ThreatQuotient

ThreatQuotient for FireEye AX Operation

Version 1.0.0

April 24, 2019

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: + 1 703.574.9893

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.

Last Updated: Monday, 24 April 2019

Contents

List of Figures and Tables

Introduction

1.1 Application Function

The ThreatQuotient for FireEye AX Operation provides a ThreatQ user with the ability to interact with their FireEye AX appliance. Users can submit files for analysis, as well as retrieve the reports back so the results can be added to ThreatQ as context. ThreatQ users can also query their FireEye AX appliance using indicators from ThreatQ to find any alerts related to those indicators. Lastly, this operation allows ThreatQ users to seamlessly add and remove YARA rules from their FireEye AX appliance.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for FireEye AX Operation. This document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning the ThreatQuotient Apps and integrations covered within the document, as well as the experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ and Security Engineers
2. ThreatQuotient Professional Services Project Team & Engineers

1.4 Scope

This document covers the implementation of the application only.

Table 1: ThreatQuotient Software & App Version Information

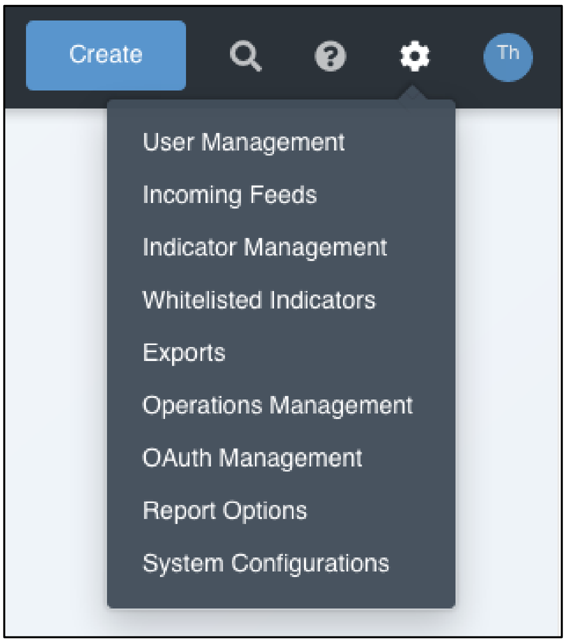
Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for FireEye AX Operation	Version 1.0.0	

1.5 Setting up the Integration

Ensure the file `tq_op_fireeye_ax-1.0.0-py3-none-any.whl` is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient for FireEye AX Operation is being installed or upgraded.

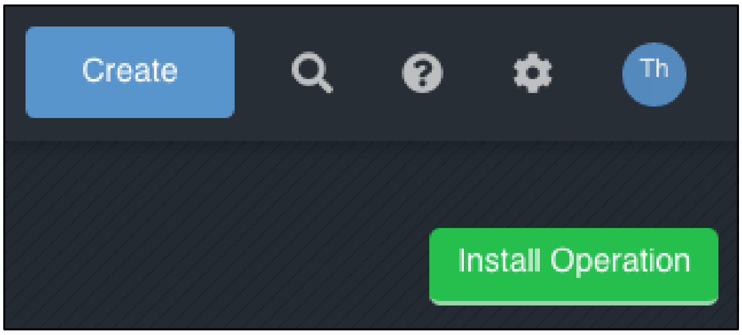
1. Navigate to the **Settings icon** > **Operations Management**.

Figure 1: Operations Management – Install



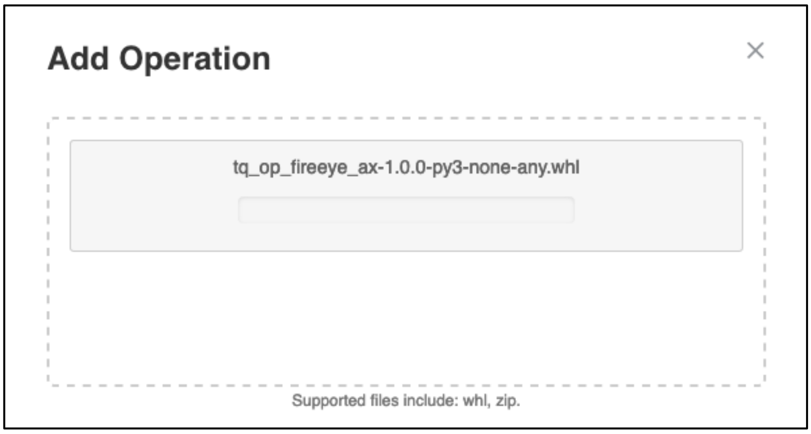
2. Click **Install Operation** in the upper right corner.

Figure 2: Install Operation



3. Drag the `tq_op_fireeye_ax-1.0.0-py3-none-any.whl` to the Add Operation Popup or **Click to Browse** and browse to the required file.

