -D, plink, chisel, microsocks, python-based
sockserver), or processes with socks-related arguments. SOCKS often
avoids typical web filtering or inspection (it simply forwards
traffic), making it a valuable tool for attackers to exfiltrate data
or bypass network controls.",
      "content": {
        "tools": [
          "CrowdStrike"
        ]
      },
      "context": {
        "tooling": [],
        "threat_names": [
          "GlassWorm"
        ],
        "threat_description": "A SOCKS proxy is a network protocol
that routes traffic between a client and server through an
intermediary process, often used for legitimate purposes such as
bypassing geographic restrictions or enhancing privacy. However, when
processes like `ssh -D`, `plink`, `chisel`, `microsocks`, or custom
Python-based SOCKS servers are created outside of expected
administrative activity, they can indicate malicious intent. Threat
actors abuse SOCKS proxies to covertly exfiltrate data, bypass
network controls, and anonymize their operations, making it difficult
for defenders to trace or block unauthorized communications. Recent
malware campaigns, such as GlassWorm and GhostSocks, have
demonstrated how attackers deploy SOCKS proxies on compromised
systems to turn victim machines into relay nodes for criminal
infrastructure, enabling lateral movement, persistent access, and
further exploitation while evading traditional security monitoring.",
        "threat_categories": [
          "Technique"
        ]
      },
      "tags": {
        "tools": [],
        "campaigns": [
          "CrowdStrike | Content Update Crash | 2024"
        ],
```

```
        "platform_types": [],
        "data_sources": [],
        "goals": [],
        "dependencies": [],
        "threat_names": [
          "GlassWorm",
          "8base Ransomware",
          "Agent Tesla"
        ],
        "threat_categories": [
          "Technique"
        ],
        "threat_types": [
          "Worm"
        ],
        "attack_surfaces": [
          "client"
        ],
        "target_oses": [
          "Linux",
          "Windows"
        ],
        "actors": [
          "Scattered Spider"
        ],
        "tooling": [],
        "diamond_models": [
          "Capability"
        ],
        "kill_chains": [
          "Actions on Objectives"
        ],
        "mitre_tactic_names": [
          "Command and Control"
        ],
        "mitre_technique_names": [
          "Multi-hop Proxy",
          "Protocol Tunneling"
        ],
        "mitre_technique_ids": [
          "T1090.003",
          "T1572"
```

```
        ],
        "source_countries": [
          "China"
        ],
        "source_regions": [],
        "target_countries": [],
        "target_regions": [
          "Global"
        ],
        "target_industries": [
          "Cryptocurrency",
          "Development"
        ],
        "exploit_or_vulns": [
          "CVE-2022-41082",
          "CVE-2025-59287"
        ],
        "motivations": [],
        "severities": [],
        "operations": [
          "DeadRinger"
        ],
        "target_os_versions": []
      }
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this action:

> The following paths are relative to each entry in `.results[]`. Values shown in the examples were verified against the captured feed-data response. Null or empty values are skipped.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`.content.categories[]`	Malware.Attribute	Category	`edr`	Added to each Data Collection object as an attribute.
`.content.tools[]`	Related Tool.value	N/A	`CrowdStrike`	Added as a related Tool object.
`.severity`	Malware.Attribute	Severity	`High`	Added to each Data Collection object as an attribute.
`.tags.attack_surfaces[]`	Malware.Attribute	Attack Surface	`Client`	Added to each Data Collection object as an attribute.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`.tags.diamond_models[]`	Malware.Attribute	Diamond Model	`Capability`	Added to each Data Collection object as an attribute.
`.tags.kill_chains[]`	Malware.Attribute	Kill Chain	`Installation`	Added to each Data Collection object as an attribute.
`.tags.mitre_tactic_names[]`	Malware.Attribute	Tactic	`Command and Control`	Added to each Data Collection object as an attribute.
`.tags.operations[]`	Malware.Attribute	Operation	`DeadRinger`	Added to each Data Collection object as an attribute.
`.tags.source_countries[]`	Malware.Attribute	Source Country	`China`	Added to each Data Collection object as an attribute.
`.tags.source_regions[]`	Malware.Attribute	Source Regions	`Unknown`	Added to each Data Collection object as an attribute.
`.tags.target_countries[]`	Malware.Attribute	Target Country	`Unknown`	Added to each Data Collection object as an attribute.
`.tags.target_industries[]`	Malware.Attribute	Target Industry	`Finance`	Added to each Data Collection object as an attribute.
`.tags.target_oses[]`	Malware.Attribute	Target OS	`Windows`	Added to each Data Collection object as an attribute.
`.tags.target_regions[]`	Malware.Attribute	Target Region	`Global`	Added to each Data Collection object as an attribute.
`.tags.threat_categories[]`	Malware.Attribute	Threat Category	`Malware`	Added to each Data Collection object as an attribute.
`.tags.threat_types[]`	Malware.Attribute	Threat Type	`Worm`	Added to each Data Collection object as an attribute.
`.tags.exploit_or_vulns[]`	Related Indicator.value	CVE	`CVE-2022-41040`	Added as a related CVE Indicator object.
`.tags.threat_names[]` or `.context.threat_names[]`	Related Malware.value	N/A	`Agent Tesla`	Values from both paths are added as related Malware objects.
`.tags.actors[]` or `.context.actors[]`	Related Adversary.value	N/A	`APT31`	Values from both paths are added as related Adversary objects.
`.tags.campaigns[]` or `.context.campaigns[]`	Related Campaign.value	N/A	`CrowdStrike | Content Update Crash | 2024`	Values from both paths are added as related Campaign objects.
`.tags.mitre_technique_ids[]`	Related Attack Pattern.value	N/A	`T1053.005`	Related only when the Attack Pattern already exists in ThreatQ.

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	< 1 minute
Adversaries	67
Attack Patterns	10
Campaigns	1
Indicators	15
Malware	89
Malware Attributes	36
Tools	17

Change Log

- **Version 1.0.0**
  - Initial release