ThreatQuotient

A Securonix Company

SPARTA Aerospace CDF

Version 1.0.0

August 31, 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	>= 5.26.0
Support Tier	ThreatQ Supported

Introduction

The SPARTA Aerospace CDF ingests the Aerospace Corporation's Space Attack Research and Tactic Analysis (SPARTA) knowledge base into ThreatQ. SPARTA provides structured information on space-system attack techniques, threats, countermeasures, D3FEND context, and behavioral detection signatures.

The integration provides the following feed:

- **SPARTA Aerospace** - imports the latest publicly available SPARTA STIX 2.1 dataset, preserving SPARTA custom properties as ThreatQ attributes or within the object description.

> External references are also rendered in the description. Attack Patterns, Courses of Action, and Signatures use the following naming convention, consistent with MITRE techniques: `<ID> - <Name>`. See the SPARTA working-with guide for more details: https://sparta.aerospace.org/resources/working-with.

The integration ingests the following object types into ThreatQ:

- Attack Patterns
  - Attack Pattern Attributes
- Courses of Action
  - Course of Action Attributes
- Signatures
  - Signature Attributes

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.

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

ThreatQ Mapping

SPARTA Aerospace

The SPARTA Aerospace feed retrieves a STIX 2.1 bundle, processes supported objects from the bundle's `.objects[]` collection, and creates ThreatQ relationships based on the STIX relationship objects.

```
GET https://sparta.aerospace.org/download/STIX?f=latest
```

Sample Response:


```
{
  "type": "bundle",
  "id": "bundle--041f6c96-c777-472c-99ca-3c07307fb982",
  "objects": [
    {
      "type": "attack-pattern",
      "id": "attack-pattern--6fe42547-e79b-4e96-b7b4-25774dffd3cc",
      "created": "2026-04-09T00:45:22.678Z",
      "name": "Gather Spacecraft Design Information",
      "x_mitre_id": "REC-0001",
      "description": "Threat actors seek a coherent picture of the
spacecraft and its supporting ecosystem.",
      "kill_chain_phases": [
        {
          "kill_chain_name": "sparta",
          "phase_name": "Reconnaissance"
        }
      ],
      "external_references": [
        {
          "source_name": "sparta",
          "url": "https://sparta.aerospace.org/technique/REC-0001/",
          "external_id": "REC-0001"
        }
      ],
      "x_sparta_is_subtechnique": "False",
      "x_aerospace_high_notional_risk_rank_score": "18"
    }
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this feed based on each supported item within the response's `.objects[]` list.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.x_mitre_id, .external_references[].external_id, .name`	Attack Pattern.Value	N/A	`.created`	SV-IT-5 - Time Synchronized Execution	The first SPARTA or D3FEND external ID is used when `.x_mitre_id` is absent. Canonical SPARTA threat titles are restored when the STIX source name contains only the ID.
`.description`	Attack Pattern.Description	N/A	N/A	Threat actors seek a coherent picture...	N/A
`.external_references[]`	Attack Pattern.Description	N/A	N/A	SPARTA, D3FEND, CAPEC, and source URLs	Rendered as an HTML table in the description and not ingested as attributes.
`.x_aerospace_high_level_requirement` or `.x_aerospace_high_level_requirements`	Attack Pattern.Description	N/A	N/A	The Program shall protect...	Appended to the description. Both the legacy singular field and the v4.0 plural field are supported.
`.kill_chain_phases[].phase_name`	Attack Pattern.Attribute	Tactic	`.created`	Reconnaissance	N/A
`.x_sparta_is_subtechnique`	Attack Pattern.Attribute	Is Subtechnique	`.created`	True	Updatable.
`.x_aerospace_did_layer`	Attack Pattern.Attribute	Defense-in-Depth Layer	`.created`	S/C Software	Updatable.
`.x_aerospace_high_notional_risk_rank_score`	Attack Pattern.Attribute	High Notional Risk Rank Score	`.created`	18	Updatable.
`.x_aerospace_medium_notional_risk_rank_score`	Attack Pattern.Attribute	Medium Notional Risk Rank Score	`.created`	15	Updatable.
`.x_aerospace_low_notional_risk_rank_score`	Attack Pattern.Attribute	Low Notional Risk Rank Score	`.created`	11	Updatable.
`.x_aerospace_threat_tier`	Attack Pattern.Attribute	Threat Tier	`.created`	III	Updatable.
`.x_aerospace_notional_risk_rank_score`	Attack Pattern.Attribute	Notional Risk Rank Score	`.created`	25	Updatable.
`.x_mitre_id, .external_references[].external_id, .name`	Course Of Action.Value	N/A	`.created`, when supplied	D3-AI - Asset Inventory	Normalized to <ID> - <Name>.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.description	Course Of Action.Description	N/A	N/A	Asset inventorying identifies...	N/A
.external_references[]	Course Of Action.Description	N/A	N/A	SPARTA and D3FEND references	Rendered as an HTML table in the description and not ingested as attributes.
.x_sparta_category	Course Of Action.Attribute	Category	.created, when supplied	Prevention	N/A
.x_sparta_deployment	Course Of Action.Attribute	Deployment	.created, when supplied	Ground Segment and Development Environment	N/A
.x_d3fend_artifacts[]	Course Of Action.Attribute	D3FEND Artifact	.created, when supplied	Digital Artifact	N/A
.x_d3fend_tactics	Course Of Action.Attribute	D3FEND Tactic	.created, when supplied	Credential	N/A
.name	Signature.Name	N/A	.created	UACE-8 - Anomalous Command Packet Signatures	The source <ID>: <Name> value is normalized to <ID> - <Name>.
.pattern	Signature.Value	Custom	.created	[x-opencti-command-log:signature != 'expected_signature']	N/A
.description	Signature.Description	N/A	N/A	Detection of anomalous command packet signatures...	N/A
.external_references[]	Signature.Description	N/A	N/A	External source URLs	Rendered as an HTML table in the description and not ingested as attributes.
.pattern_type	Signature.Attribute	Type	.created	STIX Pattern	Mapped to STIX Pattern.
STIX relationship .source_ref and .target_ref	Related Attack Pattern/ Course Of Action/ Signature.Value / Related Signature.Name	N/A	N/A	Attack Pattern ↔ Course Of Action	Relationships are indexed in both directions and applied to supported objects.

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
Attack Patterns	270
Attack Pattern Attributes	1,262
Courses of Action	268
Course of Action Attributes	590
Signatures	191
Signature Attributes	191

Change Log

- **Version 1.0.0**
  - Initial release