ThreatQuotient

A Securonix Company

Augur Security Action

Version 1.0.0

June 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	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Augur Security Action enriches supported ThreatQ indicators with threat intelligence from the Augur Security platform. Based on user-selected options, the action can ingest contextual information such as related indicators, breach intelligence, WHOIS data, MITRE ATT&CK mappings, and other threat context, providing analysts with additional intelligence to support investigation and response workflows.

The integration provides the following action:

- **Augur Security - Enrich IOCs** - queries Augur Security for each supported indicator contained in the submitted ThreatQ data collection and enriches the corresponding source indicators with configurable attributes, tags, description content, and related threat intelligence objects.

The integration is compatible with the following indicator types:

- IP Address
- MD5
- SHA-1
- SHA-256
- FQDN
- CIDR Block

The integration enriches the following object types:

- Adversaries
- Attack Patterns
- Indicators
    - ASN
    - CVE
    - Filename
    - FQDN
    - IP Address
    - MD5
    - SHA-1
    - SHA-256
    - SHA-512

    - URL
- Malware
- Reports
- Tools
- Vulnerabilities

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 Augur Security API Key.
- A data collection containing at least one of the following indicator types:
  - IP Address
  - MD5
  - SHA-1
  - SHA-256
  - FQDN
  - CIDR Block

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
API Key	Enter your Augur Security API Key.
Selected Context to Ingest	Select the context information to ingest for each enriched indicator. Options include: ◦ Country *(default)* ◦ Country Code ◦ Category *(default)* ◦ Is DGA *(default)* ◦ RIR ◦ ASN ◦ Predicted Category ◦ Predicted Importance ◦ Service Flags

PARAMETER	DESCRIPTION
	◦ Related Breaches ◦ Related Hostnames ◦ Related IPs ◦ Related URLs ◦ Related Hashes ◦ Related Filenames ◦ Related Malware ◦ Related Tools ◦ Related Actors ◦ Related MITRE ATT&CK Techniques ◦ Related Vulnerabilities The available context varies by indicator type, so some options may not be applicable to all indicators.
Selected WHOIS Context as Attributes	Select the WHOIS fields to ingest as **Attributes** on enriched indicators. By default, available WHOIS information is ingested into the **Description** field of each enriched indicator. Enabling the options below additionally stores the selected WHOIS fields as structured attributes to provide enhanced context and improve search, filtering, and analysis. Options include: ◦ Registry ◦ Registrant Name ◦ Registrant Organization ◦ Registrant Country ◦ Registrant City ◦ Registrant Status ◦ Owner Contact ◦ Admin Contact

PARAMETER	DESCRIPTION
	◦ Abuse Contact ◦ Technical Contact
Inherit Context to Related Indicators	Select the context information to inherit to related indicators, such as hostnames, URLs, and file hashes. The selected context will be added as **Attributes** or **Relationships** on the related indicators during enrichment. Currently, the only option available for this parameter is `Category`.  Context is not inherited to indicators that are marked as **Whitelisted**.
Selected Breach Context to Ingest	Select which context to ingest for related breaches. Options include: ◦ Target Industry *(default)* ◦ Target Product *(default)* ◦ Category *(default)* ◦ Source ◦ Related MITRE Techniques *(default)* ◦ Related IOCs *(default)*  Not all fields will be available for all breaches.
Ingest ASNs As	Select whether to ingest ASNs as `Indicators` or `Attributes`.
Ingest CVEs As	Select whether to ingest CVEs as `Indicators` or `Vulnerabilities`. The default value is `Indicators (CVE)`.
Objects Per Run	Enter the number of objects to process per run of the workflow.

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
Augur Security - Enrich IOCs	Performs a bulk lookup of IOCs against Augur Security	Indicators	IP Address, MD5, SHA-1, SHA-256, FQDN, CIDR Block

Augur Security – Enrich IOCs

The Augur Security – Enrich IOCs action queries Augur Security for each supported indicator contained in the submitted ThreatQ data collection and enriches the corresponding source indicators with configurable attributes, tags, description content, and related threat intelligence objects.

`GET https://api.seclytics.com/{type}/{value}`

Typical Query Parameters:

- `access_token={api_key}`
- `fields=connections,country,asn,global_threat_context,rir,whitelist,whois,services,prediction,dga,mitre_attack,breaches`