Figure 3: Add Operation



Add Operation

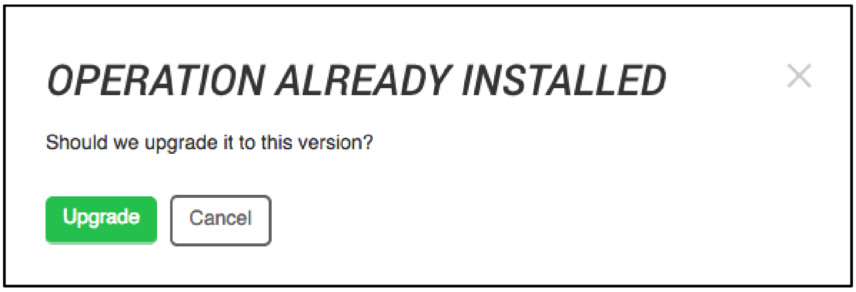
tq_op_fireeye_ax-1.0.0-py3-none-any.whl

Supported files include: whl, zip.

4. Click **Install** or **Upgrade**.

You may be presented with OPERATION ALREADY INSTALLED as shown below.

Figure 4: Add Operation



OPERATION ALREADY INSTALLED

Should we upgrade it to this version?

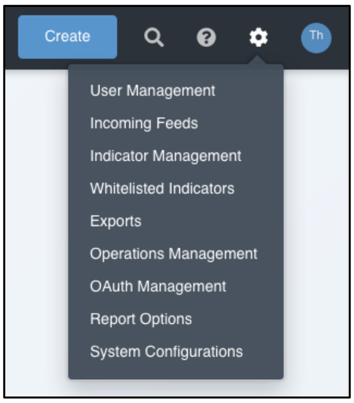
5. Installation / Upgrade is now complete.

1.6 Configuring the Operation

The following section covers the configuration of the ThreatQuotient for FireEye AX Operation.

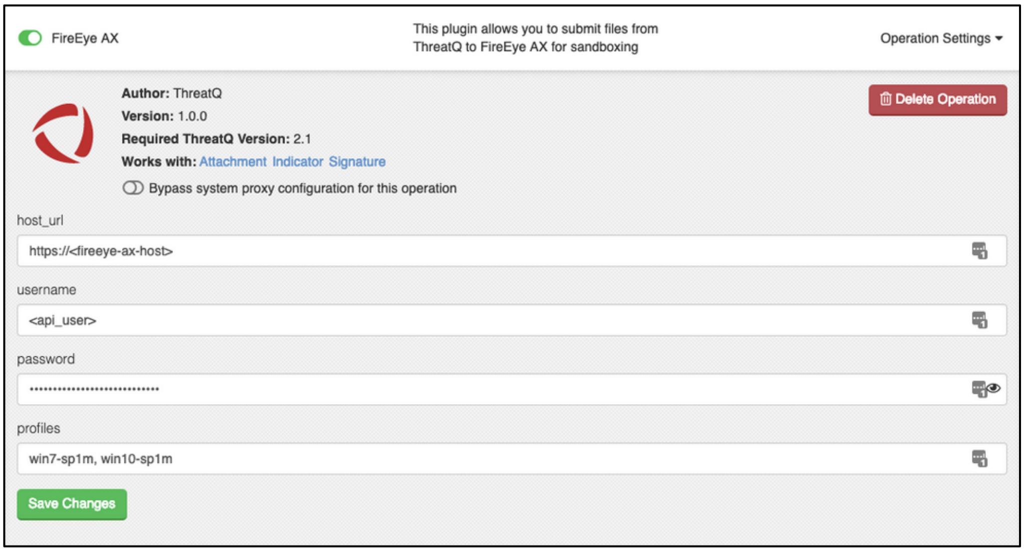
1. Navigate to the **Settings icon** > **Operations Management**.

Figure 5: Operations Management – Configuration



2. Expand the **Operations Settings** configuration.

Figure 6: Operation Configuration



FireEye AX

This plugin allows you to submit files from ThreatQ to FireEye AX for sandboxing

Author: ThreatQ
Version: 1.0.0
Required ThreatQ Version: 2.1
Works with: Attachment Indicator Signature

○ Bypass system proxy configuration for this operation

host_url
https://<fireeye-ax-host>

username
<api_user>

password
••••••••••••••••••••••••••••••

profiles
win7-sp1m, win10-sp1m

3. Input the **host_url**: Your FireEye AX Host IP or FQDN.
4. Input your FireEye AX **Username**: the username associated with your FireEye AX host.
5. Input your FireEye AX **password:** the password associated with your username for the FireEye AX host account above.
6. Input the **Profiles**: The sandboxing profiles to use to sandbox the samples.
   - Example: win7-sp1m (see FireEye AX UI for more options).
   - Multiple profiles can be specified by making a comma-separated list in this field.
   - This can be overridden when using the operation (as a parameter).
7. Click **Save Changes**. The operation is now ready for use.

