ThreatQuotient

A Securonix Company

Contextal Lens Operation

Version 1.0.0

July 14, 2026

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	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The Contextal Lens Operation enables ThreatQ users to submit file attachments to Contextal Lens for automated analysis and retrieve detailed enrichment results directly within ThreatQ. The operation supports both new file submissions and retrieval of existing analyses, allowing analysts to review Contextal work graphs, triggered actions, and other enrichment data that can be applied to ThreatQ file objects.

The integration provides the following operation actions:

- **Submit File** – Submits a ThreatQ file attachment to **Contextal Lens** for analysis and returns the resulting enrichment data for review and ingestion into ThreatQ.
- **Get Analysis** – Retrieves the results of a previously submitted Contextal Lens analysis using an existing **Contextal Lens Work ID** file attribute. If multiple Work IDs are available, the action prompts you to select the analysis to retrieve.

The integration is compatible with File (attachment) type system objects.

Prerequisites

The following is require to run the operation:

- A Contextal Platform API URL.
- A Contextal API key if required by the deployed Contextal Platform API.
- The Clens UI frontend URL for analysis links.

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
Platform URL	The base URL of your Contextal Platform deployment (the gateway that serves the API). The operation appends `/api/v1`.
Frontend URL	The base URL for the Clens UI. The operation appends `/{work_id}`.
API Key	Optional - enter the token sent as `Authorization: Bearer <token>`. Leave blank if the API endpoint does not require it.

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
Submit File	Submits an attachment to Contextal Lens and retrieves graph/actions.	File	N/A
Get Analysis	Retrieves graph/actions from an existing `Contextal Lens Work ID` file attribute.	File	N/A

Submit File

The Submit File action downloads the active ThreatQ attachment, submits it to Contextal Lens, receives a work_id, and then retrieves the Contextal work graph and triggered actions for that work request. It renders the Results and Signals Triggered tables.

`POST {Platform URL}/api/v1/submit`

The operation then calls:

- `GET {Platform URL}/api/v1/get_work_graph/{work_id}`
- `GET {Platform URL}/api/v1/actions/{work_id}`

Sample Response:


```
{
  "submit": {
    "work_id": "akieeCWNAEU",
    "object_id":
"b56c2c22898e22531a6f9bcc2afda47e0d4e54a48f54a963094f8cdeec071319"
  },
  "work_graph": {
    "object_type": "PDF",
    "size": 139352,
    "hashes": {
      "md5": "0f24399d723a4eb008133797b18b86e6",
      "sha1": "fac1121caacc67f1547aaae62dfe7a8e40b3bcf6",
      "sha256":
"b56c2c22898e22531a6f9bcc2afda47e0d4e54a48f54a963094f8cdeec071319"
    }
  },
  "work_actions": [
    {
      "actions": [
        {
          "action": "MALICIOUS",
          "scenario": "Unsafe Attachments in PDF [MITRE
ATT&CK:T1566.001]"
        }
      ]
    }
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.work_id	Attachment.Attribute	Contextal Lens Work ID	N/A	akieeCWNAEU	N/A
.object_id	Attachment.Attribute	Contextal Lens Object ID	N/A	b56c2c...71319	N/A
.work_id	Attachment.Attribute	Clens.io Analysis Link	N/A	https://clens.io/akieeCWNAEU	Composed as {Frontend URL}/{work_id}.
.object_type	Attachment.Attribute	Object Type	N/A	PDF	N/A
.size	Attachment.Attribute	Input Size / Processed Size	N/A	136.1 KB / 1.4 MB	N/A
.object_id	Attachment.Attribute	Number of Objects	N/A	8	N/A
.ctime	Attachment.Attribute	Submitted to System	N/A	June 24, 2026, 11:49 AM	Formatted local timestamp from the work graph.
[].actions[]	Attachment.Attribute	Signal	N/A	MALICIOUS: Unsafe Attachments in PDF [MITRE ATT&CK:T1566.001]	N/A

Run Configuration Options

The following configuration option is set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration options are available for this operation action:

OPTION	DESCRIPTION
Max Actions	Enter the maximum number of action result sets to retrieve from Contextal Lens. The default value is `50`.
Result Attempts	Enter the number of attempts to retrieve graph/actions after submission. The default value is 3.

OPTION	DESCRIPTION
Result Interval	Enter the seconds to wait between result retrieval attempts. The default value is 5.

Get Analysis

The Get Analysis action reads the existing Contextal Lens Work ID attribute from the active ThreatQ attachment and retrieves the Contextal work graph and triggered actions for that work request. It does not submit the file again.

`GET {Platform URL}/api/v1/get_work_graph/{work_id}`

The operation also calls:

- `GET {Platform URL}/api/v1/actions/{work_id}`

The **Get Analysis** action returns the same enrichment data and applies the same ThreatQ mappings as **Submit File**, but retrieves the results using an existing **Contextal Lens Work ID** file attribute rather than creating a new submission. Refer to the **Submit File** mapping for details on the returned data and ThreatQ object mappings.

If multiple **Contextal Lens Work ID** attributes are present on the file, the action displays an **Available Analyses** table listing the available Work IDs and their corresponding **Clens.io** links. Rerun the action and specify the desired Work ID in the **Analysis Work ID** parameter to retrieve the associated analysis.

Run Configuration Options

The following configuration option is set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration options are available for this operation action:

OPTION	DESCRIPTION
Analysis Work ID	Optional - enter the Work ID to retrieve when the file has multiple Contextal Lens analyses.
Max Actions	Enter the maximum number of action result sets to retrieve from Contextal Lens. The default value is `50`.
Result Attempts	Enter the number of attempts to retrieve graph/actions. The default value is `3`.

OPTION	DESCRIPTION
Result Interval	Enter the seconds to wait between result retrieval attempts. The default value is 5.

Known Issues / Limitations

- The Get Analysis action requires a `Contextal Lens Work ID` attribute on the active attachment.
- If multiple **Contextal Lens Work ID** attributes are associated with a file, the **Get Analysis** action requires you to specify the desired **Analysis Work ID** before the analysis can be retrieved.

Change Log

- **Version 1.0.0**
  - Initial release