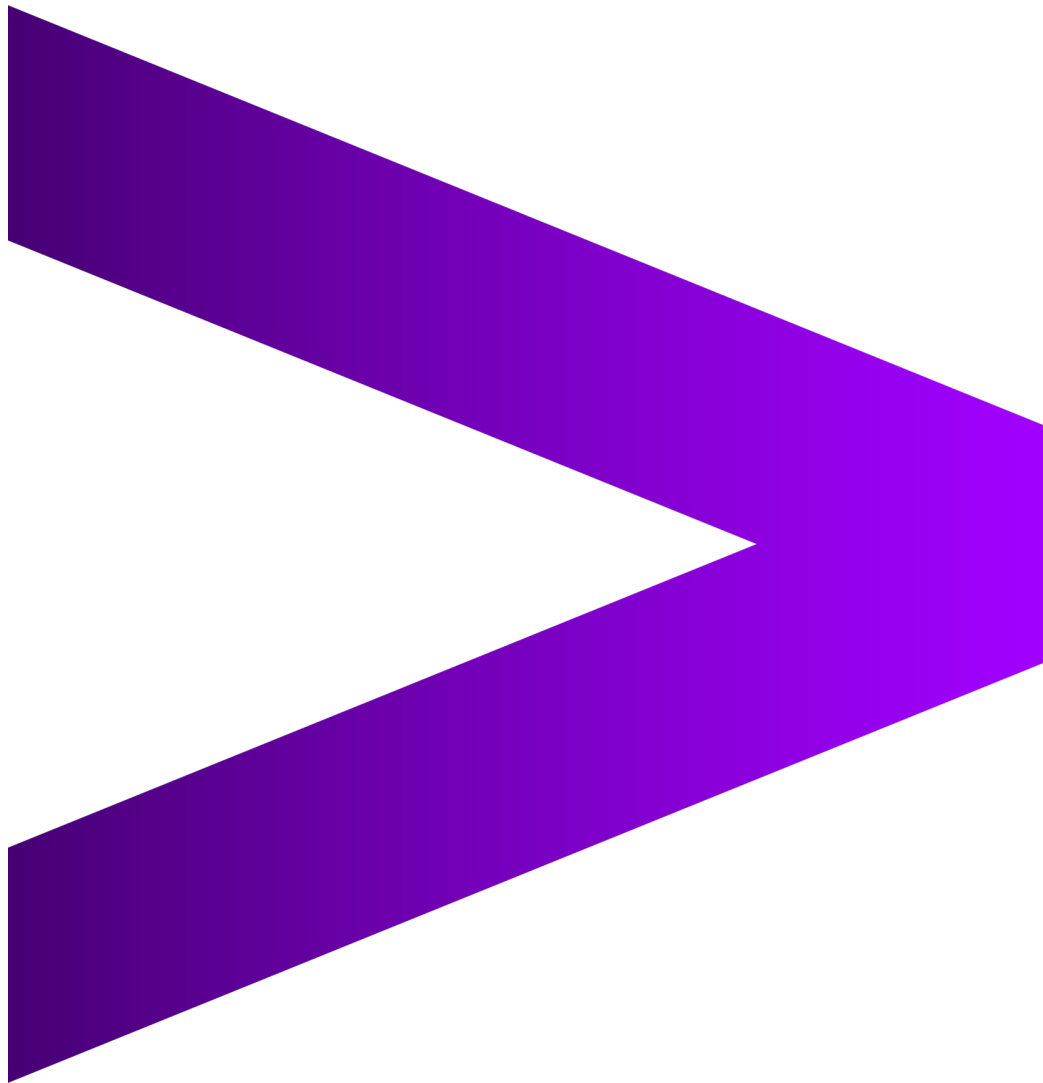


# **ACTI ADD-ON FOR SPLUNK**

## **ACCENTURE CYBER THREAT INTELLIGENCE**



Accenture Security

Table of Contents

**About .....3**

**Requirements.....3**

**Installation and Configuration .....3**

    Installation .....3

    Manually Load Historical Threat Intelligence.....5

    Change Intelligence Download Frequency.....5

    Adding Accenture CTI Notable Review Fields to Splunk ES.....6

    Configure Threat Intelligence Retention.....7

**Contents.....7**

    Threat Intelligence KV Store.....7

    Macros for Data Enrichment.....9

    Accenture CTI Integration Health Check Dashboard.....9

    Correlation Search/Alert: iDefense Threat Match .....10

**Troubleshooting .....11**

    Where to find the Logs for this Add-On .....11

    Changing Log Level.....12

    Health Check Dashboard.....13

**Splunk Mission Control.....13**

    Getting the add-on ready for Splunk Mission Control .....13

## About

The iDefense Technology Add-on provides an easy way to interact with iDefense IntelGraph API by loading threat indicators into the Splunk Enterprise Security Threat Intelligence Framework.

