# ThreatQuotient

## ThreatQ ChatGPT Operation User Guide

**Version 1.0.0**

October 03, 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

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**: 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.

# Integration Details

ThreatQuotient provides the following details for this integration:

| | |
|---|---|
| **Current Integration Version** | 1.0.0 |
| **Compatible with ThreatQ Versions** | >= 5.6.0 |
| **ChatGPT Version** | 3.5 |
| **Support Tier** | ThreatQ Supported |

# Introduction

The ThreatQ ChatGPT Operation queries ChatGPT for information on user-selected objects in the ThreatQ Threat Library.

The operation provides the following actions:

- **Tool Query -** queries ChatGPT for information on the tool object submitted.
- **Adversary Query -** queries ChatGPT for information on the adversary object submitted.
- **Malware Query -** queries ChatGPT for information on the malware object submitted.

The operation is able to work on the following object types:

- Malware
- Adversary
- Tool

# Prerequisites

The operation requires an OpenAI API Key which can be generated at https://platform.openai.com/account/api-keys.

As of this publication, users can generate and use a 3.5 API account for free with limited use. ThreatQuotient recommends upgrading to a paid OpenAI account when deploying this operation into production.

# 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.

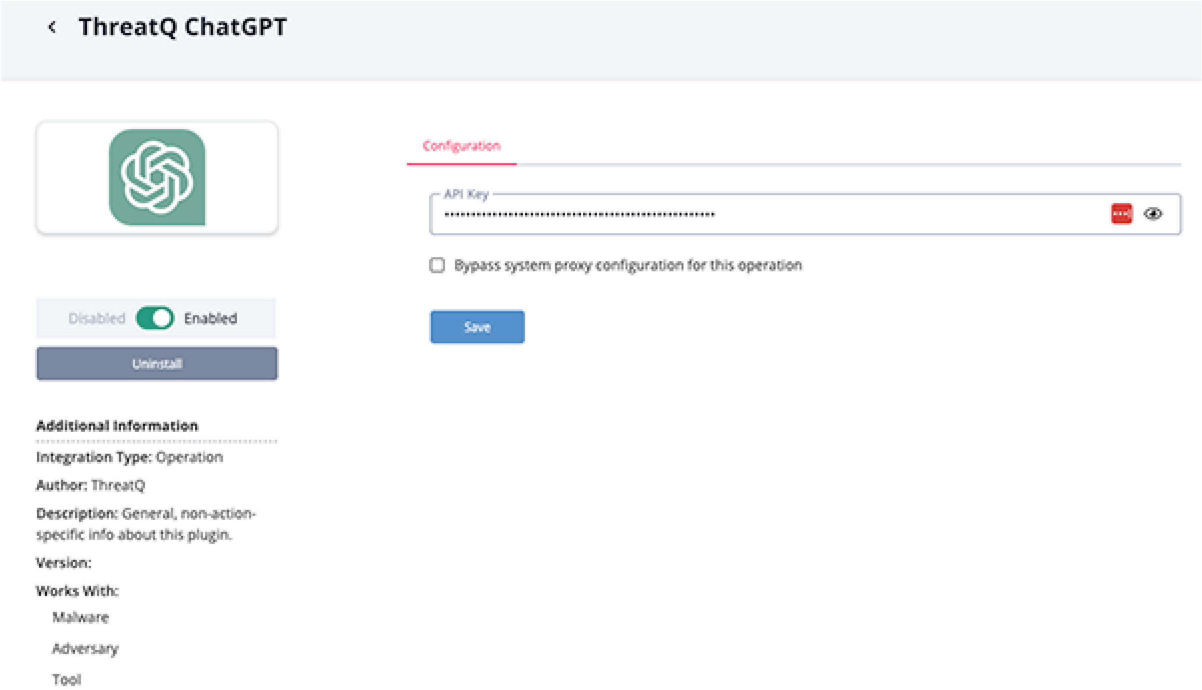
# Configuration

> 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 parameter under the **Configuration** tab:

| PARAMETER | DESCRIPTION |
|---|---|
| **API Key** | API key to be used for the ChatGPT API |



API Key ••••••••••••••••••••••••••••••••••••••••••••••••••••••

□ Bypass system proxy configuration for this operation

Additional Information

Integration Type: Operation

Author: ThreatQ

Description: General, non-action-specific info about this plugin.

