



Symantec™ Threat Intelligence Enrichment User Guide

Symantec Threat Intelligence Enrichment User Guide

Last Major Revision: 16 Apr 2021

- [Symantec Threat Intelligence Enrichment Integration Guide ThreatConnect Platform](#)
 - [Introduction](#)
 - [Configuration](#)
 - [Requirements](#)
 - [Symantec Threat Intelligence Credentials](#)
 - [Adding Symantec Threat Intelligence Attributes](#)
 - [Symantec Threat Intelligence Playbook Templates](#)
 - [Symantec Threat Intelligence Enrichment Playbooks Templates Installation](#)
 - [Browse to the existing File, Address or Host Indicators \(or\) Create a new Indicator](#)
 - [For File Indicators, you will see the “Symantec Threat Intelligence API” Playbook Action in the details page for "File Related", "File Protection" and "File Insight"](#)
 - [For Host and Address Indicators, you will see the “Symantec Threat Intelligence API” Playbook Action in the details page for "Network Related", "Network Protection" and "Network Insight"](#)
 - [Reports](#)
 - [File Insight Report](#)
 - [File Protection Report](#)

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. Copyright ©2021 Broadcom. All Rights Reserved.

- [File Related Report](#)
- [Network Insight Report](#)
- [Network Protection Report](#)
- [Network Related Report](#)
- [APPENDIX](#)
 - [Symantec Threat Intelligence File Insight](#)
 - [Symantec Threat Intelligence Network Insight](#)
 - [Symantec Threat Intelligence File Related](#)
 - [Symantec Threat Intelligence Network Related](#)
 - [Symantec Threat Intelligence File Protection](#)
 - [Symantec Threat Intelligence Network Protection](#)
 - [Symantec Threat Intelligence Network Insight - JSON](#)
 - [Symantec Threat Intelligence File Insight - JSON](#)
 - [Symantec Threat Intelligence Network Related - JSON](#)
 - [Symantec Threat Intelligence File Related - JSON](#)
 - [Symantec Threat Intelligence Network Protection - JSON](#)
 - [Symantec Threat Intelligence File Protection - JSON](#)

Symantec Threat Intelligence Enrichment Integration Guide

ThreatConnect Platform

User Guide v1.0.0

Introduction

Symantec Threat Intelligence is powered by the security industry's largest and most diverse set of threat data to deliver fast, real-time global content. Trusted by more than 15,000 enterprises globally, including over 70% of the Fortune 500, Symantec Threat Intelligence Services allow businesses to implement risk control policies to extend web security to cloud applications. A strategic component of the Symantec Security Platform, Intelligence Services employ 200+ analytics engines to identify mass-market, targeted threats, blocking more than 99.99% of known and emerging threats.

Symantec has the ability to dynamically analyze and categorize new content as soon as it is introduced. With more than 200 threat analytics engines, the Global Intelligence Network can process more than one billion web and file requests daily, in over 60 languages. It is truly the most advanced real-time content and threat categorization network available today.

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. Copyright ©2021 Broadcom. All Rights Reserved.

For more information, see <https://www.broadcom.com/info/symantec/global-intelligence-network>

This document outlines the processes to configure and integrate **Symantec Threat Intelligence** Playbooks within the ThreatConnect Platform. The Symantec Threat Intelligence Playbooks enable ThreatConnect Platform users to perform On-Demand Enrichment of indicators (files, domains and IPs) using the Symantec Threat Intelligence APIs.

Configuration

Requirements

The following requirements must be met to use the Symantec Threat Intelligence Playbooks in your ThreatConnect environment:

- Access to ThreatConnect instance.
- Access to execute ThreatConnect Playbooks.
- Symantec Threat Intelligence API key and secret provisioned by Symantec for authenticating requests to the API.
- Symantec Threat Intelligence Server API URL.
- *TBC app dependencies installed in ThreatConnect Instance.
- Symantec Threat Intelligence Playbook Templates installed in ThreatConnect Instance.
- Symantec Threat Intelligence specific custom attributes imported in ThreatConnect Instance.

Symantec Threat Intelligence Credentials

Add the following Variables to the Organization Settings page:

1. Click on the settings (gear icon) in the top right corner in the ThreatConnect platform to select Org Settings, and then navigate to **Variables**.
2. Click **New Variable** for each of the below:

Name	Type	Value
Symantec ThreatIntel client_id	TEXT	This is the API key provided to your organization by Symantec