## Requirements

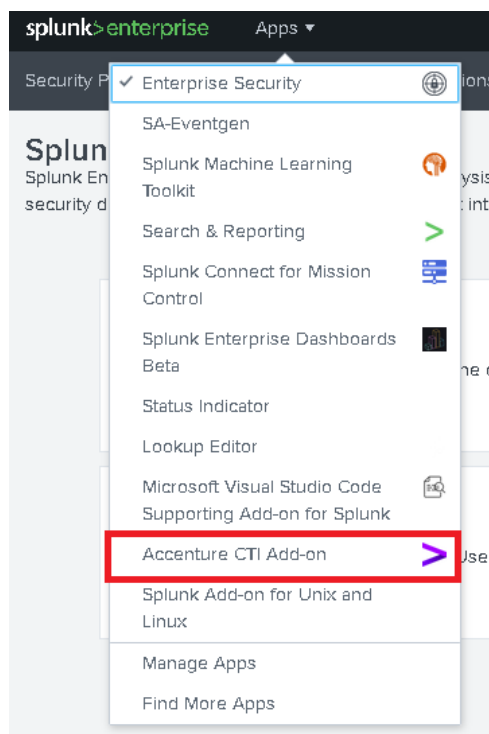
Current Add On Version	Supported Version of Splunk Enterprise
3.0.0	8.1, 8.0, 7.3
3.1.0	8.1, 8.0, 7.3

- Enterprise for Security must be installed for the TA to function correctly.
- The customer must have a subscription to Threat Indicator API and be able to generate an API token from the iDefense IntelGraph portal.

## Installation and Configuration

### Installation

- Generate API token from IG portal at the [user profile page](#). The token must have at least the "iGraph Read API Threat Indicator" role.
- Install the add-on from [Splunkbase](#) into the Splunk Search Head containing Splunk ES.
- Once installed, click on the "Apps" drop-down menu, then on the iDefense Intelgraph Add-On.



- Then click on Continue to App Setup Page.

## App configuration

The "Accenture CTI Add-on" app has not been fully configured yet.

This app has configuration properties that can be customized for this Splunk instance. Depending on the app, these properties may or may not be required.

Continue to app setup page

- In the next page, paste the API key previously generated, then submit.

splunk>enterprise
Apps
Administrator
Accenture CTI Health Check
Search
Reports
Alerts
Setup

## Setup

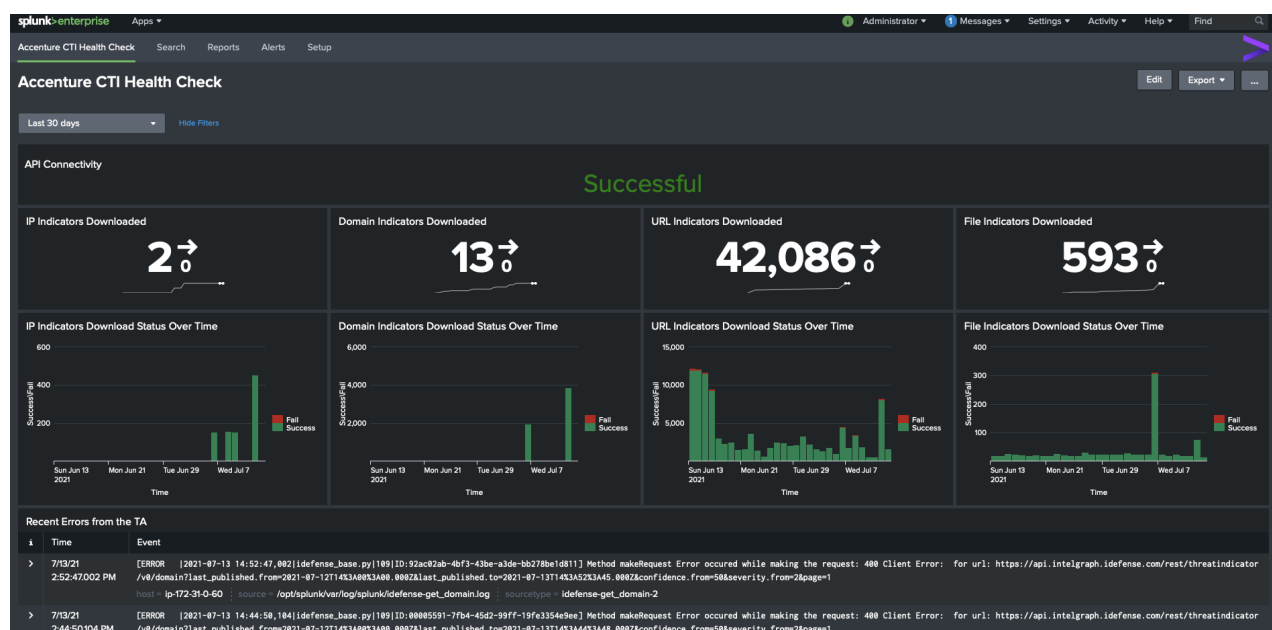
### Welcome to Accenture CTI Credentials Setup Page!

