ThreatConnect™

# ThreatConnect® VirusTotal™ Spaces App

## User Guide

**Software Version 1.0**

**July 20, 2020**

30007-02 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: .703.229.4489
www.ThreatConnect.com

# Table of Contents

# OVERVIEW

The VirusTotal Spaces app is a contextually aware Spaces app in ThreatConnect that provides VirusTotal summary, resolution, scan, and detection information on the **Details** screen of an Address, File, Host, or URL Indicator. For more information on contextually aware Spaces apps, see the *Contextually Aware Spaces* article in the ThreatConnect Knowledge Base.

This guide provides an overview of the VirusTotal Spaces app for ThreatConnect. While it includes descriptions of VirusTotal metrics, it is not a comprehensive source of VirusTotal definitions. Further, these metrics can be changed by VirusTotal at any time. For full details on VirusTotal metric definitions, visit the VirusTotal website at https://www.virustotal.com/.

# DEPENDENCIES

## ThreatConnect Dependencies

- VirusTotal Spaces app (**TCX VirusTotal v1.1**) installed by a System Administrator and added and configured as a contextually aware Spaces app for the object type

## VirusTotal Dependencies

- A VirusTotal Application Programming Interface (API) token is provided via a subscription to VirusTotal. This token is generated within VirusTotal and is required in order to use this app.

# CONFIGURATION PARAMETERS

## Parameter Definition

The parameters defined in Table 1 apply to the job-configuration parameters during the Spaces app configuration process.

**Table 1**

| Name | Description |
|---|---|
| Title | This parameter is the title of the app as it appears on the **Spaces** tab of the object's **Details** screen. |
| Logging level | This parameter, for support issues only, is for debugging. Possible values are as follows:<br>• DEBUG<br>• INFO<br>• WARNING<br>• ERROR<br>• CRITICAL |
| VirusTotal API Token | This parameter is the VirusTotal API token used by the Data Enrichment Analyze feature. |
| Comma-separated list of tags applied to indicator on an add | This parameter is the comma-separated list of Tags to apply to any Indicator added using this app. |
| Confidence applied to indicator on an add (0-100) | This parameter is the Confidence Rating (0–100%) to apply to any Indicator added using this app. |
| Rating applied to indicator on an add (0-5) | This parameter is the Threat Rating (0–5 skulls) to apply to any Indicator added using this app. |

| | |
|---|---|
| Automatically send Security Labels (comma separated values) | When this parameter is defined, Indicators that have the provided Security Labels will be automatically sent to VirusTotal upon navigation to the **Spaces** tab. |

# GETTING STARTED

The user interface initially displays a card with a **SEND TO VIRUSTOTAL** button. The screen may also include Security Label information for the object.