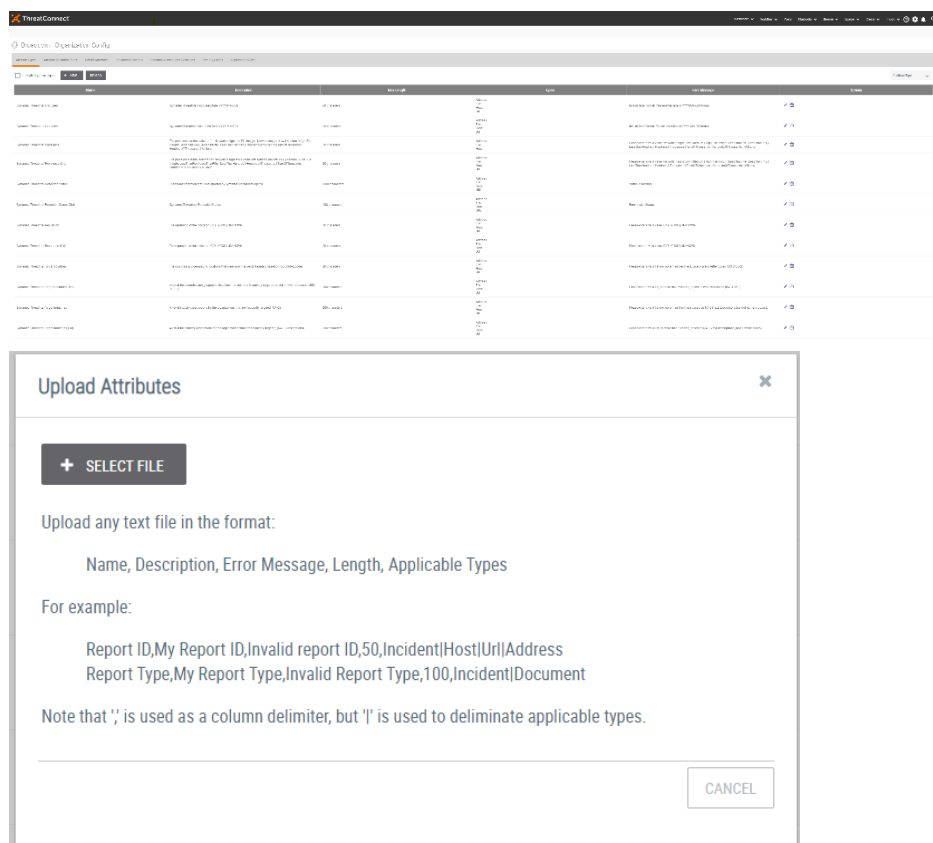
Symantec ThreatIntel client_secret	KEYCHAIN	This is the API secret provided to your organization by Symantec
---------------------------------------	----------	---



Adding Symantec Threat Intelligence Attributes

You can find the *Symantec_ThreatIntel_Attributes.json* file available on GitHub; please download it.

1. Click on the settings (gear icon) in the top right to get to your Org Config page.
2. Click **Upload**.
3. Click **Select File** and navigate to the *json* file downloaded previously.
4. Click **Save**.
5. Upon saving the *Symantec ThreatIntel Attributes* file, custom attributes are available,
6. Repeat this process for each Source used:
 1. Click on the settings (gear icon) in the top right to get to your Org Settings page.
 2. Navigate to **Communities/Sources**.
 3. Click on the **Source** in the **Name** column.
 4. Click **Source Config**.
 5. Click **Upload** and repeat the process as above from Step 2.



Symantec Threat Intelligence Playbook Templates

Symantec Threat Intelligence Enrichment Playbooks Templates Installation

Symantec Threat Intelligence provides 12 Playbook Templates, broken down into three broad types:

1. **Insight APIs** provide file and domain/ip enrichments which include first seen and last seen date, reputation and prevalence band, top N countries and industries. Default top N is currently set to 5.
2. **Related APIs** provide related file or network information, which include array of related network indicators and an array of related filenames for a given file or network IOC (domain or IP address).
3. **Protection APIs** provide information regarding whether a given IoC(file sha256, domain or an IP Address) has been blocked by any of Symantec technologies such as "AntiVirus (AV)", "Intrusion Prevention System(IPS)" and "Behavioral Analysis & System Heuristics" (BASH). If the IoC is blocked then details are provided.

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. Copyright ©2021 Broadcom. All Rights Reserved.

Name	Description
Symantec Threat Intelligence File Insight	Returns file insight enrichments for given file sha256.
Symantec Threat Intelligence Network Insight	Returns network insight enrichments for a given domain or IP.
Symantec Threat Intelligence File Related	Returns network or file related information for a given file sha2.
Symantec Threat Intelligence Network Related	Returns network or file related information for a given network domain or IP.
Symantec Threat Intelligence File Protection	Returns protection status for given file_sha256.
Symantec Threat Intelligence Network Protection	Returns protection status for given network domain or IP.
Symantec Threat Intelligence File Insight - JSON	Returns file insight enrichments JSON string for given file sha256.
Symantec Threat Intelligence Network Insight - JSON	Returns network insight enrichments JSON string for a given domain or IP.
Symantec Threat Intelligence File Related - JSON	Returns network or file related information JSON string for a given file sha2.
Symantec Threat Intelligence Network Related - JSON	Returns network or file related information JSON string for a given network domain or IP.
Symantec Threat Intelligence File Protection - JSON	Returns protection status JSON string for given file_sha256.
Symantec Threat Intelligence Network Protection - JSON	Returns protection status JSON string for given network domain or IP.