Sample Response (truncated):


```
{
  "asn": {
    "description": "LEASEWEB-DE-FRA-10",
    "number": "28753"
  },
  "country": {
    "code": "DE",
    "name": "Germany"
  },
  "cidr": {
    "block": "45.146.130.0/24",
    "size": 256,
    "status": "announced"
  },
  "context": {
    "categories": {
      "alien_vault_otx": ["malicious"],
      "spamhaus": ["spam"]
    },
    "identifiers": {
      "alien_vault_otx": ["naikon"]
    },
    "references": {
      "alien_vault_otx": [
        "https://www.forcepoint.com/blog/..."
      ]
```

```
    }
  },
  "breaches": [
    {
      "breach_id": "6877ccdd408fd221f0f3c797",
      "title": "Signed and stealing: uncovering new insights on
Odyssey infostealer",
      "source": "Jamf",
      "category": [
        "Endpoint Security",
        "Network Security"
      ],
      "iocs": [
        {
          "domains": [
            "http://45.146.130.131/log",
            "https://allteching.xyz/auto",
            "..."
          ],
          "ips": [
            "45.146.130.131"
          ],
          "hashesSha256": [

"DEC750B9D596B14AEAB1ED6F6D6D370022443CECEB127E7D2468B903C2D9477A",

"20368580A775B6F8B07BE0A59CB57CB8B9B5FD8FBEA41D90F4F10B9EBB588F50",
            "..."
          ]
        }
      ],
      "ttps": [
        {
          "number": "T1555.003",
          "title": "Credentials from Web Browsers"
        }
      ]
    }
  ],
  "global_threat_context": {
    "categories": [
      "malicious",
```

```
      "spam"
    ],
    "feeds": [
      {
        "name": "spamhaus"
      },
      {
        "name": "alien_vault_otx"
      }
    ],
    "references": [
      "https://cybersecuritynews.com/...",
      "https://www.forcepoint.com/..."
    ]
  },
  "history": {
    "first_seen_at": "2025-08-07T00:00:00",
    "last_seen_at": "2025-08-07T00:00:00"
  },
  "id": "45.146.130.131",
  "ip": {
    "address": "45.146.130.131",
    "type": "global"
  },
  "mitre_attack": [
    {
      "id": "T1329",
      "name": "Acquire and/or use 3rd party infrastructure services"
    }
  ],
  "predicted": {
    "category": "malware",
    "importance": 10,
    "predicted_at": "2025-07-15T08:17:57"
  },
  "rir": {
    "code": "RI",
    "name": "RIPE"
  },
  "type": "ip",
  "whois": [
    {
```

```
      "registry": "RIPE",
      "inet": "45.146.130.0/24",
      "name": "US-RAPIDSEEDBOX",
      "status": "ASSIGNED PA",
      "country": {
        "code": "US",
        "name": "United States"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.services.is_hosting	Indicator.Tag	N/A	N/A	hosting	Only applied if true
.services.anonymous.is_relay	Indicator.Tag	N/A	N/A	relay	Only applied if true
.services.anonymous.is_proxy	Indicator.Tag	N/A	N/A	proxy	Only applied if true
.services.anonymous.is_tor	Indicator.Tag	N/A	N/A	tor	Only applied if true
.services.anonymous.is_vpn	Indicator.Tag	N/A	N/A	vpn	Only applied if true
.services.is_anycast	Indicator.Tag	N/A	N/A	anycast	Only applied if true
.services.is_mobile	Indicator.Tag	N/A	N/A	mobile	Only applied if true
.services.is_satellite	Indicator.Tag	N/A	N/A	satellite	Only applied if true
.dga.is_dga	Indicator.Tag	N/A	N/A	dga	Only applied if true
.country.name	Indicator.Attribute	Country	N/A	Canada	N/A
.country.code	Indicator.Attribute	Country Code	N/A	CA	N/A
.global_threat_context.categories[]	Indicator.Attribute	Category	N/A	malicious	N/A
.rir.name	Indicator.Attribute	RIR	N/A	RIP	N/A
.asn.number	Indicator.Attribute	ASN	N/A	12345	If selected to be ingested as an attribute
.predicted.category	Indicator.Attribute	Predicted Category	N/A	phishing	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.predicted.importance	Indicator.Attribute	Predicted Importance	N/A	10	N/A
.asn.description	Indicator.Attribute	AS Organization	N/A	LEASEWEB-DE-FRA-10	N/A
.services.anonymous.name	Indicator.Attribute	Anonymizer Service	N/A	NordVPN	N/A
.whois.registry	Indicator.Attribute	Registry	N/A	ARIN	N/A
.whois.name	Indicator.Attribute	Registrant Name	N/A	John Doe	N/A
.whois.org	Indicator.Attribute	Registrant Organization	N/A	Example Org	N/A
.whois.country.name	Indicator.Attribute	Registrant Country	N/A	Canada	N/A
.whois.city	Indicator.Attribute	Registrant City	N/A	Toronto	N/A
.whois.status	Indicator.Attribute	Registrant Status	N/A	Active	N/A
.whois.owner_c	Indicator.Attribute	Owner Contact	N/A	owner@example.com	N/A
.whois.admin_c	Indicator.Attribute	Admin Contact	N/A	admin@example.com	N/A
.whois.abuse_c	Indicator.Attribute	Abuse Contact	N/A	abuse@example.com	N/A
.whois.tech_c	Indicator.Attribute	Technical Contact	N/A	tech@example.com	N/A
.global_threat_context.actors[].human_readable	Related Adversary.Value	N/A	N/A	Fancy Bear	N/A
.global_threat_context.actors[].sponsor	Related Adversary.Attribute	N/A	N/A	North Korea	N/A