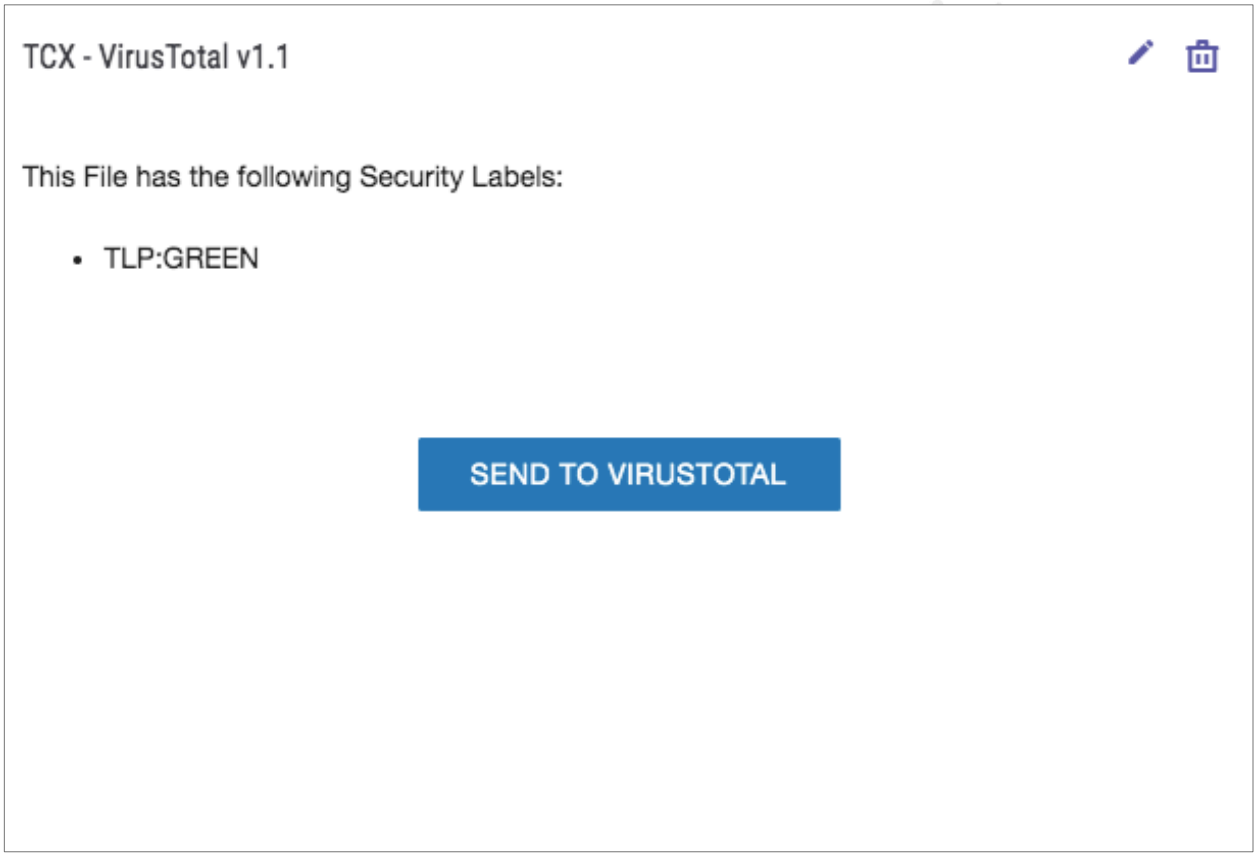


Figure 1 shows an example of the VirusTotal Spaces app card for a File object.

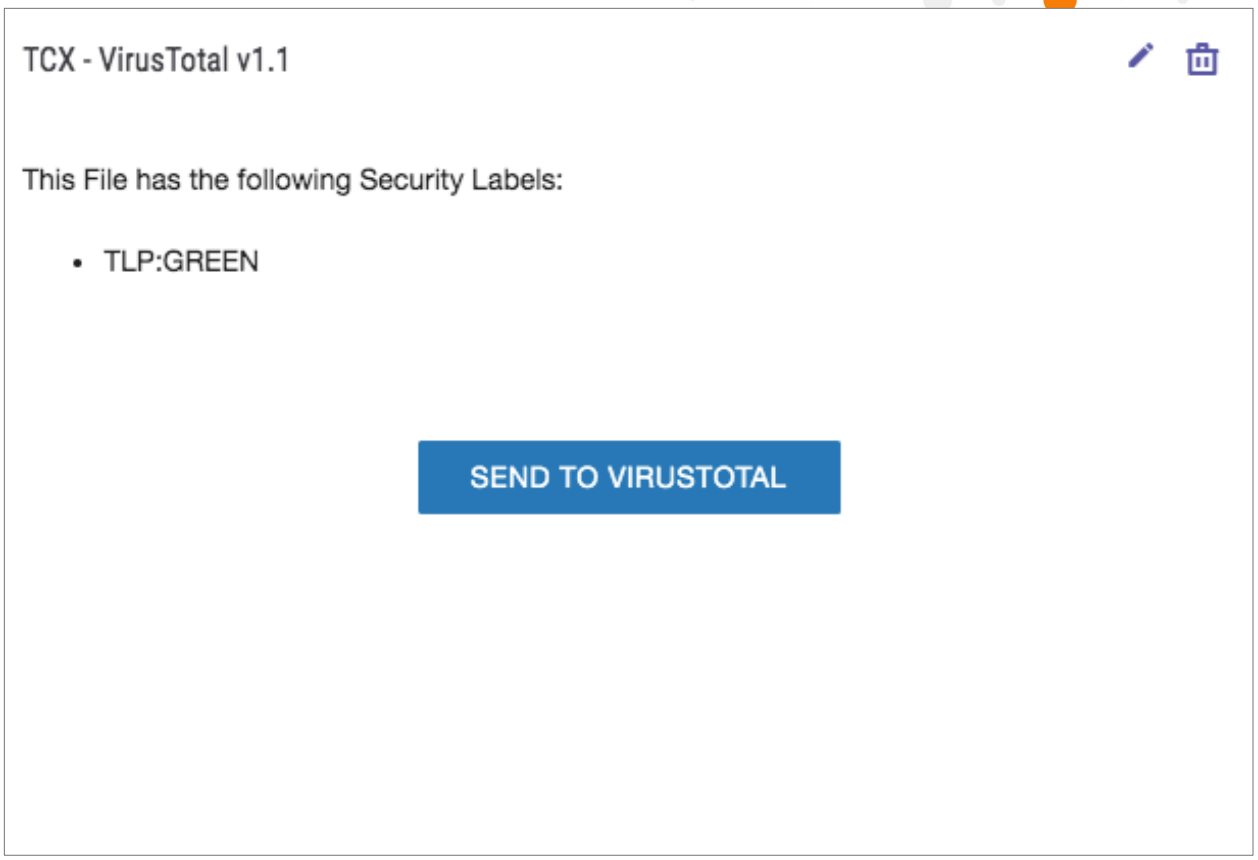


**Figure 1**

When the **SEND TO VIRUSTOTAL** button is clicked, the card will display a **Summary** screen, which provides a quick glance at key metrics, and tabs that, when clicked, provide more detailed information specific to the object type.

# ADDRESS CONTEXT

The Address Context for the VirusTotal Spaces app retrieves contextual data from the VirusTotal API for the selected IP address.

## Summary Screen

Figure 2 displays the **Summary** screen for the Address Context.