Version:

Works With:

Malware

Adversary

Tool

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 actions:

| ACTION | DESCRIPTION | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|---|
| **Malware Query** | Query the ChatGPT for malware information. | Malware | N/A |
| **Adversary Query** | Query the ChatGPT for adversary information. | Adversary | N/A |
| **Tool Query** | Query the ChatGPT for tool information. | Tool | N/A |

> All actions share the same mapping table.  The run parameters will differ based on the action.

## Action Mapping

All actions query ChatGPT for information on the submitted object.

> See the individual run parameters for what type of information can be retrieved for each object type.

`{{ POST }} https://api.openai.com/v1/chat/completions`

**Sample Response:**

```
{
  'usage': {
    'prompt_tokens': 20,
    'completion_tokens': 536,
    'total_tokens': 556
  },
  'object': 'chat.completion',
  'choices': [
    {
      'message': {
        'content': "To protect your organization from PowerNasa, a
comprehensive strategy should include the following steps:\n\n1. Educate
Employees: Train your employees about the risks associated with PowerNasa and
other similar threats. Teach them about phishing emails, suspicious
attachments, and the importance of not clicking on unknown links.\n\n2.
Implement Strong Password Policies: Enforce strong password policies across
your organization. Encourage employees to use unique, complex passwords and
enable multi-factor authentication (MFA) wherever possible.\n\n3. Keep Software
Up to Date: Regularly update all software, including operating systems,
antivirus programs, and other security tools. This helps to patch any
vulnerabilities that could be exploited by PowerNasa or other malware.\n\n4.
Use Advanced Endpoint Protection: Deploy advanced endpoint protection solutions
that can detect and block PowerNasa and other advanced threats. These solutions
use machine learning and behavior analysis to identify and stop malicious
activities.\n\n5. Secure Email Gateways: Implement secure email gateways that
can filter out phishing emails and malicious attachments. These gateways can
help prevent employees from falling victim to PowerNasa attacks delivered
through email.\n\n6. Regularly Backup Data: Implement a robust backup strategy
to ensure critical data is regularly backed up and stored securely. This helps
to mitigate the impact of a PowerNasa attack or any other data loss event.
\n\n7. Network Segmentation: Implement network segmentation to isolate critical
systems and sensitive data from the rest of the network. This helps contain the
spread of PowerNasa or other malware in case of a successful breach.\n\n8.
Conduct Regular Security Audits: Perform regular security audits to identify
any vulnerabilities or weaknesses in your organization's infrastructure. This
includes penetration testing, vulnerability scanning, and code reviews.\n\n9.
Employee Awareness Training: Conduct regular security awareness training
sessions to keep employees updated on the latest threats, including PowerNasa.
Teach them how to identify suspicious activities and report them to the IT
department.\n\n10. Incident Response Plan: Develop a comprehensive incident
response plan that outlines the steps to be taken in case of a PowerNasa attack
or any other security incident. This plan should include procedures for
containment, eradication, and recovery.\n\n11. Continuous Monitoring: Implement
a robust security monitoring system that can detect and alert on any suspicious
activities or anomalies. This helps in early detection and response to
PowerNasa attacks.\n\n12. Engage a Cybersecurity Provider: Consider engaging a
cybersecurity provider to assist with threat intelligence, incident response,
and ongoing monitoring. They can provide expertise and resources to enhance
your organization's security posture.\n\nRemember, cybersecurity is an ongoing
process, and it is crucial to regularly review and update your strategy to
adapt to evolving threats like PowerNasa.",
        'role': 'assistant'
      },
      'finish_reason': 'stop',
      'index': 0
    }
  ],
  'id': 'chatcmpl-8562MFzE1WPKRSTDTlxi04eJ1o9Q7',
  'created': 1696225538,
  'model': 'gpt-3.5-turbo-0613'
}
```