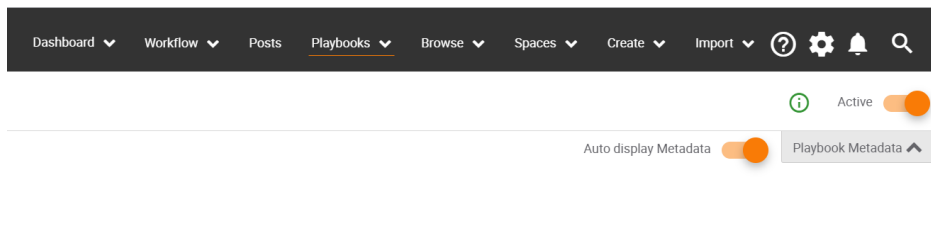
[illegible]

The Playbook Templates are available on GitHub, which provides a basic understanding on how to use the core Symantec Threat Intelligence APIs. To install the Playbook Templates:

1. Go to the Playbooks tab in the ThreatConnect Platform.
2. Select **New** and **Import**, then locate the PBX file you wish to add to your ThreatConnect Platform.
3. Follow the on-screen instructions to complete the import process.

Making sure the Playbook is set to active

1. Go to the Playbooks menu in the top banner area.
2. Click and open each of the Symantec Threat Intelligence playbooks.
3. Toggle the switch in the top-left to mark the playbook as active.



Browse to the existing File, Address or Host Indicators (or) Create a new Indicator

The screenshot shows the ThreatConnect interface with a list of indicators. The table has columns: Type, Date, Symantec ID, Symantec ID, Date, Type, and Tag. The indicators are listed with their respective dates and Symantec IDs. The interface also shows a sidebar with various navigation options and a top navigation bar.

File: [D48EB40C5D381DE1451F72BA519D932B2A86D0C2388C67BB5A164E64C0130B6C](#) [View full details](#) [Broadcast Source](#)

File: ECA5AFBF0AD20DA2E6FD7D48E1C4BC028CB8A67AD7C6FDC3E7D3500FF5F71A1D [Broadcast Source](#)

For File Indicators, you will see the “Symantec Threat Intelligence API” Playbook Action in the details page for "File Related", "File Protection" and "File Insight"

- Click on the play button to run the desired playbook:

The screenshot shows the Playbook Actions modal with a table of available playbooks. The table has columns: Run, Name, and Status. The playbooks are listed with their respective names and statuses.

Run	Name	Status
	Symantec Threat Intelligence API - File Related JSON	Ready
	Symantec Threat Intelligence API - File Related	Ready
	Symantec Threat Intelligence API - File Protection JSON	Ready
	Symantec Threat Intelligence API - File Protection	Ready
	Symantec Threat Intelligence API - File Insight JSON	Ready
	Symantec Threat Intelligence API - File Insight	Ready

- Once the playbook has completed, the status will be shown and a report is generated containing the summary information. A link to this report is provided as a *html-hover* field:







The screenshot shows the Playbook Actions modal with a table of available playbooks. The table has columns: Run, Name, and Status. The playbooks are listed with their respective names and statuses. A success message is displayed above the table.

Success- link to report







Run	Name	Status
	Symantec Threat Intelligence API - File Related	Completed
	Symantec Threat Intelligence API - File Protection	Ready
	Symantec Threat Intelligence API - File Insight	Ready

- Additionally, a playbook may have created **Symantec ThreatIntel Attributes** related to the playbook actions. These are associated with the current indicator (the page must be refreshed (F5) in order for them to be displayed immediately):

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. Copyright ©2021 Broadcom. All Rights Reserved.

Playbook Actions		
Run	Name	Status
	Symantec Threat Intelligence API - Network Insight	
	Symantec Threat Intelligence API - Network Related	Ready
	Symantec Threat Intelligence API - Network Protection	Ready
	Symantec Threat Intelligence API - Network Insight JSON	Ready
	Symantec Threat Intelligence API - Network Related JSON	Ready
	Symantec Threat Intelligence API - Network Protection JSON	Ready

- Once the playbook has completed, the status is shown and a report is generated, containing the summary information. A link to this report is provided as a *html-hover* field:

Playbook Actions		
Run	Name	Status
	Symantec Threat Intelligence API - Network Insight	Completed
	Symantec Threat Intelligence API - Network Related	Ready
	Symantec Threat Intelligence API - Network Protection	Ready
	Symantec Threat Intelligence API - Network Insight JSON	Ready
	Symantec Threat Intelligence API - Network Related JSON	Ready
	Symantec Threat Intelligence API - Network Protection JSON	Ready