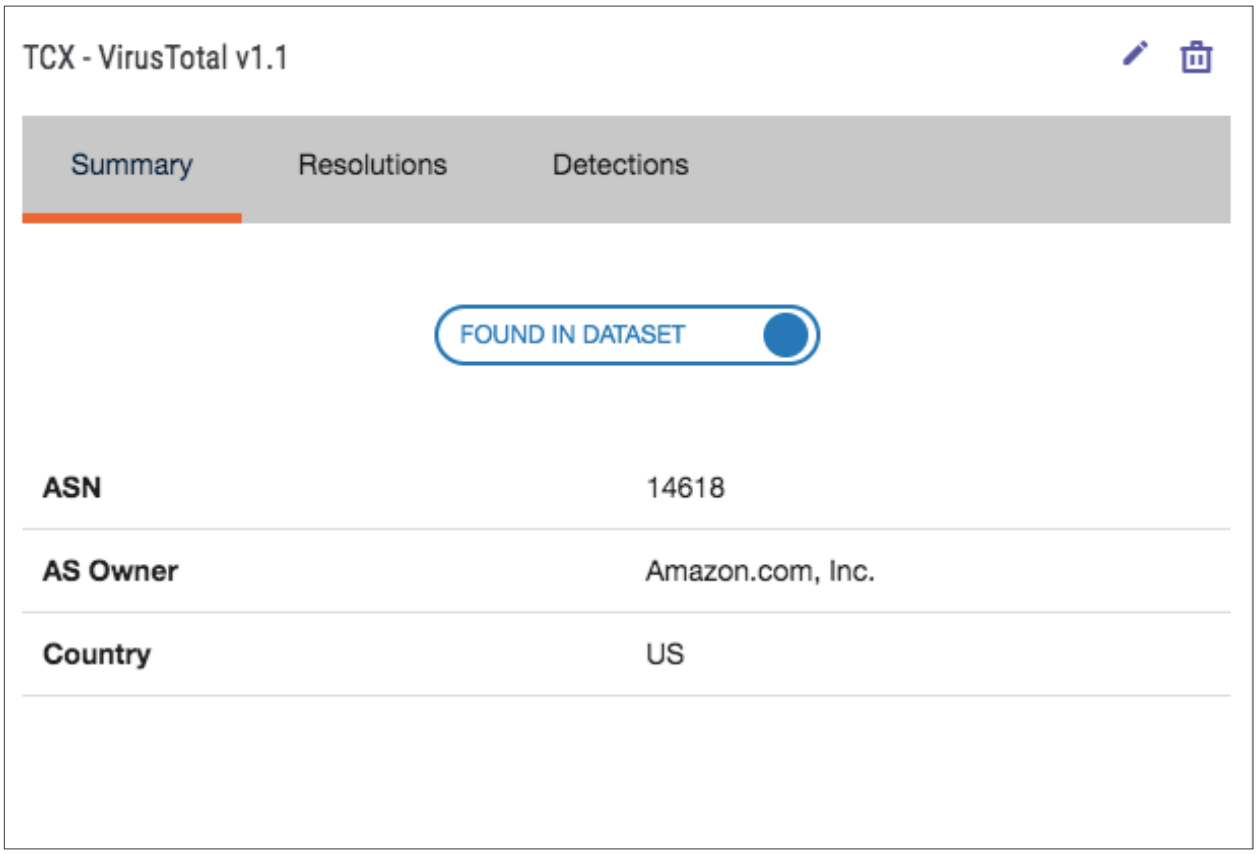


**Figure 2**

The **Summary** screen displays four fields provided by VirusTotal for an IP Address, as summarized in Table 2.

Table 2

| Field | Description |
|---|---|
| Found Switch | This field is the flag designating whether the selected IP address was found in the VirusTotal database. |
| ASN | This field is the Autonomous System Number for the IP address. |
| AS Owner | This field is the Autonomous System Owner of the group of IP networks. |
| Country | This field is the origin country for the AS Owner. |

## Resolutions Screen

The Address Context retrieves host name resolutions for selected IP addresses recorded by the VirusTotal Passive Domain Name System (DNS) infrastructure. Figure 3 displays the **Resolution** screen for an IP Address Context.

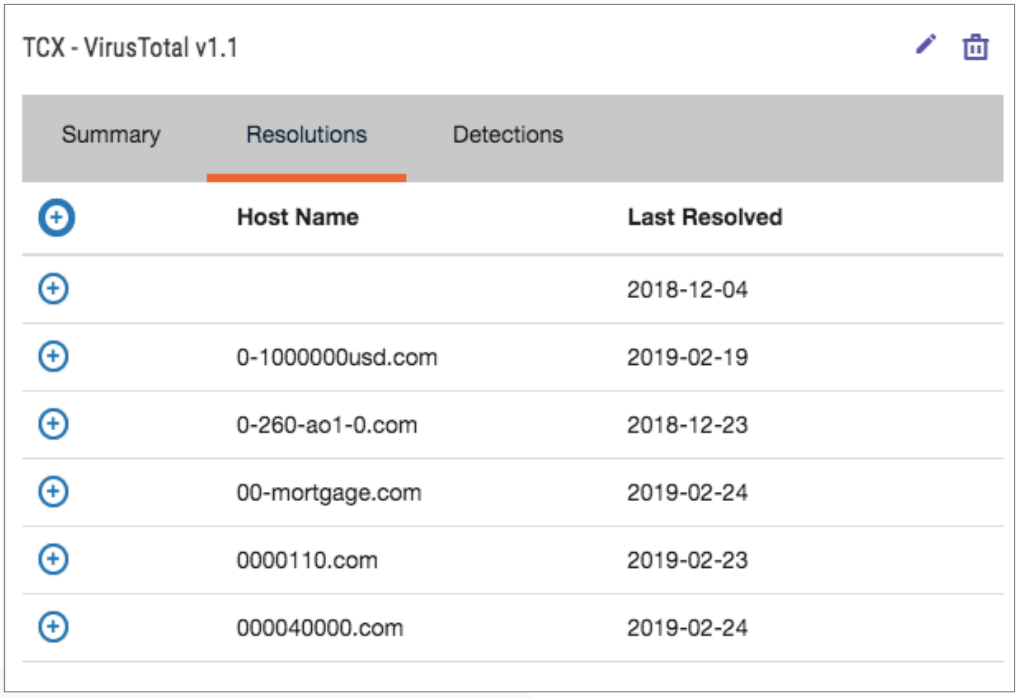


Figure 3

Table 3 displays the two fields from the VirusTotal database for the DNS resolutions.