1.7 Using the Operation

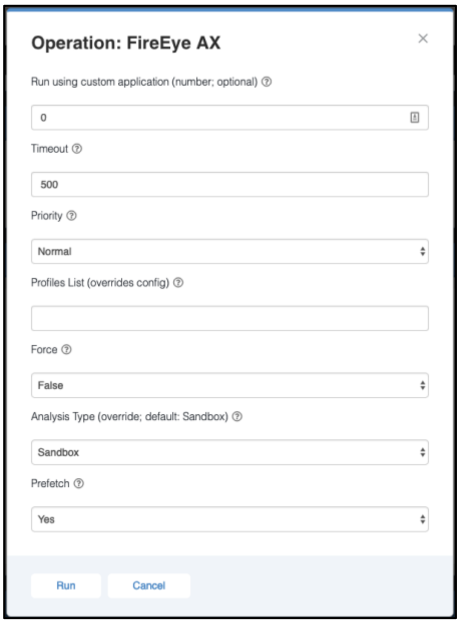
The following section covers the use of the ThreatQuotient for FireEye AX Operation.
There are 5 actions that can be carried out with this operation.

- Submit
- Get Reports
- Add a YARA Rule
- Remove a YARA Rule
- Query Alerts

1.7.1 Submit

This action will submit a file (attachment) or a URL/FQDN to FireEye AX for sandboxing parameters.

Figure 7: Operation Submit Parameters Use



Operation: FireEye AX

Run using custom application (number; optional): 0

Timeout: 500

Priority: Normal

Profiles List (overrides config):

Force: False

Analysis Type (override; default: Sandbox): Sandbox

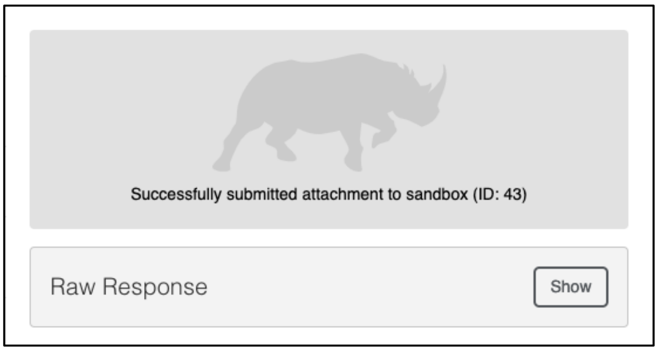
Prefetch: Yes

- **Run using custom application (number; optional)**: This option allows you to run the sample with a specific application within the sandbox profile.
  - This is a number corresponding to the custom application.
  - The default is '0', which basically asks FireEye AX to determine the application to use.
- **Timeout**: This option determines how long the sandbox will take to "timeout" after inactivity (default: 500).
- **Priority**: This option allows you to prioritize the task.
  - Options: Normal (default) or Urgent
- **Profiles List (overrides config)**: This is a list of profiles to use to sandbox the sample. The action will use the profiles set in the UI configuration if this is left blank. Otherwise, this will override the profiles listed in the UI configuration.
- **Force**: This option allows you to force resubmit a sample. If this is set to False, it will mark the sample as a duplicate and will not resubmit it.
- **Analysis Type (override; default: Sandbox)**: This allows you to set the analysis type. The default is Sandbox.

- **Prefetch**: Specifies whether to determine the file target based on an internal determination rather than browsing to the target location.
    - If you are using the Sandbox analysis type, this must be set to 1.

An example output can be seen below:

Figure 8: Submit Operation Example Result

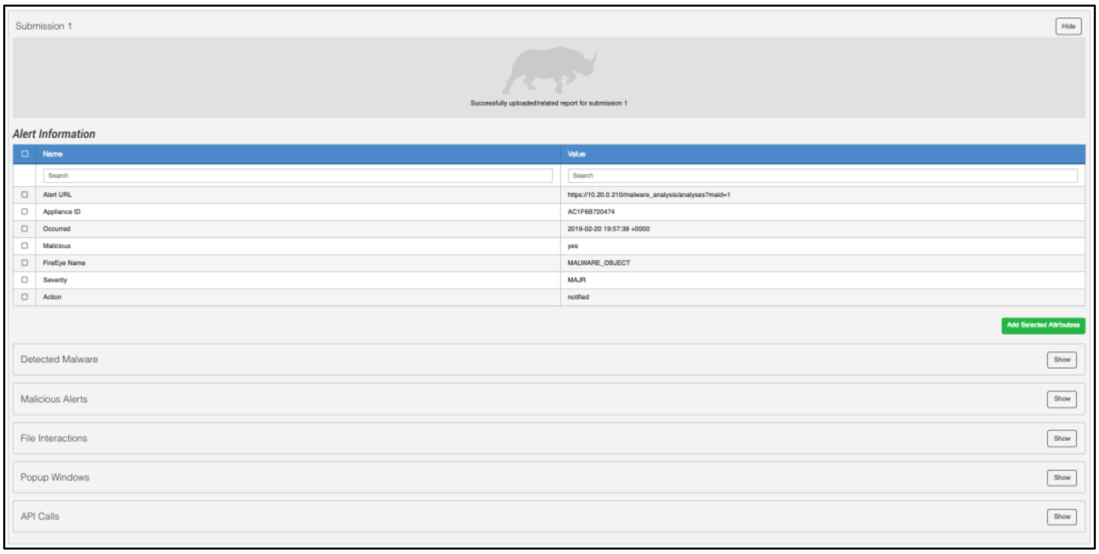


Successfully submitted attachment to sandbox (ID: 43)