- Additionally, a playbook may have created **Symantec ThreatIntel Attributes** related to the playbook actions. These are associated with the current indicator (the page must be refreshed (F5) in order for them to be displayed immediately):

Attributes	
Symantec ThreatIntel Target Countries	<div> <div></div> <div>None</div> </div> <div>us, nl, jp</div> <div>Last Updated: 04-27-2021 21:19 GMT by Broadcom / Tony Zhu</div>
Symantec ThreatIntel Reputation	<div> <div></div> <div>None</div> </div> <div>BAD</div> <div>Last Updated: 04-27-2021 21:19 GMT by Broadcom / Tony Zhu</div>
Symantec ThreatIntel Prevalence	<div> <div></div> <div>None</div> </div> <div>Low</div> <div>Last Updated: 04-27-2021 21:19 GMT by Broadcom / Tony Zhu</div>
Symantec ThreatIntel Last Seen	<div> <div></div> <div>None</div> </div> <div>2020-11-12</div> <div>Last Updated: 04-27-2021 21:19 GMT by Broadcom / Tony Zhu</div>
Symantec ThreatIntel First Seen	<div> <div></div> <div>None</div> </div> <div>2020-10-20</div> <div>Last Updated: 04-27-2021 21:19 GMT by Broadcom / Tony Zhu</div>

Reports

File Insight Report

<div> <div>Q RPT</div> <div>FILE</div> <div>COMP TO ANAL</div> <div>DOWNLOAD RPT</div> </div> <div> <div>SEARCH</div> <div>EDIT</div> <div>TABLE</div> <div>COMMENTS</div> <div>SHARE</div> <div>EXPORT</div> </div>	
<div> <div>Description</div> <div> <div>File Name: File Insight</div> <div>Report generated: 2021-04-27 09:41:48Z</div> <div>Report on: BAD</div> <div>File Name: File Insight</div> <div>File Size: 2021-04-27 09:41:48Z</div> <div>Last Seen: 2020-11-12</div> <div>Target Countries: us, nl, jp</div> <div>Target Reputation: BAD</div> </div> <div> <div>Source</div> <div> <div>File Name: File Insight</div> <div>File Size: 2021-04-27 09:41:48Z</div> <div>Last Seen: 2020-11-12</div> </div> </div> </div> <div> <div>Security Labels</div> <div> <div>File Name: File Insight</div> <div>File Size: 2021-04-27 09:41:48Z</div> <div>Last Seen: 2020-11-12</div> </div> </div> <div> <div>Report File</div> <div> <div>Original File Name</div> <div>File Type: File Insight</div> <div>File Size: 2021-04-27 09:41:48Z</div> <div>Status: Pending Review</div> </div> </div>	<div> <div>Associations</div> <div> <div>Associated Groups (0)</div> <div>Associated Indicators (7)</div> <div>Associated Victim Assets (0)</div> </div> </div> <div> <div>Details</div> <div> <div>Type: Report</div> <div>Added: 04-27-2021 09:41:48Z by Tony Zhu</div> <div>File Name: File Insight</div> </div> </div> <div> <div>Tags</div> <div> <div>File Insight</div> <div>File Insight</div> </div> </div>

File Protection Report

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. Copyright ©2021 Broadcom. All Rights Reserved.

File Related Report

Network Insight Report

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. Copyright ©2021 Broadcom. All Rights Reserved.

Network Protection Report

Symantec ThreatIntel Network Protection Report - 2021-04-27T21:29:19Z

VIEW PROTECT SELECT DOWNLOAD PDF

Overview Tasks Activity Associations Sharing Sources

Description

Broadcom / Tony Zhu says

None

Network Protection State: Antivirus: cl.commergent1 - firstDefectVersion: 2020.12.10.020, Intrusion Prevention System: System infected: Trojan.Backdoor.Activity.447, firstDefectVersion: 20210423.087

Source

Broadcom / Tony Zhu says

None

minerGate.com

Security Labels

Choose Security Labels

Report File

Original File: None

File Type: Unrecognized

File Size:

Status: Awaiting Manual

UPLOAD FILE

Attributes

Description

None

Network Protection State: Antivirus: cl.commergent1 - firstDefectVersion: 2020.12.10.020, Intrusion Prevention System: System infected: Trojan.Backdoor.Activity.447, firstDefectVersion: 20210423.087

Last Updated: 04-27-2021 21:29 GMT

by Broadcom / Tony Zhu

Associations

Graph Table

Associated Groups (0)

Associated Indicators (1)

Type	Artifact	Case	Analysis	Date
Host	minerGate.com	Broadcom		03-29-2021

Associated Victim Assets (0)

Associated Artifacts (0)

Associated Cases (0)

