

ThreatQuotient

A Securonix Company



Shadowserver Operation

Version 1.0.0

October 26, 2026

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 **ThreatQ Supported**

Support

Email: support@securonix.com

Web: <https://ts.securonix.com>

Phone: 703.574.9893

Contents

Warning and Disclaimer..... 3

Support..... 4

Integration Details..... 5

Introduction 6

Installation 7

Configuration 8

Actions 9

 Enrich 9

Change Log 14

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.

Copyright © 2026 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: 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	>= 4.35.0
---	-----------

Support Tier	ThreatQ Supported
---------------------	-------------------

Introduction

The Shadowserver Operation for ThreatQ enables analysts to fetch enrichment context from the Shadowserver API.

The integration provides the following operation action:

- **Enrich** - enriches a submitted hash with context from Shadowserver.

The integration is compatible with the following indicator types:

- MD5
- SHA-1
- SHA-256
- SHA-512

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. 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.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Enrich	Enriches a hash with context from Shadowserver.	Indicators	(MD5, SHA-1, SHA-256, SHA-512)

Enrich

The Enrich action enriches a submitted hash with context from Shadowserver.

GET <https://api.shadowserver.org/malware/info>

Sample Response:

```
[
  {
    "timestamp": "2016-08-25 02:44:39",
    "tlsh":
    "c1b52a5273fa0254f2f35f75a8b7a3944939fea11d22e08e1164314d88b6f808e75b
    b7",
    "md5": "dfe1832e02888422f48d6896dc8e8f73",
    "magic": "PE32 executable (GUI) Intel 80386, for MS Windows",
    "anti_virus": [
      {
        "vendor": "Fortinet",
        "signature": "W32/Lamer.CQ"
      },
      {
        "vendor": "Avast",
        "signature": "Win32:Lamer-A"
      },
      {
        "signature": "Win32.Generic.VC",
        "vendor": "AVG"
      },
    ],
  },
]
```

```

{
  "signature": "Win32:Malware-gen",
  "vendor": "Avast"
},
{
  "vendor": "K7GW",
  "signature": "Virus ( 004d554e1 )"
},
{
  "vendor": "MicroWorld",
  "signature": "Gen:Win32.FileInfector.uwZ@a4T!Kcmi"
},
{
  "vendor": "Sophos",
  "signature": "Troj/Agent-APCU"
},
{
  "vendor": "Eset",
  "signature": "Win32/Zatoxp.C"
},
{
  "vendor": "K7",
  "signature": "Virus ( 004d554e1 )"
},
{
  "signature": "Win32:Malware-gen",
  "vendor": "Avast"
},
{
  "signature": "TR/Dropper.Gen8",
  "vendor": "Avira"
},
{
  "vendor": "BitDefender",
  "signature": "Gen:Win32.Backdoor.ozZbauKWKdpb"
},
{
  "vendor": "DrWeb",
  "signature": "Win32.HLLW.Siggen.4657"
},
{
  "signature": "Virus ( 004d554e1 )",

```

```

        "vendor": "K7GW"
    },
    {
        "vendor": "AhnLab",
        "signature": "Trojan/Win32.FileInfector"
    },
    {
        "signature": "Trojan/Win32.FileInfector",
        "vendor": "AhnLab"
    },
    {
        "vendor": "QuickHeal",
        "signature": "W32.Sivis.A5"
    },
    {
        "signature": "PUA.Win.Packer.Purebasic-2",
        "vendor": "Clam"
    },
    {
        "signature": "Gen:Win32.FileInfector.uwZ@a4T!Kcmi",
        "vendor": "BitDefender"
    },
    {
        "signature": "Win32.Generic.VC",
        "vendor": "AVG"
    },
    {
        "signature": "Gen.Win32.FileInfector",
        "vendor": "Ikarus"
    },
    {
        "vendor": "BitDefender",
        "signature": "Trojan.PWS.Onlinegames.KEGA"
    },
    {
        "signature": "Trojan.GenericKD.40542465",
        "vendor": "BitDefender"
    },
    {
        "vendor": "BitDefender",
        "signature": "Gen:Win32.FileInfector.uwZ@a4T!Kcmi"
    },
    },

```

```

        {
            "vendor": "Clam",
            "signature": "PUA.Win.Packer.Purebasic-2"
        },
        {
            "vendor": "Sunbelt",
            "signature": "Virus.Win32.sivis.a"
        }
    ],
    "pehash": "243c35935ecc9829f30b30c45839cbf6",
    "adobe_malware_classifier": "malicious",
    "import_hash": "33f98db5bdb6a7013d52f0120248df35",
    "sha1": "c56ba498d41caa7be3c1eb5588cec27c413eb208",
    "last_seen": "2016-08-25 02:44:39",
    "type": "exe",
    "filesize": "2438340",
    "entropic": "5.952427",
    "sha512":
    "7ca1fdfe537913b8854227efc1f11b00d405f2d21e416e7023c4ebed2bfa887d2bc4
    d4d553ce41667c99def47ea05e6ce4a773c4ee7173927f1d263e724c16c2",
    "first_seen": "2016-08-25 02:44:39",
    "sha256":
    "d8d395f8744335fba53b0a4308e7b380a0aca86bfc8939ded9f4c8c5cb1e838a"
    }
]

```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.first_seen	Attribute	First Seen	N/A	2021-01-01 01:01:01	N/A
.last_seen	Attribute	Last Seen	N/A	2021-01-01 01:01:01	N/A
.sha1	Indicator Value	SHA-1	N/A	N/A	N/A
.sha256	Indicator Value	SHA-256	N/A	N/A	N/A
.md5	Indicator Value	MD5	N/A	N/A	N/A
.sha512	Indicator Value	SHA-512	N/A	N/A	N/A
.type	Attribute	File Type	N/A	exe	N/A
.filesize	Attribute	File Size	N/A	exe	N/A
.type	Attribute	File Type	N/A	exe	N/A
.magic	Attribute	File Magic	N/A	exe	N/A
.adobe_malware_classifier	Attribute	Malware Classifier	N/A	malicious	N/A
.entropic	Attribute	Entropy	N/A	5.4213	N/A
.anti_virus[].signature	Attribute	Detection Signature	N/A	Win32.Generic.VC	N/A

Change Log

- **Version 1.0.0**
 - Initial release