1.7.2 Get Reports

This action will get all the reports for the sample, with the only condition being that the sample (in ThreatQ) has an attribute with the name "FireEye AX Submission ID" and the value will be the submission ID. For each of these attributes, it will fetch a report correlating to the submission ID. If submission results are found, results will be shown and the full JSON report will be uploaded and related to the sample in ThreatQ.

Figure 9: Get Report Operation Example

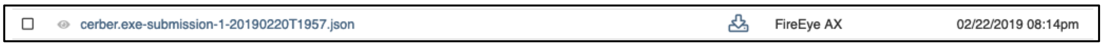


Successfully uploaded/related report for submission 1

Alert Information

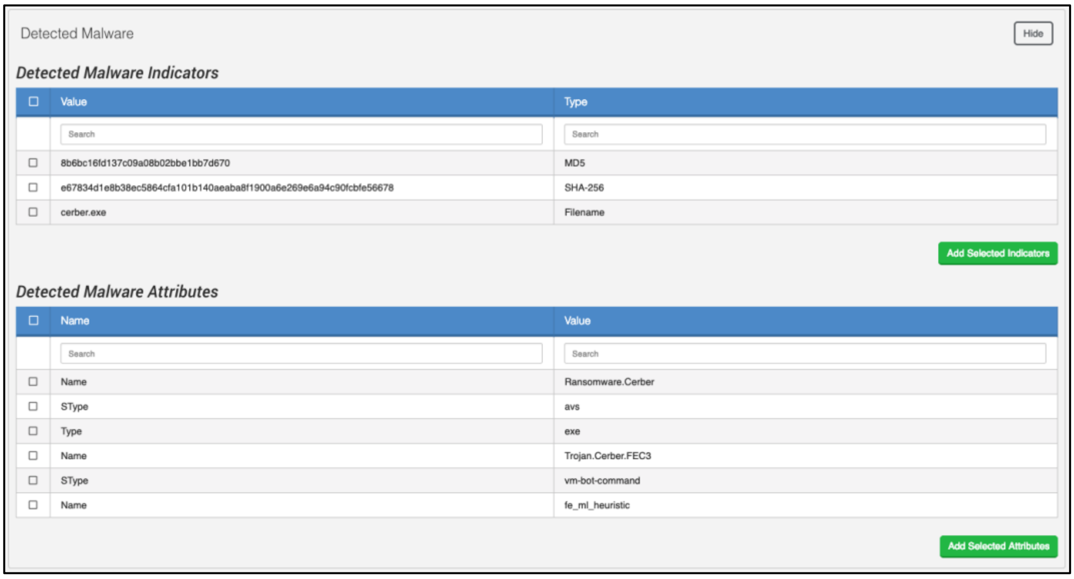
□	Name	Value
	Search	Search
□	Alert URL	https://10.20.0.210/malware_analysis/analyses?maid=1
□	Appliance ID	AC1F6B720474
□	Occurred	2019-02-20 19:57:39 +0000
□	Malicious	yes
□	FireEye Name	MALWARE_OBJECT
□	Severity	MAJR
□	Action	notified

Figure 10: Get Report Operation Related Report Example



□	cerber.exe-submission-1-20190220T1957.json	FireEye AX	02/22/2019 08:14pm

Figure 11: Get Report Operation Detected Malware Example



Detected Malware

Hide

Detected Malware Indicators

□	Value	Type
	Search	Search
□	8b6bc16fd137c09a08b02bbe1bb7d670	MD5
□	e67834d1e8b38ec5864cfa101b140aeaba8f1900a6e269e6a94c90fcbfe56678	SHA-256
□	cerber.exe	Filename

