ThreatQuotient

A Securonix Company

Fortra Phishlabs CDF

Version 1.1.0

June 23, 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.

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: 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	1.1.0
Compatible with ThreatQ Versions	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The Fortra Phishlabs integration enables ThreatQ users to ingest Email Incident Response (EIR) and Digital Risk Protection (DRP) incidents, along with associated indicators and impacted identities, directly into the ThreatQ platform. By incorporating PhishLabs intelligence into ThreatQ, security teams gain enhanced visibility into phishing, business email compromise (BEC), brand impersonation, and other external threats, improving threat analysis, investigation, and response capabilities.

The integration provides the following feeds:

- **Phishlabs** - ingests incidents (EIR & Other Services) and associated indicators from PhishLabs into ThreatQ.
- **Phishlabs DRP Incidents** - ingests Digital Risk Protection (DRP) incidents and impacted employee identities from PhishLabs into ThreatQ.

The integration ingests the following system objects:

- Events
- Files
- Identities
- Incidents
- Indicators

Prerequisites

The following is required to run the integration:

- A PhishLabs license with appropriate permissions to access EIR and DRP APIs.
- Your PhishLabs Email Address and API Key (PhishLabs feed)
- Your PhishLabs Client ID and Secret (DRP Incidents feed).

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
6. Select the individual feeds to install, when prompted, and click **Install**.

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

The feed(s) will be added to the integrations page. You will still need to configure and then enable the feed(s).

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 **Commercial** option from the *Category* dropdown (optional).

   If you are installing the integration for the first time, it will be located under the **Disabled** tab.
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

Phishlabs Parameters

PARAMETER	DESCRIPTION
Email Address	Enter your Phishlabs account email address.
API Key	Enter your Phishlabs account API key.
Service	Enter the service name to use to filter incidents. The default setting is `EIR`.

Phishlabs DRP Incidents Parameters

PARAMETER	DESCRIPTION
Client ID	Enter your Phishlabs Client ID.
Client Secret	Enter your Phishlabs Client Secret

PARAMETER	DESCRIPTION
Brand Names	Optional - enter a line-separated list of brand names to filter the incidents.
Severity Levels	Select the severity levels to ingest. Options include: ◦ Low *(Default)* ◦ Medium *(Default)* ◦ High *(Default)*
Statuses	Select the incident statuses to ingest. Options include: ◦ New *(Default)* ◦ Closed *(Default)* ◦ Requires Input *(Default)* ◦ Mitigation *(Default)* ◦ Monitoring *(Default)* ◦ Closed, No Action *(Default)* ◦ Pending *(Default)* ◦ Requires Approval *(Default)* ◦ Input Provided *(Default)* ◦ Persistent Threat *(Default)* ◦ Duplicate *(Default)*
Incident Types	Select the incident types to ingest. Options include: ◦ Dark Web *(Default)* ◦ Social Media *(Default)*
Dark Web Threat Type	Select the threat types to ingest for Dark Web incidents. Options include: ◦ Account Credentials For Sale *(Default)* ◦ Consumer Goods For Sale *(Default)*

PARAMETER	DESCRIPTION
	◦ Credit/Debit Card Data *(Default)* ◦ Cyber Risk *(Default)* ◦ Deposit Fraud *(Default)* ◦ Executive Mention In Post *(Default)* ◦ Fraud Tools *(Default)* ◦ Personal Identifiable Information *(Default)* ◦ Physical Threat To Executive *(Default)* ◦ Source Code *(Default)* ◦ Third Party Corporate Email Leaks *(Default)* ◦ Stealer Malware Credentials *(Default)* ◦ Botnet Credentials *(Default)* ◦ Remote Access Trojan Credentials *(Default)*
Social Media Threat Types	Select the threat types to ingest for Social Media incidents. Options include: ◦ BIN/IIN Details *(Default)* ◦ Brand Mention On Page *(Default)* ◦ Cyber Risk *(Default)* ◦ Deposit Fraud *(Default)* ◦ Executive Mention On Page *(Default)* ◦ Generic Physical Threat *(Default)* ◦ Impersonation Of Employee *(Default)* ◦ Impersonation Of Executive *(Default)* ◦ Impersonation Of Brand *(Default)* ◦ Leaked Credentials *(Default)* ◦ Leaked Documents *(Default)* ◦ Legal Threat *(Default)* ◦ Negative Comment Toward Employee *(Default)* ◦ Negative Comment Toward Organization *(Default)*