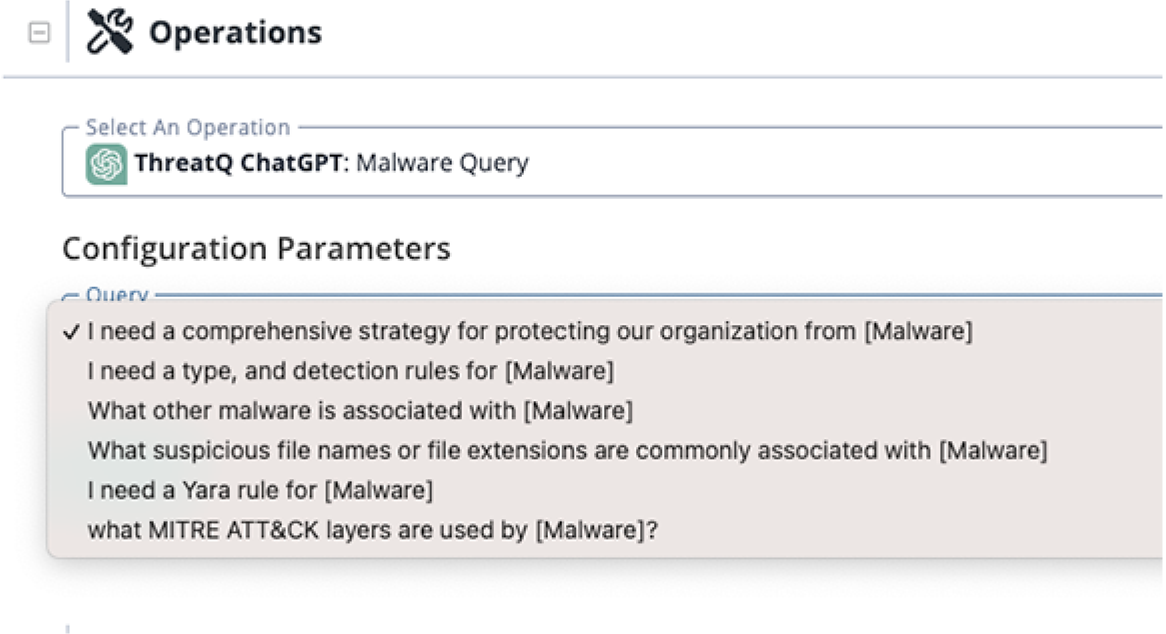
ThreatQuotient provides the following default mapping for all actions:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| choices[].message.content | Attribute | ChatGPT Response | N/A | To protect your organization from PowerNasa, a comprehensive ... | N/A |

## Malware Query Run Parameters

The Malware Query action provides the following parameter:

| PARAMETER | DESCRIPTION |
|---|---|
| **Query** | The following options are available:<br>• I need comprehensive strategy for protecting organization from <object><br>• I need a type, and detection rules for <object><br>• What other malware is associated with <object><br>• What suspicious file names or file extensions are commonly associated with <object><br>• I need a Yara rule for <object><br>• What MITRE ATT&CK layers are used by <object> |