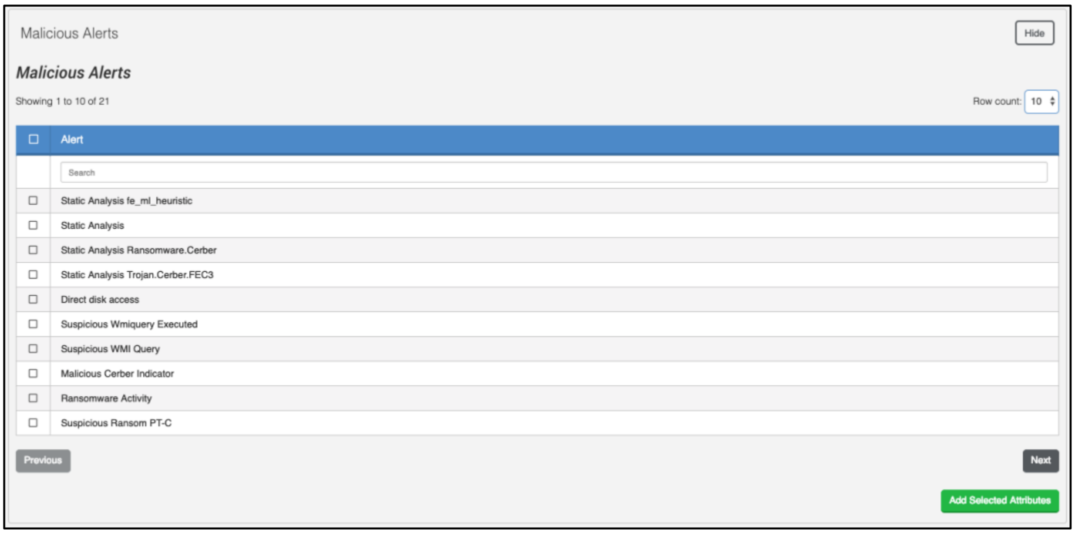
Add Selected Indicators

Detected Malware Attributes

□	Name	Value
	Search	Search
□	Name	Ransomware.Cerber
□	SType	avs
□	Type	exe
□	Name	Trojan.Cerber.FEC3
□	SType	vm-bot-command
□	Name	fe_ml_heuristic

Add Selected Attributes

Figure 12: Get Report Operation Malicious Alerts Example



Malicious Alerts

Hide

Malicious Alerts

Showing 1 to 10 of 21

Row count: 10

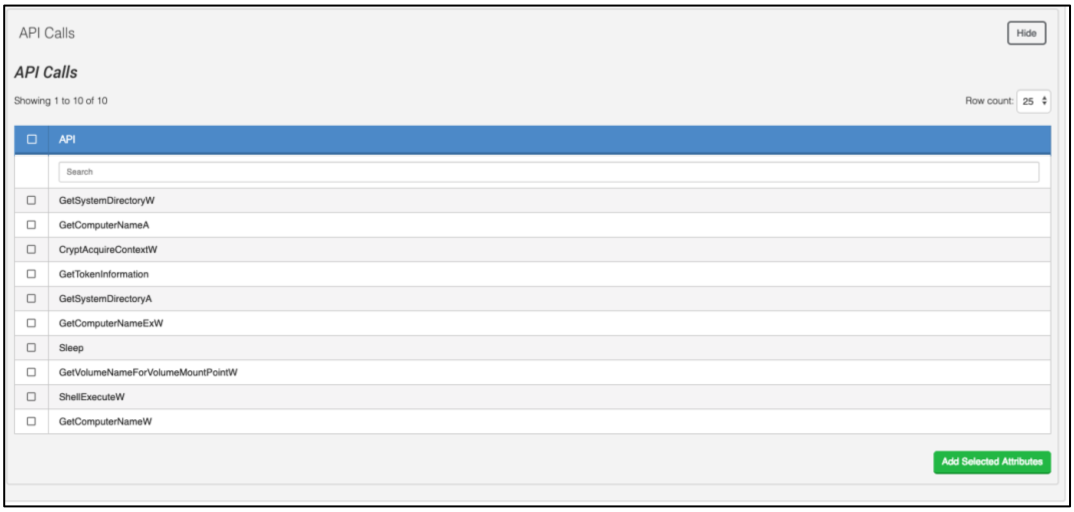
□	Alert
	Search
□	Static Analysis fe_ml_heuristic
□	Static Analysis
□	Static Analysis Ransomware.Cerber
□	Static Analysis Trojan.Cerber.FEC3
□	Direct disk access
□	Suspicious Wmiquery Executed
□	Suspicious WMI Query
□	Malicious Cerber Indicator
□	Ransomware Activity
□	Suspicious Ransom PT-C

Previous

Next

Add Selected Attributes

Figure 13: Get Report Operation API Calls Example



API Calls

Hide

API Calls

Showing 1 to 10 of 10

Row count: 25

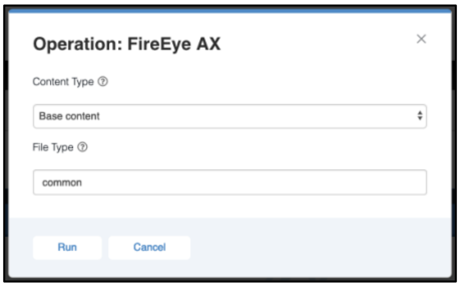
□	API
	Search
□	GetSystemDirectoryW
□	GetComputerNameA
□	CryptAcquireContextW
□	GetTokenInformation
□	GetSystemDirectoryA
□	GetComputerNameExW
□	Sleep
□	GetVolumeNameForVolumeMountPointW
□	ShellExecuteW
□	GetComputerNameW

Add Selected Attributes

1.7.3 Add a YARA Rule

This action will allow you to add YARA rules from ThreatQ to FireEye AX.

