ThreatQuotient

A Securonix Company

MITRE D3FEND Operation

Version 1.0.0

December 22, 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

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	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

The MITRE D3FEND operation integrates MITRE ATT&CK techniques with the MITRE D3FEND knowledge base to enhance defensive context and remediation guidance. The operation submits an ATT&CK technique ID to MITRE D3FEND and ingests the associated remediation URI as an attribute, along with relevant properties captured as the attack pattern description.

The integration provides the following operation action:

- **Get Mitre Defend Remediation** - enriches Attack Patterns with Mitre D3FEND remediation properties.

The integration is compatible with Attack Pattern type objects.

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

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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

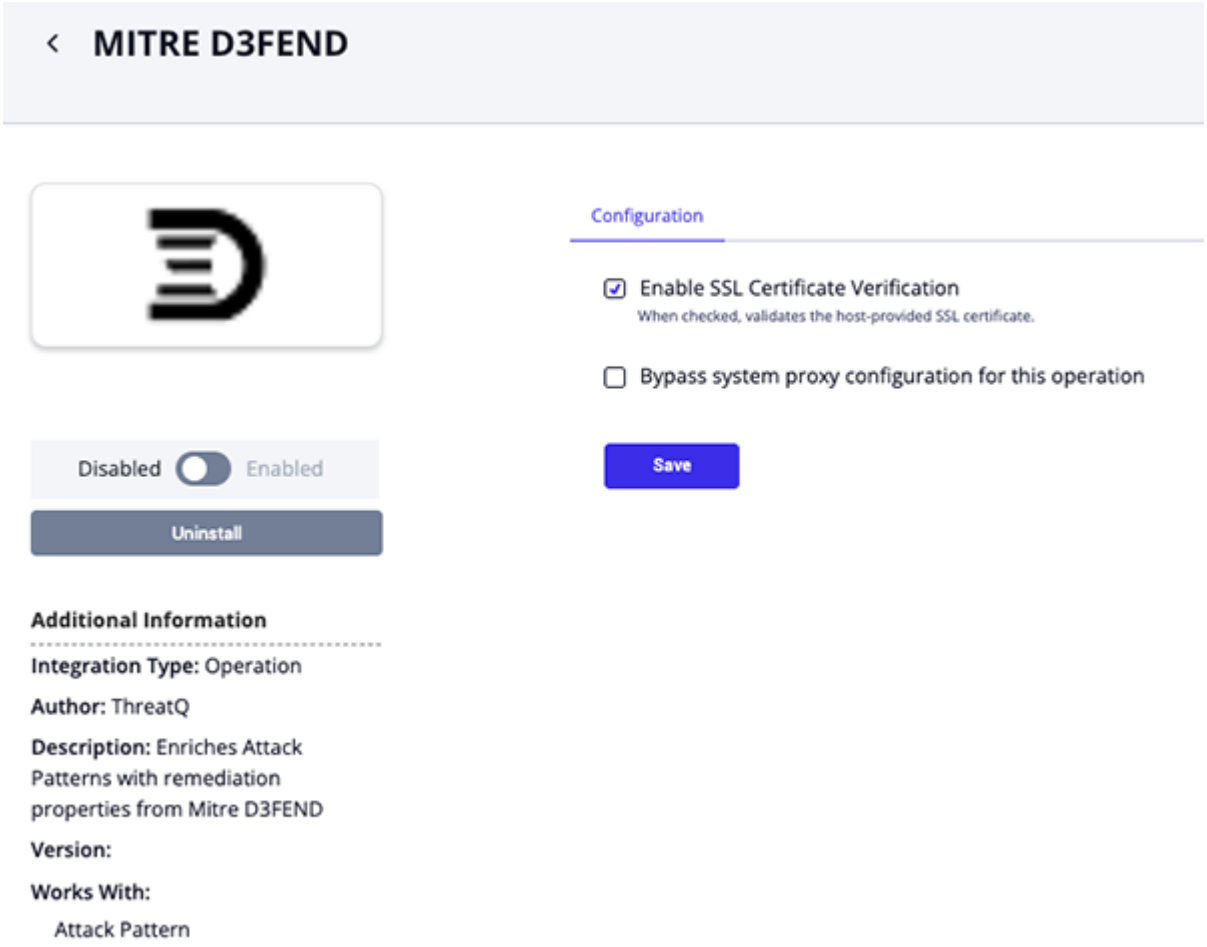
Configuration

> 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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the operation should validate the host-provided SSL certificate.
Bypass System Proxy Configuration for this Operation	Enable this parameter if the operation should not honor proxies set in the ThreatQ UI.



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.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Get Mitre Defend Remediation	Enriches Attack Patterns with Mitre D3FEND remediation properties.	Attack Pattern	N/A

Get Mitre Defend Remediation

The Get Mitre Defend Remediation action sends an ATT&CK technique ID to MITRE D3FEND and ingests remediation URI as attribute and properties as attack pattern description.

```
GET https://d3fend.mitre.org/api/offensive-technique/attack/{technique_id}.json
```

Sample Response:


```
{
    "off_to_def": {
        "head": {
            "vars": [
                "def_tactic_label",
                "def_tactic_rel_label",
                "def_tech_parent_is_toplevel",
                "def_tech_parent_label",
                "def_tech_label",
                "def_tech_id",
                "def_artifact_rel_label",
                "def_artifact_label",
                "sc",
                "off_artifact_label",
                "off_artifact_rel_label",
                "off_tech_label",
                "off_tactic_rel_label",
                "off_tactic_label",
                "def_tactic",
                "def_tactic_rel",
                "def_tech",
                "def_artifact_rel",
                "def_artifact",
                "off_artifact",
                "off_artifact_rel",
                "off_tech",
                "off_tech_id",
                "off_tactic_rel",
                "off_tactic"
            ]
        },
        "results": {
            "bindings": []
        }
    },
    "description": {
        "@context": {
            "rdfs": "http://www.w3.org/2000/01/rdf-schema#",
            "owl": "http://www.w3.org/2002/07/owl#",
            "d3f": "http://d3fend.mitre.org/ontologies/d3fend.owl#",
            "skos": "http://www.w3.org/2004/02/skos/core#"
        },
        "@graph": [
            {
                "@id": "d3f:T1590.006",
                "@type": "owl:Class",
                "d3f:attack-id": "T1590.006",
                "d3f:definition": "Adversaries may gather information about the victim's network security appliances that can be used during targeting. Information about network security appliances may include a variety of details, such as the existence and specifics of deployed firewalls, content filters, and proxies/bastion hosts. Adversaries may also target information about victim network-based intrusion detection systems (NIDS) or other appliances related to defensive cybersecurity operations.",
```

```
                "rdfs:label": "Network Security Appliances",
                "rdfs:subClassOf": {
                    "@id": "d3f:T1590"
                }
            }
        ]
    },
    "subtechniques": {
        "@context": {
            "rdfs": "http://www.w3.org/2000/01/rdf-schema#",
            "owl": "http://www.w3.org/2002/07/owl#",
            "d3f": "http://d3fend.mitre.org/ontologies/d3fend.owl#",
            "skos": "http://www.w3.org/2004/02/skos/core#"
        },
        "@graph": []
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Attack Pattern Attribute	D3FEND ID (URI)	N/A	https://d3fend.mitre.org/offensive-technique/attack/T1590.006/	URI to Mitre D3FEND matrix
`.description.@graph[].d3f:definition`	Attack Pattern Description	N/A	N/A	`Adversaries may gather information about the victim's network ...`	N/A

Change Log

- **Version 1.0.0**
  - Initial release