**API Access Token:**

Please specify the API token that will be used to authenticate to the API.



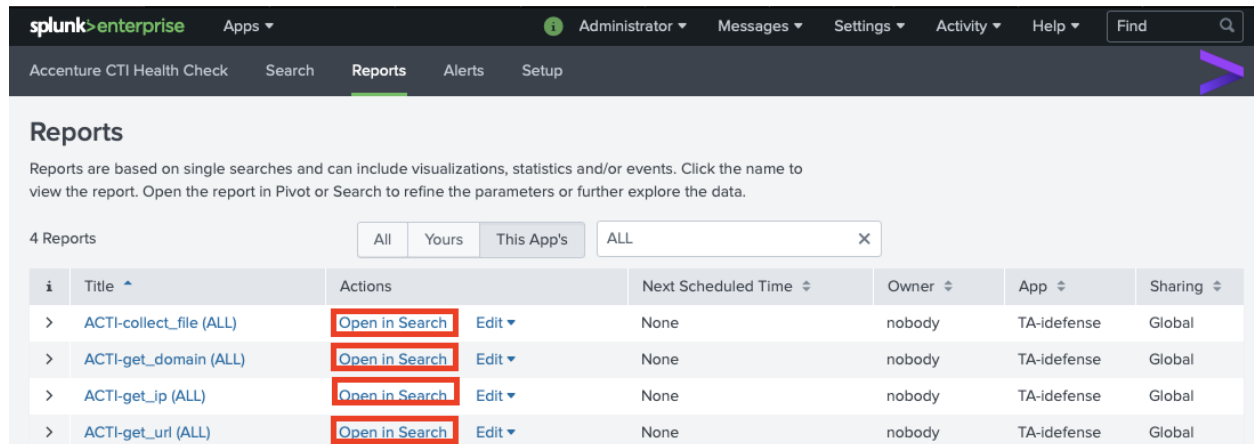
- Clicking on the app should now present the Health Check Dashboard. Connectivity to the API server should show as successful in the Health Check Dashboard.



## Manually Load Historical Threat Intelligence

The Technical Add-On automatically fetches Threat Intelligence updates every 4 hours from Accenture IntelGraph. However, after the first install, the data can be downloaded manually for the first time to get historical context and alerts for historical intelligence data. To do this, run the following searches, in the following order:

1. ACTI-get\_url (ALL)
2. ACTI-get\_ip (ALL)
3. ACTI-get\_domain (ALL)
4. ACTI-collect\_file(ALL)



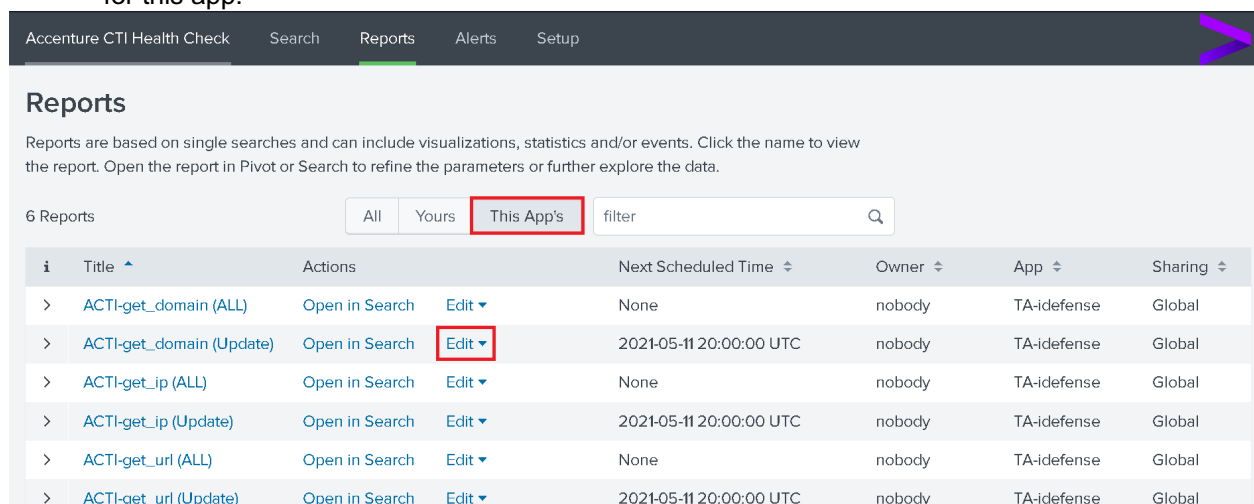
The screenshot shows the Splunk interface with the 'Reports' tab selected. The 'Reports' section displays a list of 4 reports. The 'Open in Search' button for each report is highlighted with a red box.

i	Title ^	Actions	Next Scheduled Time ⇅	Owner ⇅	App ⇅	Sharing ⇅
>	ACTI-collect_file (ALL)	<a href="#">Open in Search</a> <a href="#">Edit</a>	None	nobody	TA-idefense	Global
>	ACTI-get_domain (ALL)	<a href="#">Open in Search</a> <a href="#">Edit</a>	None	nobody	TA-idefense	Global
>	ACTI-get_ip (ALL)	<a href="#">Open in Search</a> <a href="#">Edit</a>	None	nobody	TA-idefense	Global
>	ACTI-get_url (ALL)	<a href="#">Open in Search</a> <a href="#">Edit</a>	None	nobody	TA-idefense	Global

## Change Intelligence Download Frequency

The TA downloads threat intel updates every four hours by default. However, this interval can be configured within Splunk by following the steps below:

- Navigate to the App in Splunk, then to the Reports Tab. Update the filter to show reports only within the scope for this app.



The screenshot shows the Splunk interface with the 'Reports' tab selected. The 'Reports' section displays a list of 6 reports. The 'Edit' button for the 'ACTI-get\_domain (Update)' report is highlighted with a red box.

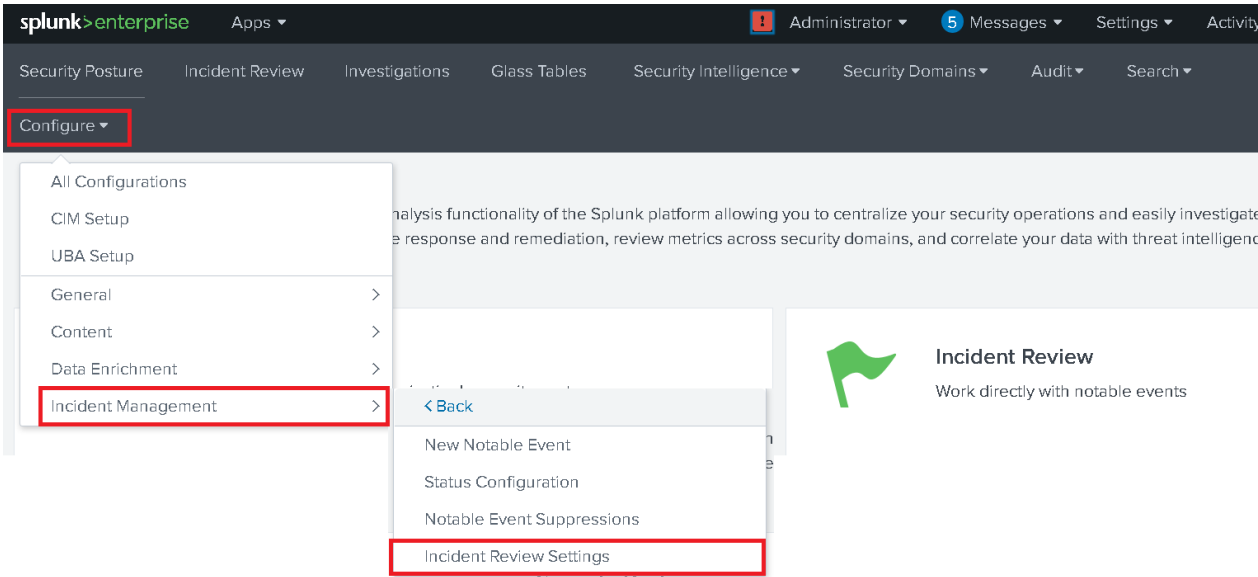
i	Title ^	Actions	Next Scheduled Time ⇅	Owner ⇅	App ⇅	Sharing ⇅
>	ACTI-get_domain (ALL)	<a href="#">Open in Search</a> <a href="#">Edit</a>	None	nobody	TA-idefense	Global
>	ACTI-get_domain (Update)	<a href="#">Open in Search</a> <a href="#">Edit</a>	2021-05-11 20:00:00 UTC	nobody	TA-idefense	Global
>	ACTI-get_ip (ALL)	<a href="#">Open in Search</a> <a href="#">Edit</a>	None	nobody	TA-idefense	Global
>	ACTI-get_ip (Update)	<a href="#">Open in Search</a> <a href="#">Edit</a>	2021-05-11 20:00:00 UTC	nobody	TA-idefense	Global
>	ACTI-get_url (ALL)	<a href="#">Open in Search</a> <a href="#">Edit</a>	None	nobody	TA-idefense	Global
>	ACTI-get_url (Update)	<a href="#">Open in Search</a> <a href="#">Edit</a>	2021-05-11 20:00:00 UTC	nobody	TA-idefense	Global