Figure 14: Operation Add Yara Parameters Use Example



Operation: FireEye AX

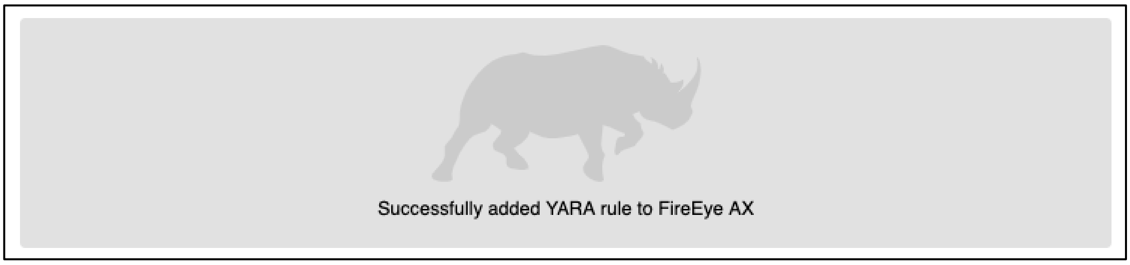
Content Type: Base content

File Type: common

- **Content Type**: Specifies which content type the new YARA rule should be applied to.
  - Active content: Extracts the macros from files and executes special YARA rules on them.
  - Base (default): If file contains a macro, do not extract and analyse macros; only analyse the base file.
  - All: Does both
- **File Type**: The file type of the YARA rules file being submitted, such as exe, pdf, or ppt.
  - Default: `common`

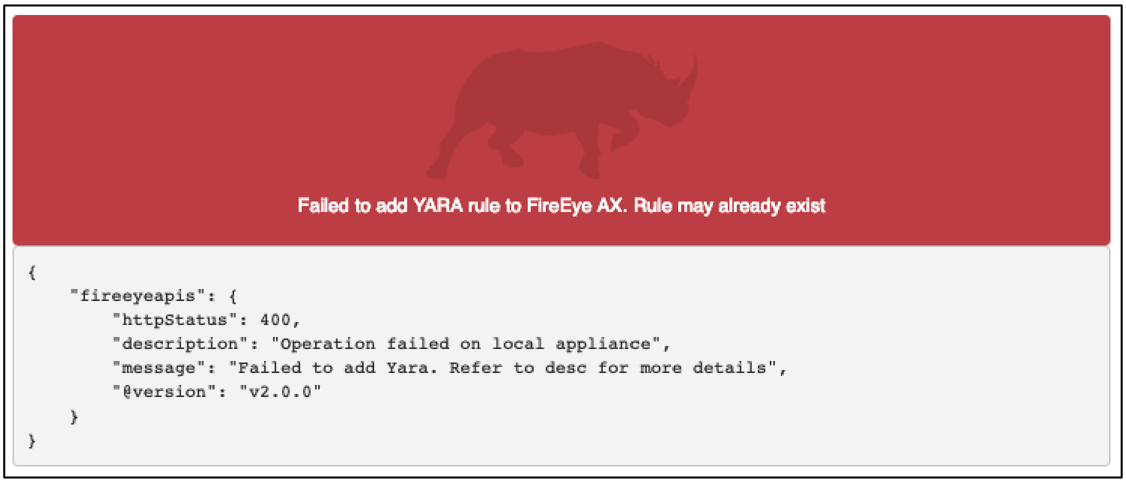
Examples of both a successful addition of a YARA rule and an Unsuccessful addition.

Figure 15: Operation Add Yara Parameters Success Example



Successfully added YARA rule to FireEye AX

Figure 16: Operation Add Yara Parameters Unsuccessful Example



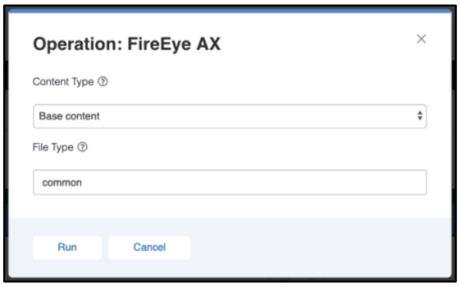
Failed to add YARA rule to FireEye AX. Rule may already exist

```
{
    "fireeyeapis": {
        "httpStatus": 400,
        "description": "Operation failed on local appliance",
        "message": "Failed to add Yara. Refer to desc for more details",
        "@version": "v2.0.0"
    }
}
```

1.7.4 Remove a YARA Rule

This action will allow you to remove YARA rules from ThreatQ to FireEye AX.