Potential Associations (0)

Artifacts (0)

Cases (0)

Details

Type: Report

Added: 04-27-2021 21:29 GMT by Tony Zhu

Published Date: 04-27-2021

Network Related Report

Symantec ThreatIntel Network Related Report - 2021-04-27T21:53:31Z

VIEW PROTECT SELECT DOWNLOAD PDF

Overview Tasks Activity Associations Sharing Sources

Description

Broadcom / Tony Zhu says

None

Report generated: 2021-04-27T21:53:31Z

Related Files: fadecdf732bf4318ee3bdc31bee87763256c96dab0851cb94e456c725e7d5, f405a7510f5ca015d0f966e0e44c9ca160443ee9fa72cd54807f2241b16dd

Related Hosts: None

Related Addresses: None

Source

Broadcom / Tony Zhu says

None

minerGate.com

Security Labels

Choose Security Labels

Report File

Original File: None

File Type: Unrecognized

File Size:

Status: Awaiting Upload

UPLOAD FILE

Associations

Graph Table

Associated Groups (0)

Associated Indicators (1)

Type	Artifact	Case	Analysis	Date
Host	minerGate.com	Broadcom		03-29-2021

Associated Victim Assets (0)

Associated Artifacts (0)

Associated Cases (0)

Potential Associations (0)

Artifacts (0)

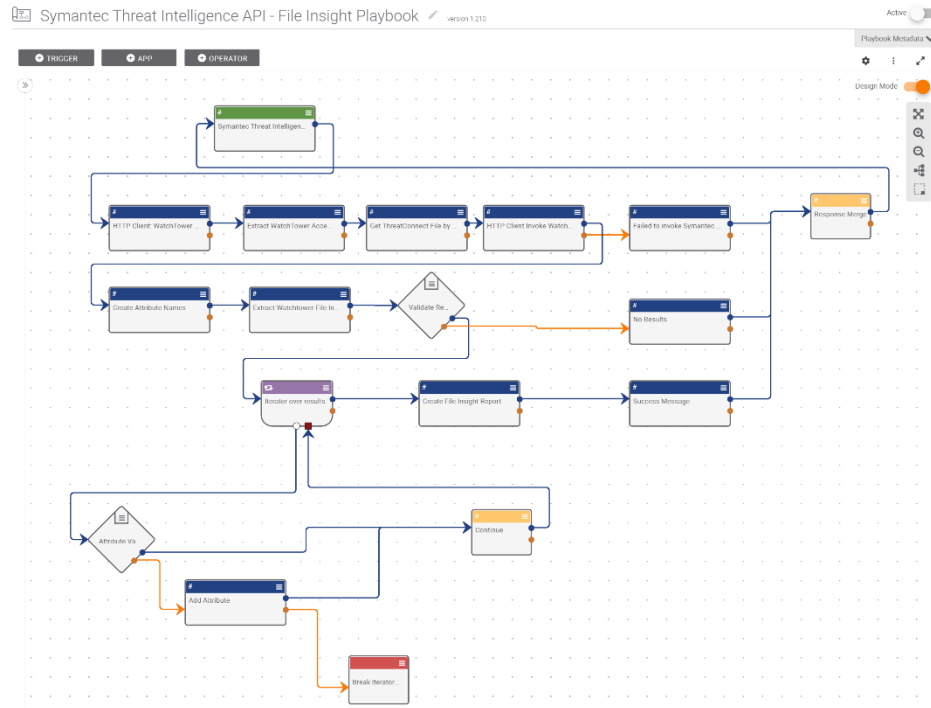
Cases (0)

APPENDIX

Symantec Threat Intelligence File Insight

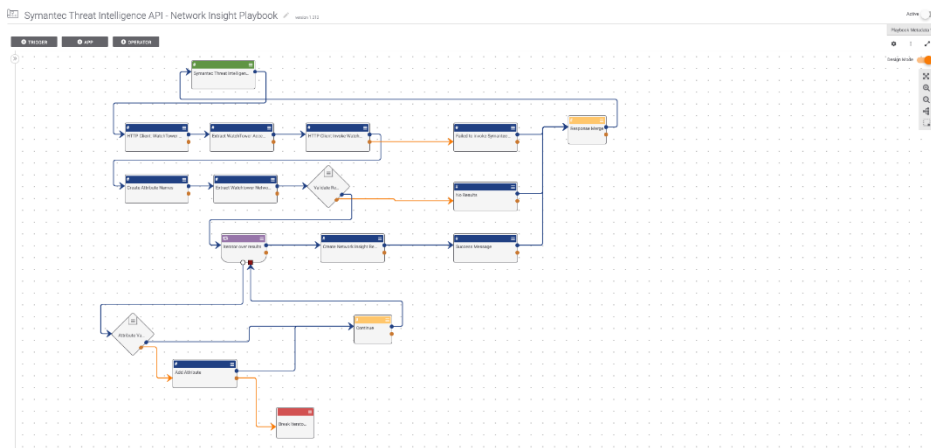
Returns file insight enrichments for given file sha256.