.global_threat_context.malware_families[].human_readable	Related Malware.Value	N/A	N/A	Emotet	N/A
.tools[].human_readable	Related Tool.Value	N/A	N/A	AnyDesk	Extracted from .global_threat_context.malware_families[] when the family name matches the built-in tool list.
.accessed_by_files[]	Related Indicator.Value	MD5, SHA-1, SHA-256, or SHA-512	N/A	DEC750B9D596B14AEAB1ED6F6D6D370022443CECEB127E7D2468B903C2D9477A	N/A
.connections[{indicator_value}]	Related Indicator.Attribute	Whitelist Reason	N/A	benign infrastructure	Applied to related indicators when the indicator value exists as a key in connections.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.global_threat_context.md5[]	Related Indicator.Value	MD5	N/A	N/A	N/A
.global_threat_context.sha1[]	Related Indicator.Value	SHA-1	N/A	N/A	N/A
.global_threat_context.sha256[]	Related Indicator.Value	SHA-256	N/A	N/A	N/A
.global_threat_context.sha512[]	Related Indicator.Value	SHA-512	N/A	N/A	N/A
.global_threat_context.hostnames[]	Related Indicator.Value	FQDN	N/A	N/A	N/A
.global_threat_context.urls[]	Related Indicator.Value	URL	N/A	N/A	N/A
.global_threat_context.names[]	Related Indicator.Value	Filename	N/A	N/A	N/A
.global_threat_context.ips[]	Related Indicator.Value	IP Address	N/A	N/A	N/A
.mitre_attack[].id	Attack Pattern.Value	N/A	N/A	N/A	Translated to corresponding ThreatQ Attack Pattern object
.global_threat_context.vulnerabilities[].human_readable	Related Indicator.Value or Related Vulnerability.Value	N/A	N/A	CVE-2026-12345	Ingested based on user-selection
.breaches[].title	Related Report.Value	N/A	N/A	Signed and stealing: uncovering new insights on Odyssey infostealer	N/A
.breaches[].affected_industries	Related Report.Attribute	Target Industry	N/A	Energy	N/A
.breaches[].affected_technologies	Related Report.Attribute	Target Product	N/A	Adobe Reader	N/A
.breaches[].category	Related Report.Attribute	Category	N/A	Endpoint Security	N/A
.breaches[].source	Related Report.Attribute	Source	N/A	Jamf	N/A
.breaches[].ttps[].number,	Related Attack Pattern.Value	N/A	N/A	T1024 - MITRE Technique Name	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.breaches[].ttps[].title					
.breaches[].iocs[].cves[]	Related Indicator.Value or Related Vulnerability.Value	CVE	N/A	CVE-2026-12345	Ingested based on user-selection
.breaches[].iocs[].domains[]	Related Indicator.Value	FQDN	N/A	example.com	N/A
.breaches[].iocs[].hashesMd5[]	Related Indicator.Value	MD5	N/A	d41d8cd98f00b204e9800998ecf8427e	N/A
.breaches[].iocs[].hashesSha1[]	Related Indicator.Value	SHA-1	N/A	da39a3ee5e6b4b0d3255bfef95601890afd80709	N/A
.breaches[].iocs[].hashesSha256[]	Related Indicator.Value	SHA-256	N/A	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	N/A
.breaches[].iocs[].ips[]	Related Indicator.Value	IP Address	N/A	45.12.67.13	N/A

Endpoint Type Mapping

The Endpoint Type Mapping defines how the action translates each supported ThreatQ indicator type into the appropriate Augur Security API endpoint. When the action processes an indicator from the submitted ThreatQ data collection, it automatically selects the correct endpoint based on the indicator type and substitutes the indicator value into the endpoint path before querying the Augur Security API.

The action uses the following mappings:

THREATQ INDICATOR TYPE	AUGUR SECURITY ENDPOINT
IP Address	`ips/{value}`
MD5	`files/{value}`
SHA-1	`files/{value}`
SHA-256	`files/{value}`

THREATQ INDICATOR TYPE	AUGUR SECURITY ENDPOINT
FQDN	`domains/{value}`
CIDR Block	`cidrs/{value}`

For example:

- An IP address of `45.146.130.131` is queried using:

  ```
  GET /ips/45.146.130.131
  ```

- A SHA-256 hash is queried using:

  ```
  GET /files/<sha256>
  ```

- A domain such as `example.com` is queried using:

  ```
  GET /domains/example.com
  ```

- A CIDR block such as `45.146.130.0/24` is queried using:

  ```
  GET /cidrs/45.146.130.0/24
  ```

Using this mapping allows the action to support multiple indicator types while automatically selecting the appropriate Augur Security API endpoint for each lookup. The returned intelligence is then normalized and used to enrich the corresponding ThreatQ indicator with the selected attributes, tags, descriptions, and related threat intelligence objects.

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	2 minutes
Indicators	279
Indicator Attributes	5,109

Use Case Example

I have a list of IP Addresses and want to figure out the likelihood of any of them being used for fraudulent activity. I can use this action to enrich each IP with Augur Security data, including risk scores, proxy information, ISP information, and additional context from various aggregated external data sources.

Change Log

- **Version 1.0.0**
  - Initial release