Figure 17: Operation Remove Yara Parameters Use Example



Operation: FireEye AX

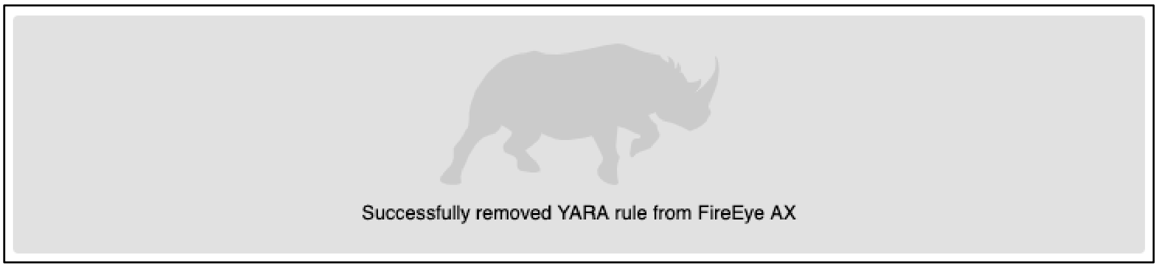
Content Type: Base content

File Type: common

- **Content Type**: Specifies which content type where the new YARA rule should be applied.
  - Active content: Extracts the macros from files and executes special YARA rules on them.
  - Base (default): If file contains a macro, do not extract and analyze macros; only analyze the base file.
  - All: Does both
- **File Type**: The file type of the YARA rules file being submitted, such as exe, pdf, or ppt.
  - Default: `common`

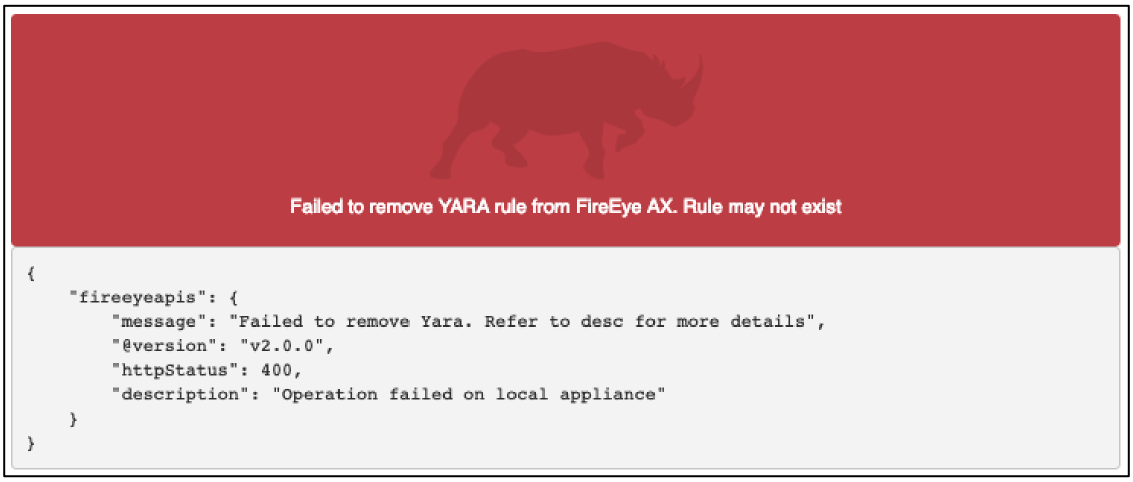
Examples of both a successful removal of a YARA rule and an Unsuccessful removal.

Figure 18: Operation Remove Yara Parameters Success Example



Successfully removed YARA rule from FireEye AX

Figure 19: Operation Remove Yara Parameters Unsuccessful Example



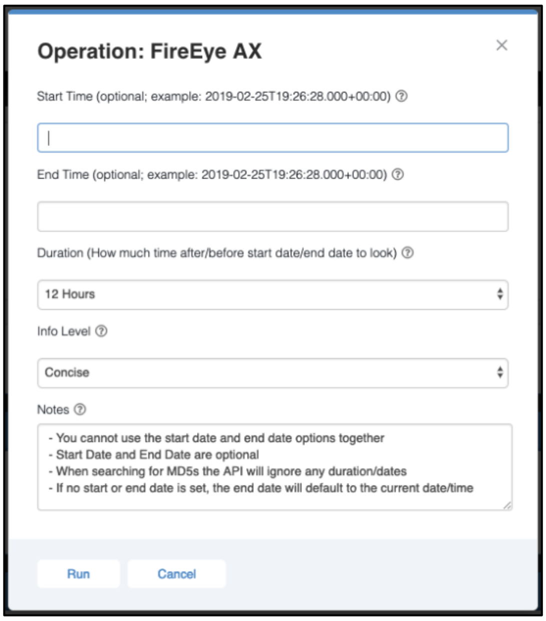
Failed to remove YARA rule from FireEye AX. Rule may not exist

```
{
    "fireeyeapis": {
        "message": "Failed to remove Yara. Refer to desc for more details",
        "@version": "v2.0.0",
        "httpStatus": 400,
        "description": "Operation failed on local appliance"
    }
}
```

1.7.5 Query Alerts

This action allows you to query alerts in FireEye AX. This action only applies to FQDNs, Filenames, Emails, and IP Addresses.