**Table 3**

| Field | Description |
|---|---|
| Host Name | This field is the domain resolving to the selected IP address. |
| Last Resolved | This field is the date on which the domain was last resolved for the selected IP address. |

***NOTE: Hosts can be directly added to ThreatConnect by clicking on the Plus (+) button. See the "ADDING INDICATORS" section for more details.***

## Detections Screen

The **Detections** screen, under an Address Context, displays the latest URLs detected by at least one URL scanner and hosted at such domain under the selected IP address (Figure 4).

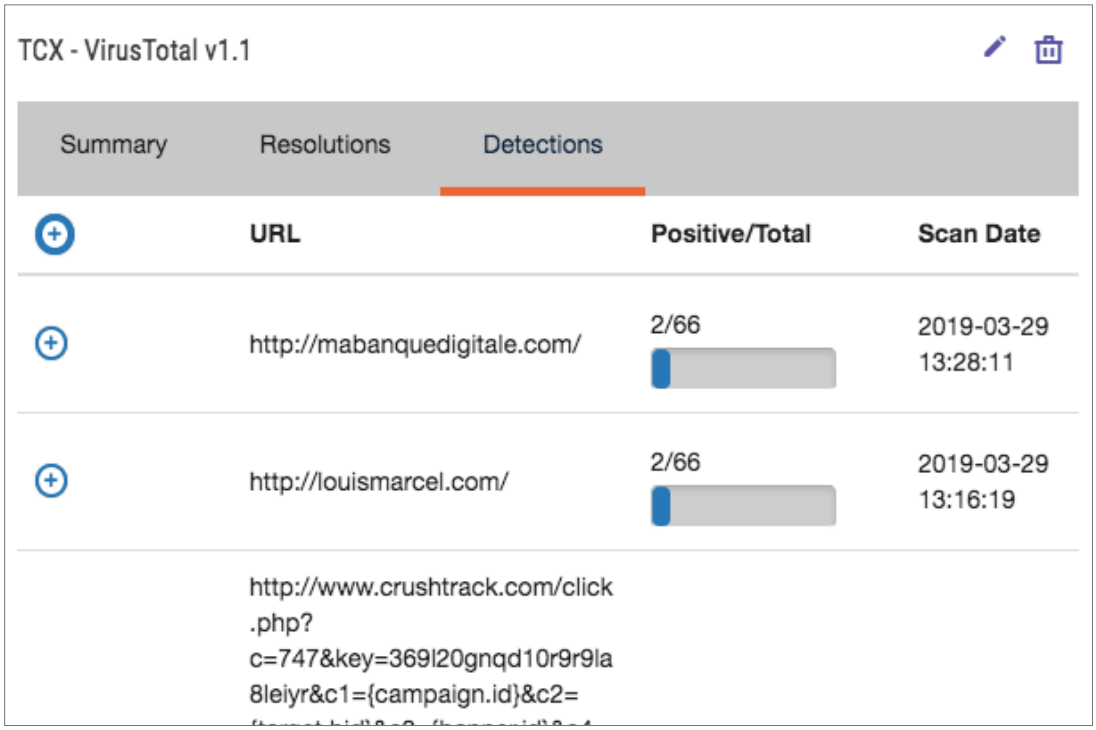


**Figure 4**

***NOTE: Multiple URLs can be detected under the Passive DNS domain resolutions.***

Table 4 displays the fields on the **Detections** screen.

**Table 4**

| Field | Description |
|---|---|
| URL | This field is a URL detected under the resolved domains. |
| Positive/Total | This field is the number of positive scans detecting this URL out of the total number of scanners run by VirusTotal. |
| Scan Date | This field is the date on which the VirusTotal scanners last ran on the detected URL. |

***NOTE: URLs can be directly added to ThreatConnect by clicking on the Plus (+) button. See the "ADDING INDICATORS" section for more details.***

# FILE CONTEXT

The File Context for the VirusTotal Spaces app retrieves contextual data from the VirusTotal API for the selected File.

## Summary Screen

Figure 5 displays the **Summary** screen for the File Context. The **Summary** screen is the only tab provided for this object type.