- Click on Edit > Edit Schedule for the Intel type that you wish to update the download frequency. Then change the CRON schedule as necessary.

### Adding Accenture CTI Notable Review Fields to Splunk ES

For data and notable enrichment, it is recommended to add Accenture CTI-specific notable review fields to Splunk ES. Please note that this is a required step if using the Splunk Mission Control Plugin. To add notable review fields, follow the steps below:

- Navigate to the Enterprise Security App, then to Configure > Incident Management > Incident Review Settings.



- In the Incident Review - Event Attributes, add the following Fields and Labels.

Field	Label
acti_confidence	ACTI Confidence Score
acti_key	ACTI Key
acti_key_type	ACTI Key Type
acti_last_published	ACTI Published Date
acti_malware_family	ACTI Malware Family
acti_severity	ACTI Severity
acti_threat_campaigns	ACTI Threat Campaigns
acti_threat_types	ACTI Threat Types
acti_uuid	ACTI UUID

- Click on Save, once finished adding the fields.

bytes_out	Bytes Out	<a href="#">Edit</a>   <a href="#">Remove</a>
category	Category	<a href="#">Edit</a>   <a href="#">Remove</a>
change_type	Change Type	<a href="#">Edit</a>   <a href="#">Remove</a>
channel	Channel	<a href="#">Edit</a>   <a href="#">Remove</a>
command	Command	<a href="#">Edit</a>   <a href="#">Remove</a>
cpu_load_percent	CPU Load (%)	<a href="#">Edit</a>   <a href="#">Remove</a>
creator	Creator	<a href="#">Edit</a>   <a href="#">Remove</a>
+ Add Field		

[Back to ES Configuration](#)
[Save](#)

## Configure Threat Intelligence Retention

<TO DO>

## Contents

### Threat Intelligence KV Store

The add-on stores the threat intelligence data from iDefense IntelGraph in the Splunk KV stores. The KV store for each intelligence type and their schema is as follows:

- acti\_threatindicator\_ip
- acti\_threatindicator\_domain
- acti\_threatindicator\_url

