

ThreatQuotient



Zeek Indicator Exports User Guide

Version 1.0.0 rev-a

August 14, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 **ThreatQ Supported**

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer 3

Support 4

Export Details..... 5

Introduction 6

Creating the Export 7

Change Log 9

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 © 2023 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@threatq.com

Support Web: <https://support.threatq.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.

Export Details

ThreatQuotient provides the following details for this export:

Current Guide Version	1.0.0
------------------------------	-------

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

Introduction

This guide provides steps to export Zeek indicators for use with an external threat detection system.

Creating the Export

The following section will detail how to create the exports in ThreatQ.



See the Managing Exports topic for more details on ThreatQ exports.

1. Select the **Settings icon > Exports**.

The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**

The Connection Settings dialog box appears.

3. Enter an **Export Name**.

4. Click **Next Step**.

The Output Format dialog box appears.

5. Provide the following information based on the type of indicator:

Tenable FQDNs

FIELD	VALUE
Which type of information would you like to export?	Indicators
Output Type	text/plain
Special Parameters	<code>indicator.status=Active&indicator.deleted=N</code>

6. Enter the following for the **Output Template**:

```
<> #fields{$tab}indicator{$tab}indicator_type{$tab}meta.source{$tab}
meta.url
{foreach $data as $indicator}
{$indicator_type=""}
{$source_found=0}
{if $indicator.type eq "CIDR Block"}
{$indicator_type="Intel::SUBNET"}{/if}
{if $indicator.type eq "IP Address"}
{$indicator_type="Intel::ADDR"}{/if}
{if $indicator.type eq "URL"}{$indicator_type="Intel::URL"}{/if}
{if $indicator.type eq "Email Address"}
{$indicator_type="Intel::EMAIL"}{/if}
{if $indicator.type eq "FQDN"}{$indicator_type="Intel::DOMAIN"}{/if}
{if $indicator.type eq "MD5"}{$indicator_type="Intel::FILE_HASH"}
{/if}
{if $indicator.type eq "SHA-1"}
{$indicator_type="Intel::FILE_HASH"}{/if}
{if $indicator.type eq "SHA-256"}
{$indicator_type="Intel::FILE_HASH"}{/if}
{if $indicator.type eq "SHA-384"}
{$indicator_type="Intel::FILE_HASH"}{/if}
{if $indicator.type eq "SHA-512"}
{$indicator_type="Intel::FILE_HASH"}{/if}
{if $indicator.type eq "Filename"}
{$indicator_type="Intel::FILE_HASH"}{/if}
{if $indicator_type ne ""}
{$indicator.value}{$tab}{$indicator_type}{$tab}{foreach
$indicator.Sources item=source name=Sources}{if
$smartyy.foreach.Sources.first == true}
{$source.value}{$source_found=1}{/if}{/foreach}{if $source_found
== 0}-{/if}
{$tab}https://{http_host}/indicators/{$indicator.id}/details
{/if}
{/foreach}
```

7. Click on **Save Settings** and enable the export via the On/Off toggle switch.

Change Log

- **Version 1.0.0 rev-a**
 - Removed a duplicate line in the output template.
- **Version 1.0.0**
 - Initial release