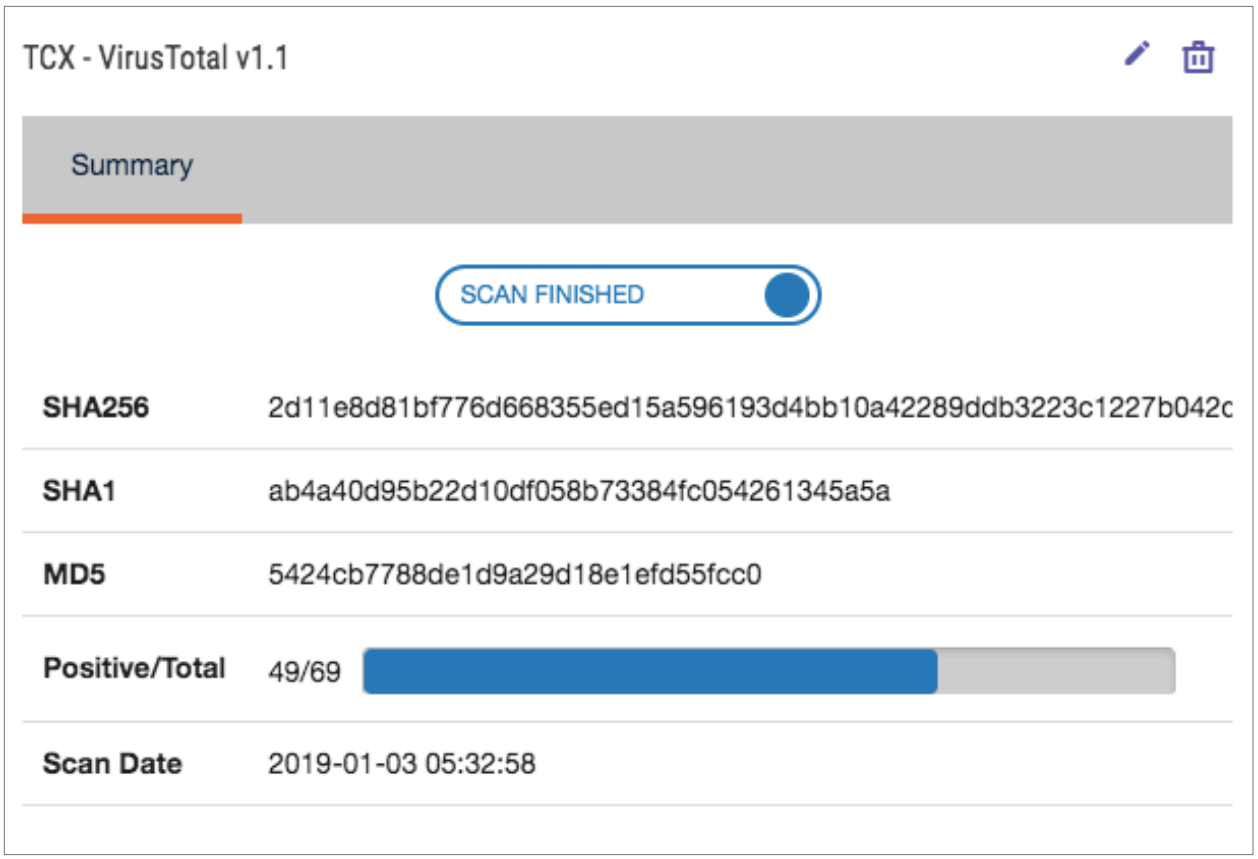


**Figure 5**

The **Summary** screen displays the six fields provided by VirusTotal for a File, as summarized in Table 5.

Table 5

| Field | Description |
| --- | --- |
| Scan Finished Switch | This field is the flag designating whether the scan for the selected File in the VirusTotal database was completed. |
| SHA256 | This field is the SHA256 hash for the File. |
| SHA1 | This field is the SHA1hash for the File. |
| MD5 | This field is the MD5 hash for the File. |
| Positive/Total | This field is the number of positive scans detecting this File out of the total number of scanners run by VirusTotal. |
| Scan Date | This field is the date on which the VirusTotal scanners last ran on the detected File. |

# HOST CONTEXT

The Host Context for the VirusTotal Spaces app retrieves contextual data on the selected domain name from the VirusTotal database.

## Summary Screen

Figure 6 displays the **Summary** screen for the Host Context.