Select An Operation
**ThreatQ ChatGPT**: Malware Query

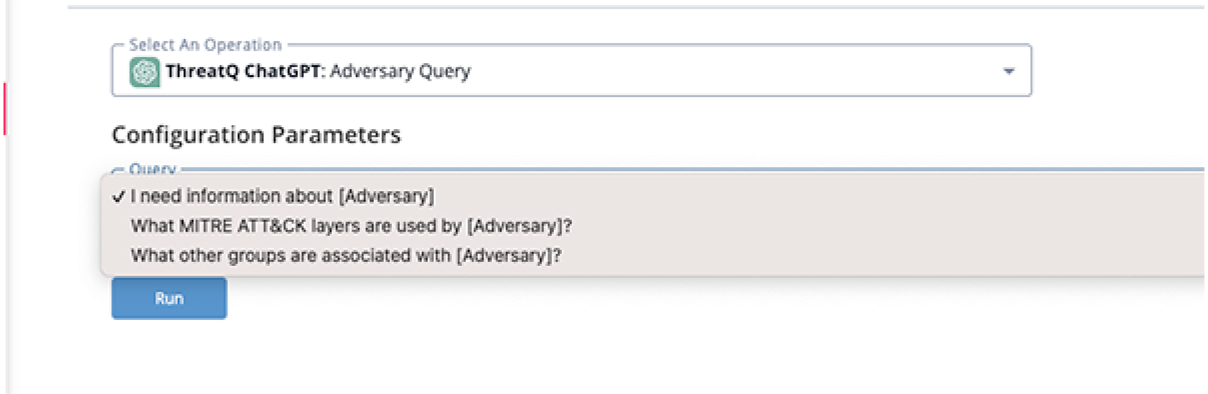
Configuration Parameters

Query
✓ I need a comprehensive strategy for protecting our organization from [Malware]
I need a type, and detection rules for [Malware]
What other malware is associated with [Malware]
What suspicious file names or file extensions are commonly associated with [Malware]
I need a Yara rule for [Malware]
what MITRE ATT&CK layers are used by [Malware]?

## Adversary Query Run Parameters

The Adversary Query action provides the following parameter:

| PARAMETER | DESCRIPTION |
|---|---|
| **Query** | The following options are available:<br>• I need more information about <object><br>• What MITRE ATT&CK layers are used by <object><br>• What other groups are associated with <object> |



Select An Operation
ThreatQ ChatGPT: Adversary Query

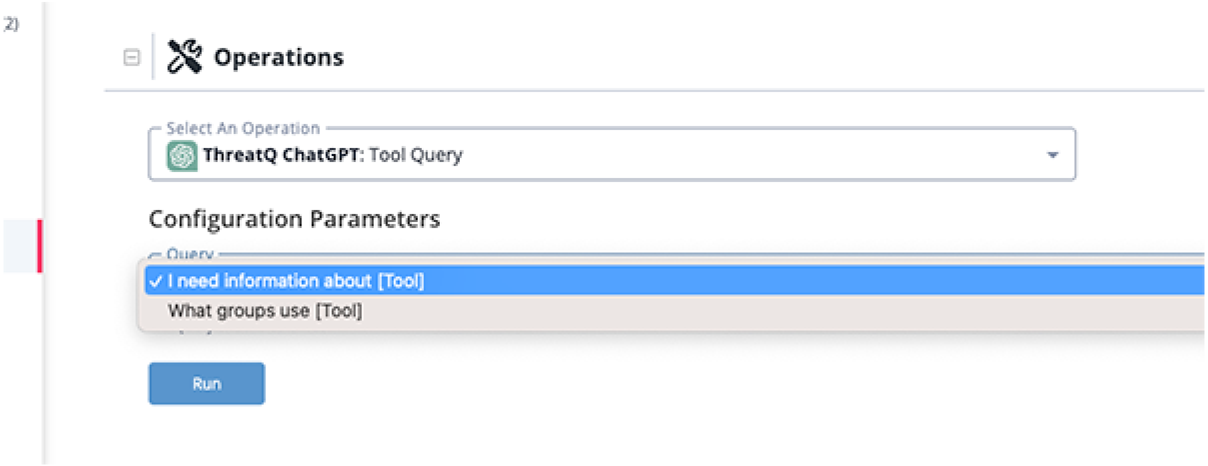
Configuration Parameters

Query
✓ I need information about [Adversary]
What MITRE ATT&CK layers are used by [Adversary]?
What other groups are associated with [Adversary]?

## Tool Query Run Parameters

The Tool Query action provides the following parameter:

| PARAMETER | DESCRIPTION |
|---|---|
| **Query** | The following options are available:<br>• I need information about <object><br>• What groups use <object> |



# Known Issues / Limitations

- The operation is only compatible with ChatGPT 3.5 as of this publication. Future versions of this integration will include additional functionality.
- The information returned from ChatGPT can be added as an attribute.  Future releases of the ThreatQ platform will provide the ability to store this information as a description.

# Change Log

- **Version 1.0.0**
  - Initial release