PARAMETER	DESCRIPTION
	◦ News PR Stock Commentary *(Default)* ◦ Personal Identifiable Information *(Default)* ◦ Phishing *(Default)* ◦ Physical Threat To Employee *(Default)* ◦ Physical Threat To Event *(Default)* ◦ Physical Threat To Executive *(Default)* ◦ Physical Threat To Location *(Default)* ◦ Protest Petition Boycotts *(Default)* ◦ Source Code *(Default)* ◦ Event *(Default)* ◦ Cryptocurrency Scam *(Default)* ◦ Counterfeit *(Default)*
Ingest Images as Related Files	Enable this option to ingest image files collected by PhishLabs as related File objects within ThreatQ. The ingested files will be associated with the corresponding Event object, providing additional context and supporting evidence for analysis and investigation.
Ingest Files as	Select how files containing compromised/leaked credentials should be ingested. Options include: ◦ Related File Objects *(Default)* ◦ Part of the Event Description (CSV & TXT Only)

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.

ThreatQ Mapping

Phishlabs

The Phishlabs feed ingests incidents (EIR and Other Services) and associated indicators from PhishLabs into ThreatQ.

```
GET https://caseapi.phishlabs.com/idapi/v1/incidents/{{ service }}
```

Sample Response:


```
{
    "metadata": {
        "count": 1
    },
    "incidents": [
        {
            "id": "INC0763488",
            "service": "EIR",
            "title": "Fwd: CONFIRMATION OF YOUR OVERDUE PAYMENT BY
ATTACHE FILE",
            "description": "Incident description",
            "status": "Closed",
            "details": {
                "caseType": "Payload",
                "classification": "Do Not Engage",
                "subClassification": "Do Not Engage",
                "severity": null,
                "emailReportedBy": "Billy Smith
<bsmith@phishlabs.com>",
                "submissionMethod": "Forwarded",
                "sender": "Billy Smith <bsmith@phishlabs.com>",
                "emailBody": "\"\\r\\n\\r\\nBilly Smith\\r\
\n843-283-7421\\r\\n\\r\\nBegin forwarded message:\\r\\n\\r\\nFrom:
UN ECOSOC / 2019 <china@medicalcables.eu>\\r\\nDate: November 17,
2019 at 5:22:31 PM EST\\r\\nSubject: CONFIRMATION OF YOUR OVERDUE
PAYMENT BY ATTACHE FILE\\r\\nReply-To: <services@etscc.com>\\r\\n\\r\
\n [External]\\r\\nDear Sir/Madam, Please confirm the attache message
file for more information regard of your payment. Best Regards, World
Bank Group Finance Ministry\\r\\n\\r\\nExternal email\\r\\n\\r\
\nForward suspicious emails to bad@phishlabs.com\\r\\n\"",
                "urls": [
```

```
                    {
                        "url": "http://purl.org/dc/elements/1.1/",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url": "https://www.un.org/press/en/2005/
ik486.doc.htm",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url": "http://www.un.org/",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url": "http://ns.adobe.com/xap/1.0/mm/",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url": "http://ns.adobe.com/pdf/1.3/",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url": "http://www.w3.org/1999/02/22-rdf-
syntax-ns#",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url": "http://ns.adobe.com/xap/1.0/",
                        "malicious": false,
                        "maliciousDomain": false
                    }
                ],
                "attachments": [
                    {
                        "fileName": "ATT00001.htm",
                        "mimeType": "text/html",
```

```
                        "md5": "07cbbf25d210d17c6df7ce17695a8f5f",
                        "sha256":
"e19f4d5b6a2341e3ba9437f152f4f6739fd8a0842fbc36d531ffa7ec938a289f",
                        "malicious": false
                    }
                ],
                "furtherReviewReason": null,
                "offlineUponReview": false
            },
            "created": "2019-11-17T22:23:16Z",
            "modified": "2019-11-17T22:37:27Z",
            "closed": "2019-11-17T22:37:27Z",
            "duration": 852
        }
    ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.incidents[].title, .incidents[].id	Incident.value	N/A	.incidents[].created	Fwd: CONFIRMATION OF YOUR OVERDUE PAYMENT BY ATTACHE FILE - INC0763488	An incident's value is in the format {{title}} - {{id}} if .incidents[].title has a value; otherwise, only .incidents[].id is used.
.incidents[].description	Incident.description	N/A	.incidents[].created	Incident description	
.incidents[].id	Incident.attribute	ID	.incidents[].created	INC0763488	
.incidents[].details.caseType	Incident.attribute	Case Type	.incidents[].created	Payload	
.incidents[].details.classification	Incident.attribute	Classification	.incidents[].created	Do Not Engage	
.incidents[].details.subClassification	Incident.attribute	Subclassification	.incidents[].created	Do Not Engage	
.incidents[].details.severity	Incident.attribute	Severity	.incidents[].created	Low	
.incidents[].details.emailReportedBy	Incident.attribute	Email Reported By	.incidents[].created	Billy Smith <bsmith@phishlabs.com>	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.incidents[].details.emailBody	Incident.attribute	Email Body	.incidents[].created	\"\\r\\n\\r\\nBilly Smith\\r\\n843-283-7421\\r\\n\\r\\nBegin forwarded...	
.incidents[].details.submissionMethod	Incident.attribute	Submission Method	.incidents[].created	Forwarded	
.incidents[].details.sender	Incident.attribute	Sender	.incidents[].created	Billy Smith <bsmith@phishlabs.com>	
.incidents[].details.furtherReviewReason	Incident.attribute	Further Review Reason	.incidents[].created	reason example	
.incidents[].details.offlineUponReview	Incident.attribute	Offline Upon Review	.incidents[].created	false	
.incidents[].status	Incident.attribute	Status	.incidents[].created	Closed	
.incidents[].modified	Incident.attribute	Modified At	.incidents[].created	2019-11-17T22:23:16Z	
.incidents[].closed	Incident.attribute	Closed At	.incidents[].created	2019-11-17T22:23:16Z	
.incidents[].duration	Incident.attribute	Duration	.incidents[].created	852	
.incidents[].service	Incident.attribute	Service	.incidents[].created	EIR	
.incidents[].details.urls	Indicator.value	URL	.incidents[].created		see URL Indicators mappings
.incidents[].details.attachments	Indicator.value	Filename / MD5 / SHA-256	.incidents[].created		see Attachments Indicators mappings
.incidents[].details.sender	Indicator.value	Email Address	.incidents[].created	bsmith@phishlabs.com	This indicator is parsed by extracting the email from incidents.details.sender

URL Indicator Mapping

Sample Response:


```
[
  {
    "url": "http://purl.org/dc/elements/1.1/",
    "malicious": false,
    "maliciousDomain": false
},
{
    "url": "https://www.un.org/press/en/2005/ik486.doc.htm",
    "malicious": false,
    "maliciousDomain": false
},
{
    "url": "http://www.un.org/",
    "malicious": false,
    "maliciousDomain": false
}
]
```


ThreatQuotient provides the following default mapping:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
url	indicator.value	URL	"http://purl.org/dc/elements/1.1/"
malicious	indicator.attribute	Malicious URL	false
maliciousDomain	indicator.attribute	Malicious Domain	true

Attachment Indicators Mapping

Sample Response:

```
[
  {
    "fileName": "ATT00001.htm",
    "mimeType": "text/html",
    "md5": "07cbbf25d210d17c6df7ce17695a8f5f",
    "sha256":
"e19f4d5b6a2341e3ba9437f152f4f6739fd8a0842fbc36d531ffa7ec938a289f",
    "malicious": false
}
]
```

ThreatQuotient provides the following default mapping:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
fileName	indicator.value	Filename	"ATT00001.htm"	Indicator of type "Filename"
md5	indicator.value	MD5	"07cbbf25d210d17c6 df7ce 17695a8f5f"	Indicator of type "MD5"
sha256	indicator.value	SHA-256	"e19f4d5b6a2341e3b a94 37f152f4f6739fd8a0 842fb c36d531ffa7ec938a2 89f"	Indicator of type "SHA-256"
malicious	indicator.attri bute	Malicious Domain	true	
mimeType	indicator.attri bute	Mime Type	"text/html"	

An indicator of type Filename, MD5 and SHA-256 will be created from the values of the fields "fileName", "sha256" and "md5". Each of these indicators will have the attributes from the fields "malicious" and "mimeType".

Phishlabs DRP Incidents

The PhishLabs DRP Incidents feed ingests Digital Risk Protection (DRP) incidents from the PhishLabs platform into ThreatQ. The feed provides visibility into external threats, including compromised credentials, brand impersonation and abuse, social media threats, and dark web intelligence, enabling organizations to identify, investigate, and respond to digital risks more effectively.