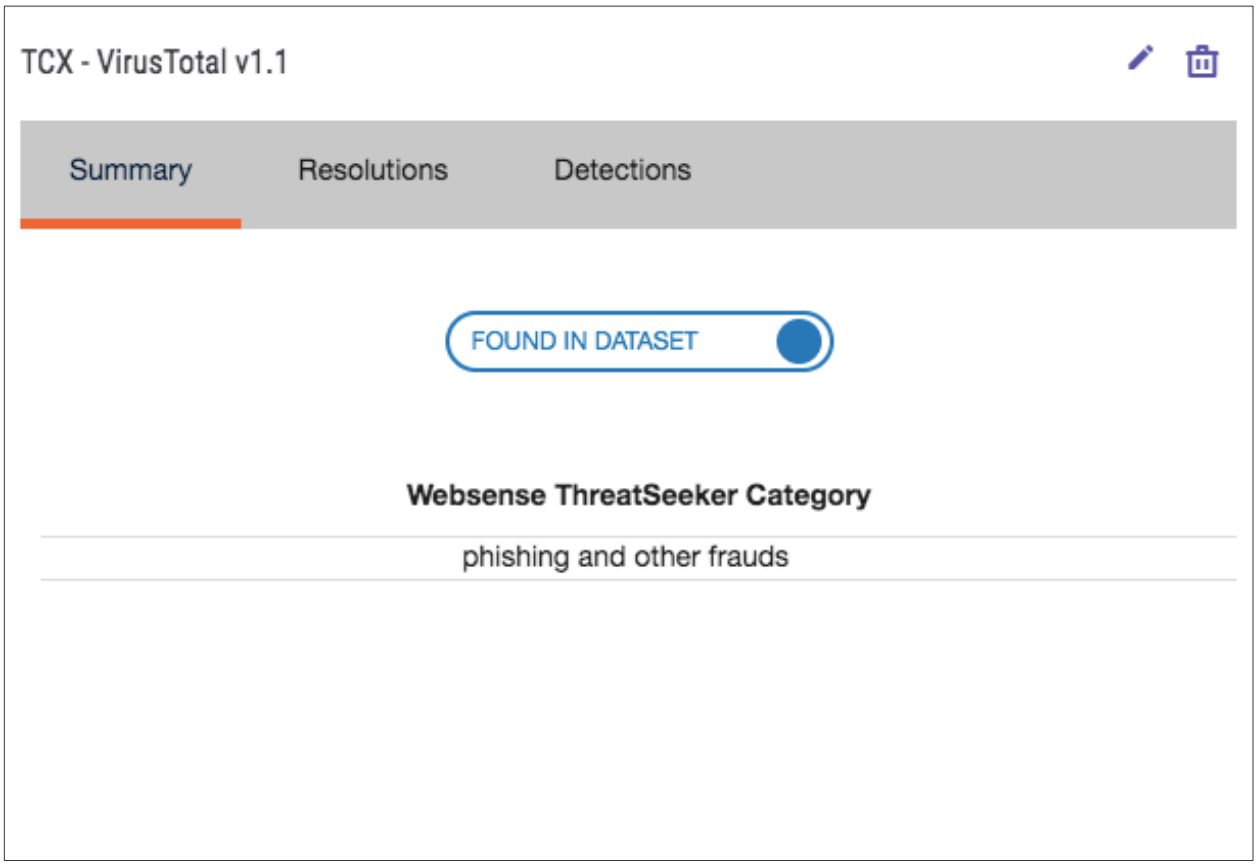


**Figure 6**

The **Summary** screen contains a snapshot of the status for the selected Host, as summarized in Table 6.

**Table 6**

| Field | Description |
|---|---|
| Found Switch | This field is the flag designating whether the selected Host was found in the VirusTotal database. |
| Websense® ThreatSeeker® Category | This field is the domain category according to Websense ThreatSeeker. For more information about ThreatSeeker categories, visit http://www.websense.com/content/home.aspx. |

## Resolutions Screen

The Host Context retrieves IP address resolutions for the selected Host recorded by the VirusTotal Passive DNS infrastructure. Figure 7 displays the **Resolution** screen for a Host Context.

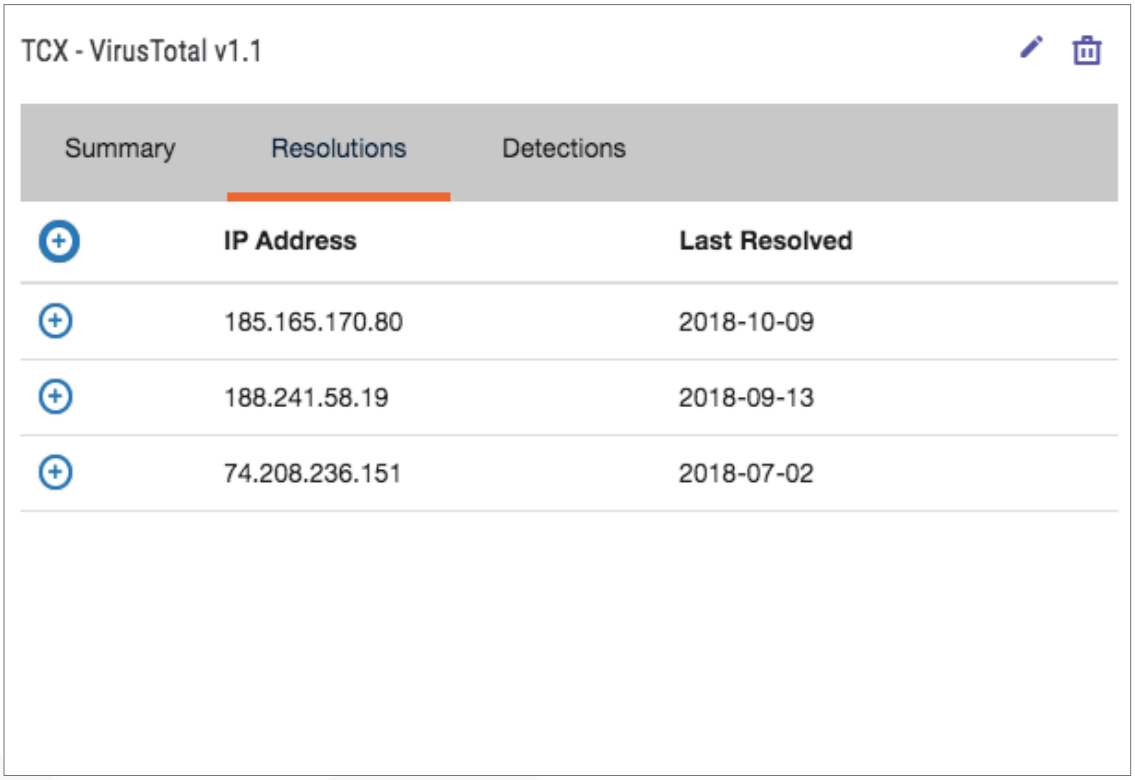


**Figure 7**

Table 7 displays the two relevant fields from the VirusTotal database for the DNS resolutions.