<b>uuid</b>	<b>string</b>	<b>The UUID for the indicator in IntelGraph.</b>
<b>type</b>	string	Denotes indicator type (IP, Domain or URL).
<b>threat_types</b>	array	List of associated critical intelligence requirement (CIR) types.
<b>threat_campaigns</b>	array	Threat Campaigns the indicator is associated with, if any.
<b>severity</b>	number	Numerical representation of severity from 1 to 5 with 1 being the least severe and 5 the most severe with the following options: Minimal, Low, Medium, High, Extreme.
<b>seen_at</b>	array	Other nodes in IntelGraph where this indicator was observed.
<b>mentioned_by</b>	array	If this indicator is mentioned by other nodes in IntelGraph.
<b>malware_family</b>	array	Classification of Malware, if associated with malware
<b>last_seen_as</b>	array	Lists any other Indicators that this might have been associated with.
<b>last_seen</b>	string	Date when the indicator was last observed in action.
<b>last_published</b>	string	Date when the indicator was published in IntelGraph.
<b>idn (Domain Only)</b>	array	Internationalized Domain Name, if the actual domain is in PunyCode
<b>files</b>	array	Files associated with this indicator.
<b>confidence</b>	array	Confidence Score for the indicator.
<b>asns (IP only)</b>	array	Autonomous System Numbers associated with the IP, if any.
<b>arguments (URL Only)</b>	array	List of arguments objects each containing a key value pair
<b>md5 (File Only)</b>	String	File Hash in MD5
<b>Sha1 (File Only)</b>	String	File hash in Sha1
<b>Sha256 (File Only)</b>	String	File hash in Sha256

The KV store above can be used to correlate against any logs and data models using the `lookup` and `inputlookup` command. The data from above KV store also gets incorporated into the Splunk's Threat Intelligence Framework. The data gets stored into the following KV stores that are within Splunk ES:

- ip\_intel
- http\_intel
- file\_intel



Check this [link](#) for more information on the Splunk's threat intel framework.

## Macros for Data Enrichment

The add on comes packaged with following Splunk Macros that can be used for enriching events with ACTI threat fields and used to correlate events:

- `acti_enrich_ip($ip$)`
- `acti_enrich_domain($domain$)`
- `acti_enrich_url($url$)`
- `acti_enrich_indicator($indicator$)`
- `acti_enrich_file_md5($indicator$)`
- `acti_enrich_file_sha1($indicator$)`
- `acti_enrich_file_sha256($indicator$)`

Use the macros above to look up IP addresses, domain names, URLs, or an indicator in general in the local ACTI KV store. Here is an example of the usage of the indicator enrichment macro:

The screenshot shows a Splunk search interface with the following details:

- Search Query:** `sourcetype="cisco:asa" | `acti_enrich_indicator(src)` | where isnotnull(acti_key)`
- Results:** 40,394 of 340,700 events matched. No Event Sampling.
- Visualization:** A timeline view showing a single event on May 12, 2021 at 9:00 AM.
- Event Details:**

Time	Event
5/12/21 5:31:58.000 PM	May 12 17:31:58 FR0THLY-FW1 %ASA-2-106001: Inbound TCP connection denied from 90.190.252.235/443 to 192.168.10.18/11144 flags FIN ACK on interface outside
- Enriched Fields (Highlighted in Red):**

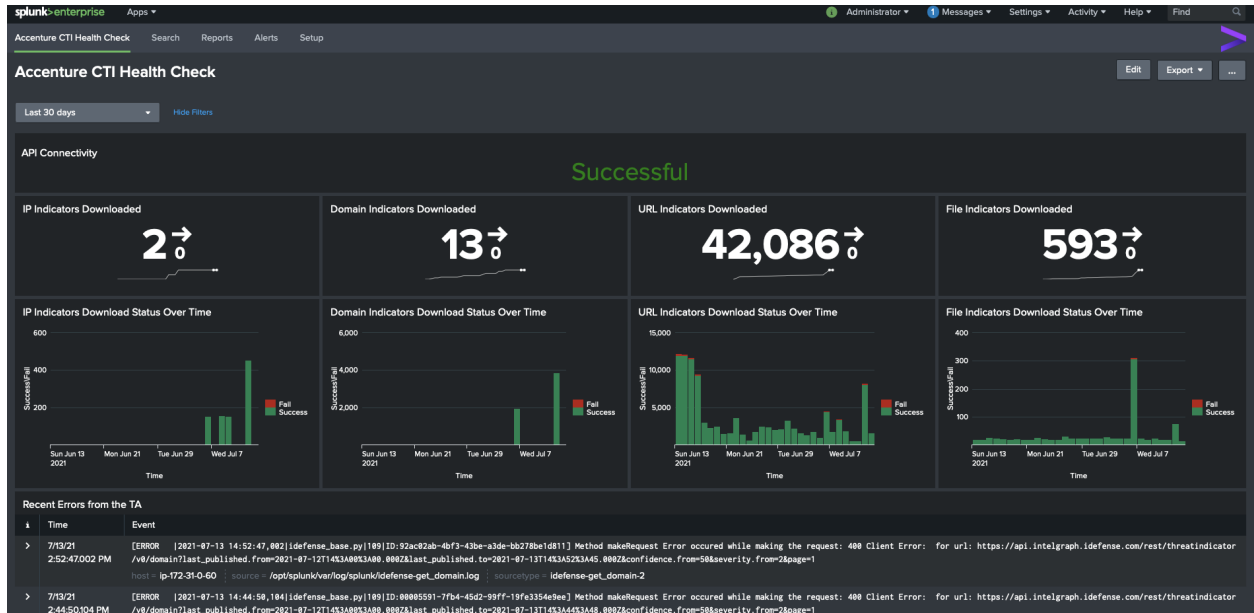
<code>acti_associated_files = 1eab299d86019a180e97ebf03b185</code>	<code>acti_confidence = 100</code>
<code>acti_key = 90.190.252.235</code>	<code>acti_key_type = ip</code>
<code>acti_last_modified = 2017-01-13T17:36:55.000Z</code>	<code>acti_last_published = 2017-01-13T16:46:28.000Z</code>
<code>acti_last_seen = 2017-01-13T17:36:08.000Z</code>	<code>acti_severity = 4</code>
<code>acti_threat_types = Cyber Espionage</code>	<code>acti_threat_types = Cyber Crime</code>
<code>acti_uuid = dd169b1a-5bbb-4ece-a337-5a3a17e39618</code>	<code>host = 127.0.0.1</code>
<code>source = eventgen:asa</code>	