```
POST https://threatintel.phishlabs.com/api/external/incident/search
```

Sample Response:


```
{
    "totalCount": 1921,
    "pagesCount": 20,
    "pageSize": 100,
    "pageNumber": 1,
    "items": [
        {
            "id": 1072798,
            "title": "Credentials Compromised by Stealer Malware",
            "created": "2025-03-13T00:05:29.1812475Z",
            "createdBy": "PhishLabs Operations",
            "incidentType": "Dark Web Monitoring",
            "brandName": "Acme Corp",
            "threatType": "Stealer Malware Credentials",
            "lastModified": "2025-03-13T00:05:29.2644753Z",
            "status": "Closed, No Action",
            "statusReason": "Informational Only",
            "severity": "High",
            "executiveName": null,
            "summary": "Credentials have been identified that were
compromised through the deployment of stealer malware. Compromised
credentials can include both potential employee or customer logins
and other associated personal identifiable information tied to those
accounts. The details of the compromised credentials have been
captured in this incident for review.",
            "mitigationStarted": null,
            "closed": "2025-03-13T00:05:29.1735405Z",
            "observables": [
                {
                    "type": "Post",
                    "id": 6324794,
```

```
                    "url": "https://www.acme.org",
                    "data": null
                }
            ],
            "changeLogs": [
                {
                    "timeStamp": "2025-03-13T00:05:29.2644753Z",
                    "createdBy": "PhishLabs Operations",
                    "content": "Documents - 144374 - added to
incident"
                },
                {
                    "timeStamp": "2025-03-13T00:05:29.1812475Z",
                    "createdBy": "PhishLabs Operations",
                    "content": "Incident created"
                },
                {
                    "timeStamp": "2025-03-13T00:05:29.1812475Z",
                    "createdBy": "PhishLabs Operations",
                    "content": "Posts - 6324794 - added to incident"
                }
            ]
        }
    ]
}
```


A supplemental API call is made for each incident to fetch the full details of the incident:

`GET https://threatintel.phishlabs.com/api/external/incident/{{ id }}/details`

When enabled, for each image/document file associated with an incident, an additional API call is made to fetch the file content:

`GET https://threatintel.phishlabs.com/api/external/file/{{ type }}/{{ id }}`

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title, .id`	`Event.title`	`Incident`	`.created`	`Leaked Credentials Found | ID: 123456`	`N/A`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.summary, .observables, .changeLogs	Event.description	N/A	N/A	N/A	Other fields are included to build a rich text HTML description
.incidentType	Event.attribute	Incident Type	.created	Dark Web Monitoring	
.threatType	Event.attribute	Threat Type	.created	Credit/Debit Card Data	
.brandName	Event.attribute	Affected Brand	.created	Acme Corp	
.status	Event.attribute	Status	.created	Closed, No Action	N/A
.statusReason	Event.attribute	Status Reason	.created	Informational Only	
.severity	Event.attribute	Severity	.created	High	
.executiveName	Identity.value	Identity	.created	Jane Doe	Only created when the incident has an associated executive
.executiveName	Identity.attribute	Employee Type	.created	Executive	Only added when the incident has an associated executive
.documentFiles[]	Event.attachment	File (Generic Text)	.timeStamp	123456-doc-credentials.csv	Related to the Event; ingested when "Related File Objects" is selected
.imageFiles[]	Event.attachment	File (Image)	.timeStamp	123456-img-screenshot.png	Related to the Event; ingested when "Ingest Images as Related Files" is enabled

Average Feed Run

Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Phishlabs

METRIC	RESULT
Run Time	1 minute
Indicators	1,017
Indicator Attributes	3,175
Incidents	194
Incidents Attributes	2,687

Phishlabs DRP Incidents

METRIC	RESULT
Run Time	2 minutes
Events	10
Event Attributes	60
Files	8
Identities	10

METRIC	RESULT
Identity Attributes	10

Change Log

- **Version 1.1.0**
  - Added a new feed, **PhishLabs DRP Incidents**, feed to ingest Digital Risk Protection (DRP) incidents and impacted employee identities from PhishLabs into ThreatQ.
  - Enhanced incident parsing to automatically extract and ingest **Email Address** indicators from the **Sender** attribute when a valid email address is present.
  - Updated event title generation to append the incident ID using the format **{Title} - {ID}**, ensuring unique object names within ThreatQ.
  - Updated the integration's name from Phishlabs CDF to Fortra Phishlabs CDF.
  - Updated the minimum ThreatQ version to 5.29.0.
- **Version 1.0.0**
  - Initial release