**Table 7**

| Field | Description |
|---|---|
| IP Address | This field is the IP address resolving to the selected Host. |
| Last Resolved | This field is the date on which the IP address was last resolved for the selected Host. |

***NOTE: IP addresses can be directly added to ThreatConnect by clicking on the Plus (+) button. See the "ADDING INDICATORS" section for more details.***

## Detections Screen

The **Detections** screen, under a Host Context, displays the latest URLs detected by at least one URL scanner and hosted at the selected domain (Figure 8).

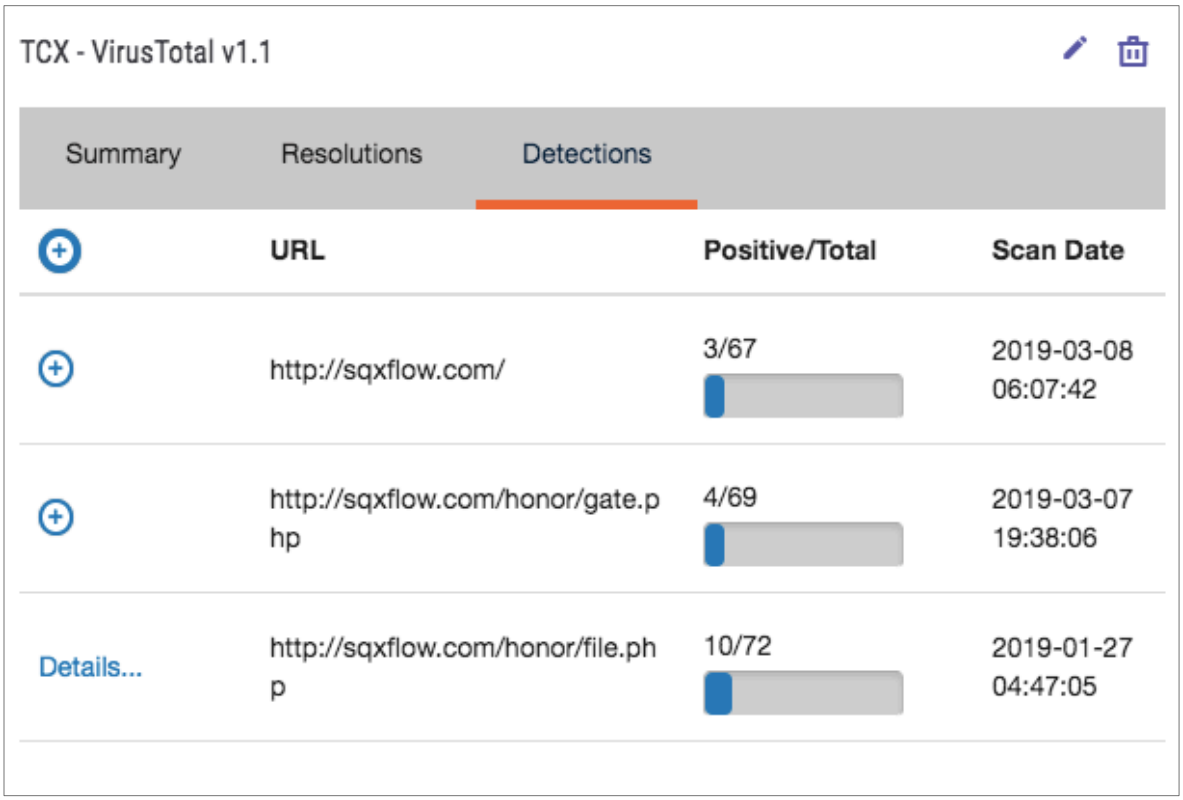


**Figure 8**

***NOTE: Multiple URLs can be detected under the Passive DNS domain resolutions.***

Table 8 displays the three fields on the **Detections** screen.

**Table 8**

| Field | Description |
|---|---|
| URL | This field is a URL detected under the resolved domains. |
| Positive/Total | This field is the number of positive scans detecting this URL out of the total number of scanners run by VirusTotal. |
| Scan Date | This field is the date on which the VirusTotal scanners last ran on the detected URL. |

***NOTE: URLs can be directly added to ThreatConnect by clicking on the Plus (+) button. See the "ADDING INDICATORS" section for more details.***

# URL CONTEXT

The URL Context for the VirusTotal Spaces app retrieves contextual data from the VirusTotal API for the selected URL.

## Summary Screen

Figure 9 displays the **Summary** screen for the URL Context. The **Summary** screen is the only tab provided for this object type.