## Accenture CTI Integration Health Check Dashboard

The add-on has a Health Check Dashboard that admins can use to check the health of the integration between Accenture CTI and Splunk. The Health Check dashboard has the following panels:

- **API Connectivity:** Shows the Connectivity Status to the ACTI API endpoints.
- **IP, Domain, URL Indicators Download:** Shows the number of indicators downloaded over the given time range.
- **IP, Domain, URL Indicator Download Status:** Shows each time the TA tried to pull indicators from ACTI and whether those attempts were successful.
- **Final Panel** shows recent errors from the TA.

The Health Check Dashboard appears as follows:



## Correlation Search/Alert: iDefense Threat Match

This TA comes bundled with a correlation search that triggers Splunk ES notables. This search looks for any indicator matches for data that is correctly parsed into either the Splunk Common Information Model and the threat intelligence data model. The correlation search is disabled by default so as to avoid unintentional impact to the customers SOC environment. The customer can enable the correlation search to enable alerts for any indicator matches against appropriately onboarded data. Following is an example of a notable that gets triggered by this alert:

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
<input checked="" type="checkbox"/>	5/11/21 5:05:04.000 PM	Threat	ACTI Threat Activity Detected for 109.206.187130 in Sourcetype cisco:asa	Medium	New	unassigned	
<b>Description:</b> Threat Activity was detected for 109.206.187130 from ACTI Threat Indicator List for sourcetype: cisco:asa and field: dest							
<b>Related Investigations:</b> Currently not investigated.							
<b>Correlation Search:</b> Threat - ACTI Threat Match							
<b>History:</b> View all review activity for this Notable Event							
<b>Contributing Events:</b> Search cisco:asa for 109.206.187130 in field dest							
<b>Original Event:</b> 05/11/2021 16:15:00 +0000, search_name="Threat - Source And Destination Match - Threat Gen", search_now=1620749700.000, info_min_time=1620747000.000, info_max_time=1620749700.000, info_search_time=1620749702.266, src="192.168.9.26", dest="109.206.187.130", weight=100, threat_match_field=dest, threat_match_value="109.206.187.130", orig_sourcetype="cisco:asa", threat_key=acti_ip_ioc, threat_collection=ip_intel, threat_collection_key="acti_ip_ioc 109.206.187.130"							
View original event							
<b>Additional Fields</b>		<b>Value</b>	<b>Action</b>				
ACTI Confidence Score		100					
ACTI Indicator		109.206.187130					
ACTI Key Type		ip					
ACTI Last Modified		2018-01-11T11:14:40.000Z					
ACTI Last Published		2018-01-11T11:14:40.000Z					
ACTI Malware Family		Satori					
ACTI Severity		3					
ACTI Threat Types		Cyber Crime					
ACTI UUID		909cd8f4-e2ff-42c3-87bb-12eb6fe870d9					
Destination		109.206.187130					
Host		ip-172-31-0-60					
Source		192.168.9.26					
Threat Category		threatlist_direct_csv					
Threat Collection		ip_intel					
Threat Collection Key		acti_ip_ioc 109.206.187130					