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. Copyright ©2021 Broadcom. All Rights Reserved.



Symantec Threat Intelligence Network Insight

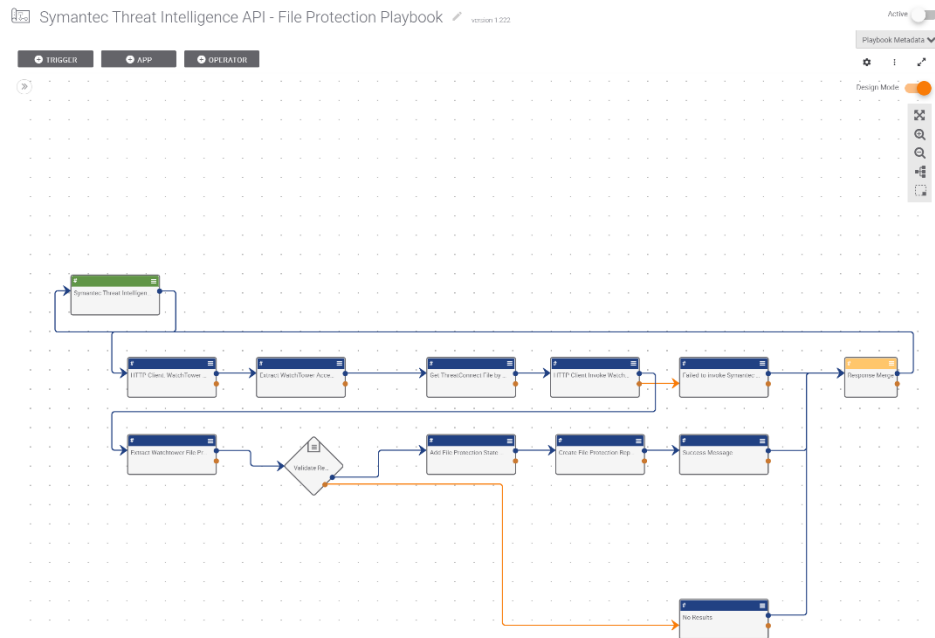
Returns network insight enrichments for a given domain or IP.



Symantec Threat Intelligence File Related

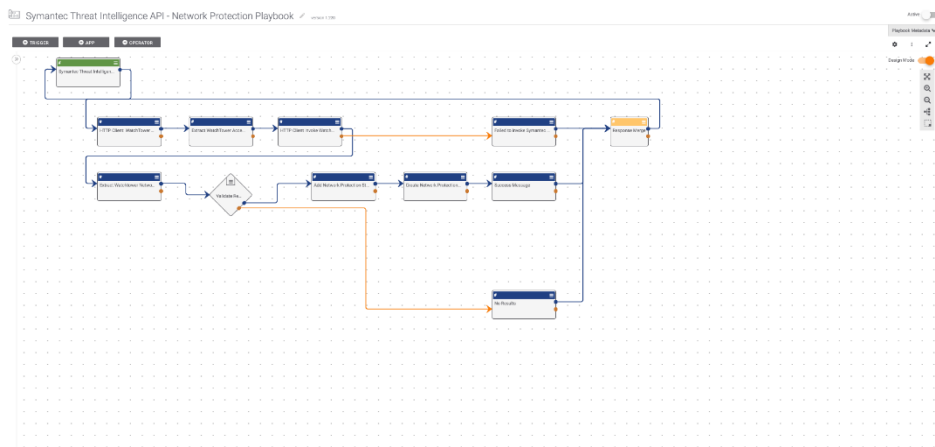
Returns network or file related information for a given file sha256.

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. Copyright ©2021 Broadcom. All Rights Reserved.



Symantec Threat Intelligence Network Protection

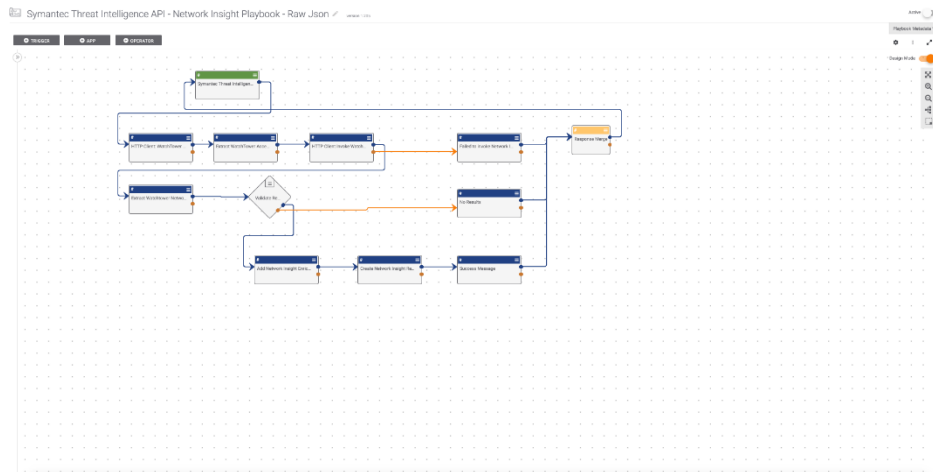
Returns protection status for given a given domain or IP.