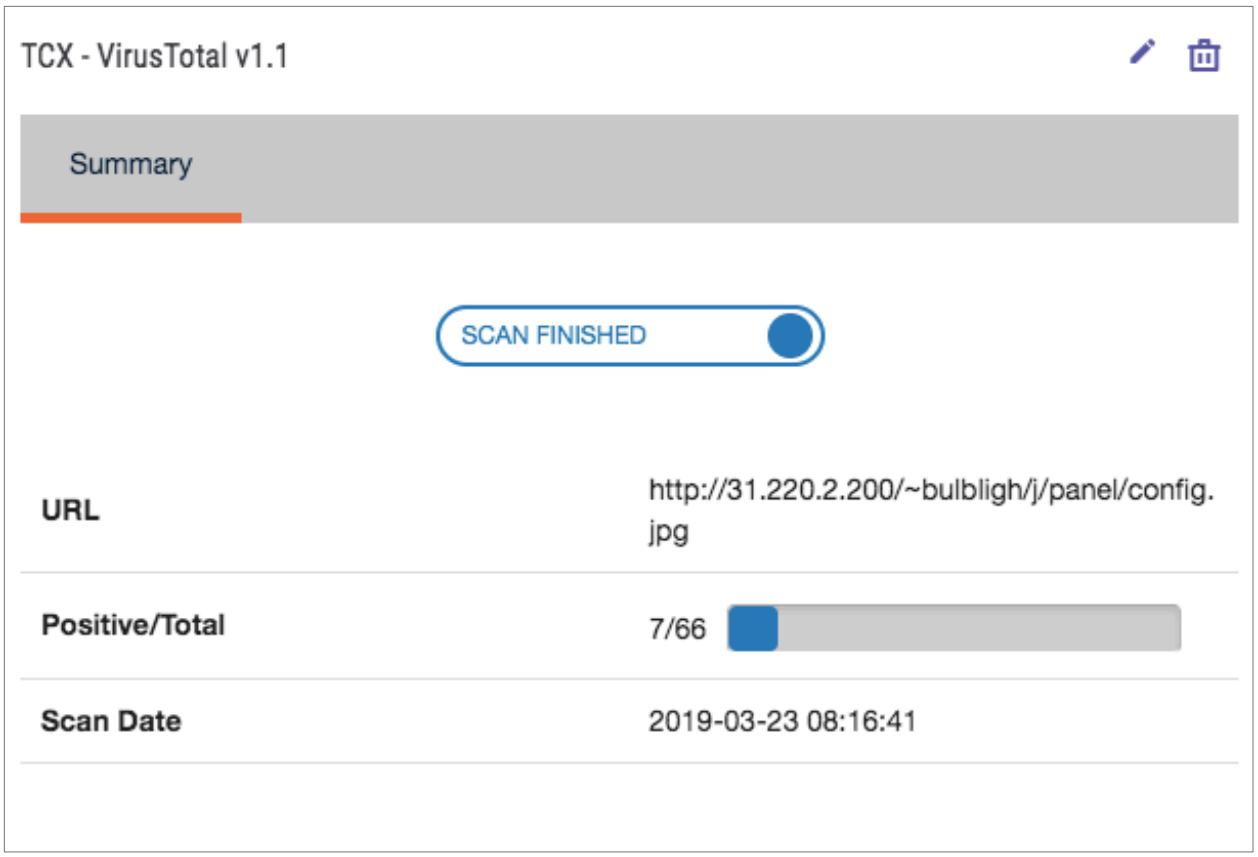


**Figure 9**

The **Summary** screen contains a snapshot of the status for the selected URL, as detailed in Table 9.

Table 9

| Field | Description |
| --- | --- |
| Scan Switch | This field is the flag designating whether the selected URL scan has finished in the VirusTotal infrastructure. |
| URL | This field is the scanned URL acknowledged from the VirusTotal database. |
| Positive/Total | This field is the number of positive scans detecting this URL out of the total number of scanners run by VirusTotal. |
| Scan Date | This field is the date on which the VirusTotal scanners last ran on the detected URL. |

# ADDING INDICATORS

Indicators can be directly added to the current owner by clicking on a contextual **Plus (+)** button next to the Indicator (Figure 10).

**Figure 10**

Indicators displayed within the app can provide valuable insight for an analyst. Leveraging the **Add** functionality from the VirusTotal Spaces app offers another level of integration while maintaining a consistent user experience. There are two ways to add a contextual Indicator within the app, as summarized in Table 10.

**Table 10**

| Type | Description |
|---|---|
| Single Add  | This button appears to the left of an Indicator and adds the Indicator individually with a single click. |
| Add All  | This button appears in the header row of the Indicator table. Clicking it brings up a confirmation window allowing all Indicators in the current table to be added. This feature saves time in cases where there are hundreds of Indicators to add. |

When an Indicator is added to the current owner, the app uses the parameters in Table 11, as highlighted in the "Parameter Definition" section. These parameters automate the task of adding Indicators with Tags, a Confidence Rating, and a Threat Rating. Once an Indicator has been added, the button will change to a **Details…** link, along with a success message. Clicking on the link will display the **Details** screen for that Indicator, and further updates can be performed if needed.

Table 11

| Name | Description |
| --- | --- |
| Comma-separated list of tags applied to indicator on an add | This parameter is a comma-separated list of Tags to apply to any Indicator added using this app. |
| Confidence applied to indicator on an add (0-100%) | This parameter is the confidence to apply to any Indicator added using this app. |
| Rating applied to indicator on an add (0-5 skulls) | This parameter is the rating to apply to any Indicator added using this app. |

On subsequent page loads for the added Indicators, the app recognizes if the Indicator exists for the current owner and will display a **Details…** hyperlink in place of the **Add** button. The hyperlink indicates that the Indicator exists, and clicking on it will display its **Details** screen.