Figure 20: Operation Query Alerts Parameters Use



Operation: FireEye AX

Start Time (optional; example: 2019-02-25T19:26:28.000+00:00)

End Time (optional; example: 2019-02-25T19:26:28.000+00:00)

Duration (How much time after/before start date/end date to look): 12 Hours

Info Level: Concise

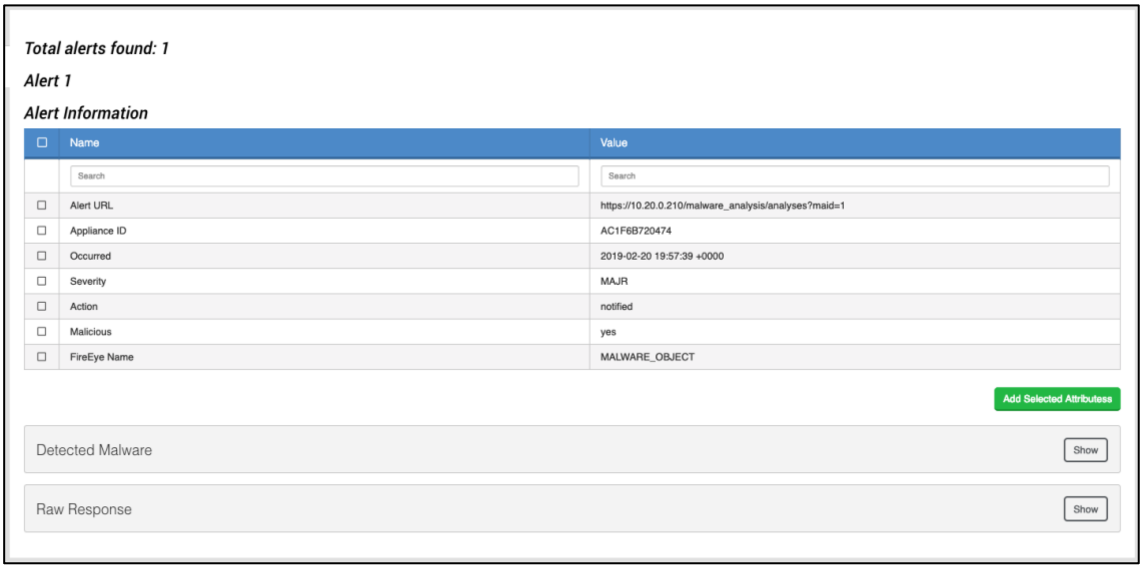
Notes

- You cannot use the start date and end date options together
- Start Date and End Date are optional
- When searching for MD5s the API will ignore any duration/dates
- If no start or end date is set, the end date will default to the current date/time

- **Start Time (optional)**: This allows you to set the start time to search for alerts. This is used in conjunction with the Duration parameter. You cannot use this at the same time as using the End Time parameter.
  - Format: YYYY-MM-DDTHH:mm:ss.sss-OH:om
  - Example: 2019-02-21T16:30:00.000-07:00
- **End Time (optional)**: This allows you to set the end time to search for alerts. This is used in conjunction with the Duration parameter. You cannot use this at the same time as using the Start Time parameter.
  - Format: YYYY-MM-DDTHH:mm:ss.sss-OH:om
  - Example: 2019-02-21T16:30:00.000-07:00
  - If no end time or start time is provided, the end time will be set to the current date/time.
- **Duration (How much time after/before start date/end date to look)**: This option allows you to set the amount of time you want to either look after a start time or before an end time. This field defaults to 12 hours.
- **Info Level**: This field allows you to set the detail level of the alerts.
  - Choices: Concise (default), Normal, Extended
  - Normal and Extended will provide a very large alert and may take longer to download.
- **Notes**: This field can be ignored. It is just some notes to give you more information/context.

An example of a successful query request can be seen below.

__Figure 21: Operation Query Alerts Success Example__



__Total alerts found: 1__

__Alert 1__

__Alert Information__

□	Name	Value
	Search	Search
□	Alert URL	https://10.20.0.210/malware_analysis/analyses?maid=1
□	Appliance ID	AC1F6B720474
□	Occurred	2019-02-20 19:57:39 +0000
□	Severity	MAJR
□	Action	notified
□	Malicious	yes
□	FireEye Name	MALWARE_OBJECT

Trademarks and Disclaimers

THE SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE TERMS AND CONDITIONS WHEN PURCHASED. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing.
Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer’s responsibility.
In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.