Symantec Threat Intelligence Network Insight - JSON

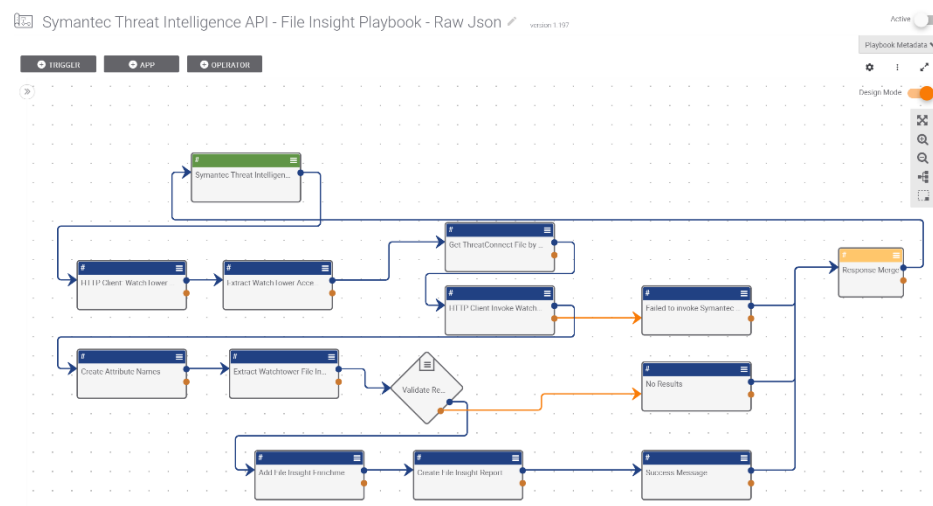
Returns network insight enrichments JSON string for a given domain or IP.

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. Copyright ©2021 Broadcom. All Rights Reserved.



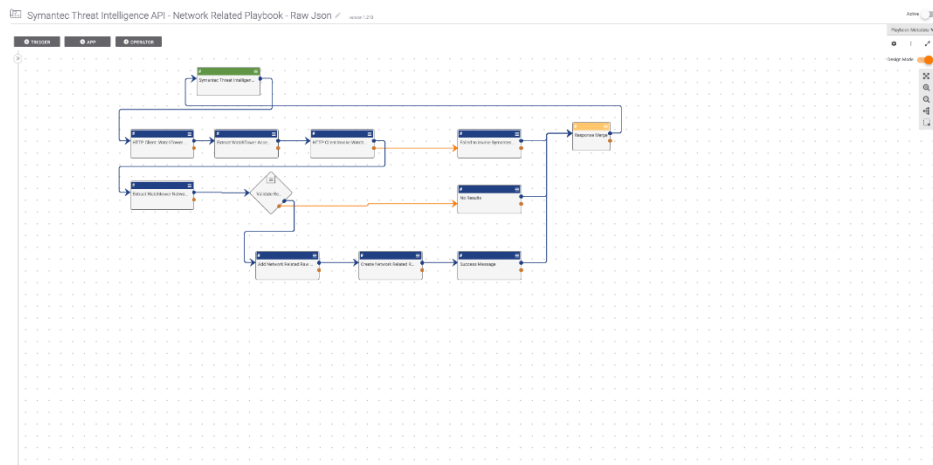
Symantec Threat Intelligence File Insight - JSON

Returns file insight enrichments JSON string for a given sha256.



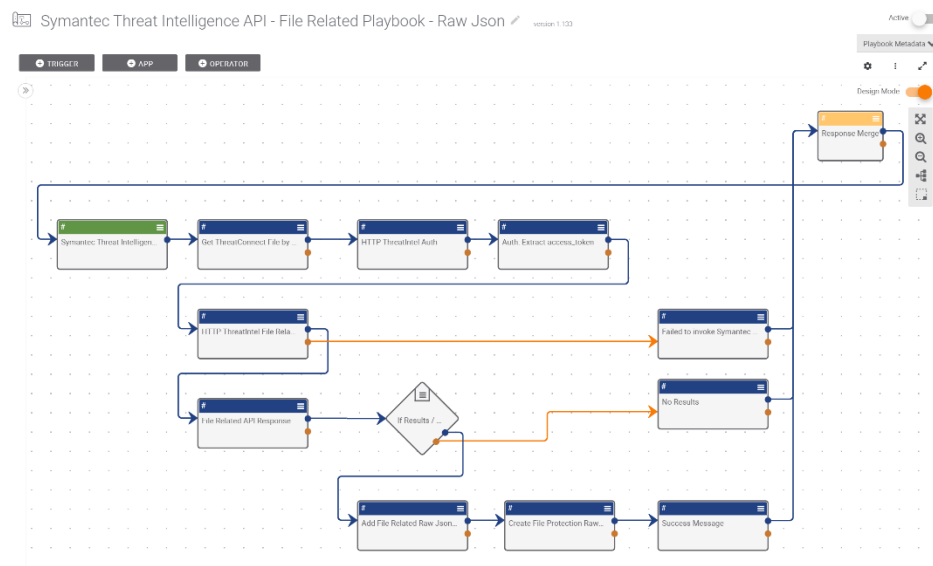
Symantec Threat Intelligence Network Related - JSON

Returns network or file related information JSON string for a given domain or IP.



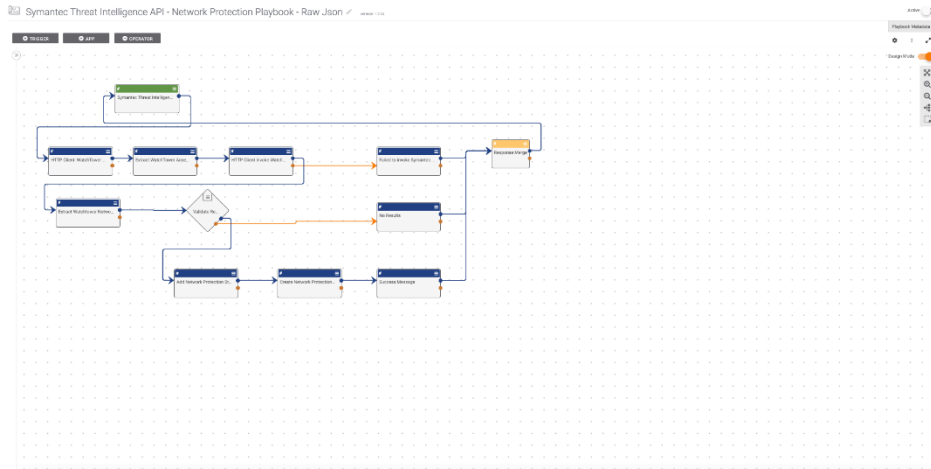
Symantec Threat Intelligence File Related - JSON

Returns network or file related information JSON string for a given sha256.



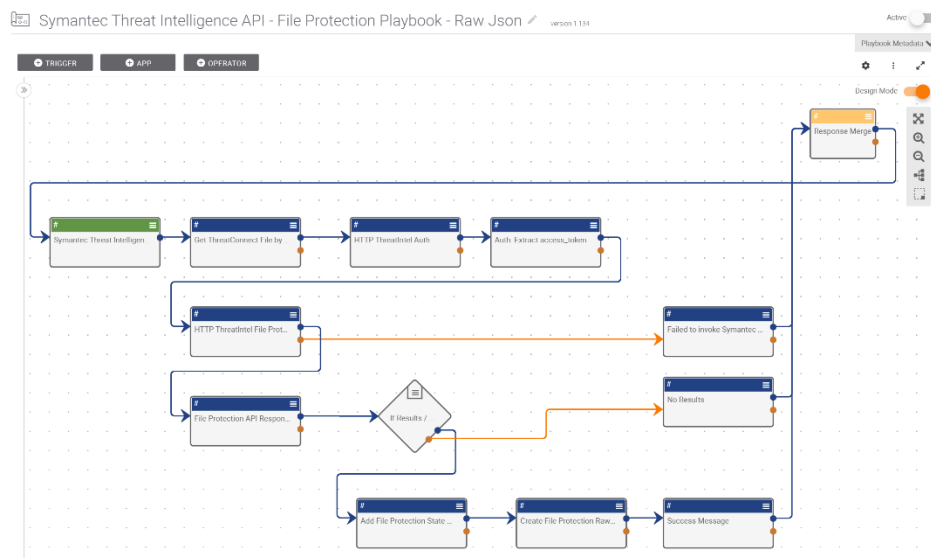
Symantec Threat Intelligence Network Protection - JSON

Returns protection status JSON string for given a given domain or IP.



Symantec Threat Intelligence File Protection - JSON

Returns protection status JSON string for given a given sha256.



Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. Copyright ©2021 Broadcom. All Rights Reserved.

Support

Technical Support and Enterprise Customer Support Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:
<https://entced.symantec.com/default/ent/supportref>

To contact Symantec Support, see: https://support.symantec.com/en_US/contact-support.html