If the default correlation search for threat match is enabled ("Threat - Threat List Activity - Rule"), then this can cause problems. Enabling the correlation search above might lead to duplicate notables for the same threat types. To disable or suppress duplicate notables, add the following suppression rules:

×

Edit Suppression

Name

Suppress Duplicate Threat Match

Description

Suppression rule to suppress duplicate notables

Search

`get\_notable\_index` search\_name="Threat - Threat List Activity - Rule" threat\_group=idefense\_\*\_ioc OR threat\_group=acti\_\*\_ioc

Full search preview

`get\_notable\_index` search\_name="Threat - Threat List Activity - Rule" threat\_group=idefense\_\*\_ioc OR threat\_group=acti\_\*\_ioc \_time>1618549200

Use Start Time

☒

Start Time

4/16/2021

Events before this time will not be suppressed.

Use Expiration Time

☐

Expiration Time

5/12/2021

Events after this time will not be suppressed.

Cancel

Save

## Troubleshooting

### Where to find the Logs for this Add-On

This add-on logs to the following locations:

- \$SPLUNK\_HOME/var/log/idefense-get\_ip.log
- \$SPLUNK\_HOME/var/log/idefense-get\_domain.log
- \$SPLUNK\_HOME/var/log/idefense-get\_url.log
- \$SPLUNK\_HOME/var/log/idefense-collect\_file.log
- \$SPLUNK\_HOME/var/log/idefense-validate.log

The logs for each run of a TI pull can also be viewed in the Search Head UI, by viewing the search log. To view this log for a TI download that was run recently, follow the steps below:

- Navigate to the app's Home Page, then click on Reports. Then update the filters to view contents for only this app.

- Then, click on the report or TI pull that you want to view logs for. Then click on Job and then Inspect Job.

**iDefense-get\_domain (Update)**  
Retrieves new domains (updated in last 4 hours) from iDefense ThreatIndicator API

This scheduled report runs on cron schedule 0 \*14 \*\*\*. Its time range is last 24 hours. The following results were generated 3 hours ago.

✓ 0 events (4/18/21 12:00:00.000 PM to 4/19/21 12:00:00.000 PM)

Job ▾  
 Edit Job Settings...  
 Send Job to Background  
 Inspect Job

No results found

- Click on "search.log" in the pop-up that comes up to view search logs for the last run of the TI pull.

Search job inspector | Splunk 8.1.1 — Mozilla Firefox

https://35.80.149.186:8000/en-US/manager/TA-idefense/job\_inspector?sid=scheduler\_\_nobody\_VEEtaWRIZmV...

### Search job inspector

This search has completed in 1.351 seconds, but did not match any events. The terms specified in the highlighted portion of the search:

```
idefensegetdomain Output_KVstore=True Output_Threatlist=True confidence_from=50 severity_from=2 [| makeresults | addinfo | rename info_ma
st, info_min_time as earliest | return latest, earliest]
```

over the time range:

4/18/21 12:00:00.000 PM - 4/19/21 12:00:00.000 PM

did not return any data. Possible solutions are to:

- relax the primary search criteria
- widen the time range of the search
- check that the default search indexes for your account include the desired indexes

Learn more about troubleshooting empty search results at [Splunk Documentation](#)

(SID: scheduler\_\_nobody\_VEEtaWRIZmVuc2U\_\_RMD53b80620e582f4c7a\_at\_1618833600\_37214) [search.log](#)

Execution costs

Duration (seconds)	Component	Invocations	Input count	Output count
0.33	command.idefensegetdomain	1	-	-
0.00	command.timeline	1	-	-

## Changing Log Level

The log level for the add-on can be changed by updating its configuration file. To update the log level for the app, follow the steps below:

- Create a file named "idefense.conf" in the directory \$SPLUNK\_HOME/etc/apps/TA-idefense/local/
- Add the following config to the file above:

```
[default]
log_level=INFO
#Following values are allowed for log level
# INFO, WARNING, ERROR, CRITICAL
```

Restarting the Splunk service is not required for the above config file to take effect.

### Health Check Dashboard

The add-on comes with a Health Check Dashboard, providing a single place to view the health of integration between Splunk and IntelGraph. Please refer to the Health Check Dashboard [section](#) for more information.

## Splunk Mission Control

### Getting the add-on ready for Splunk Mission Control

The following steps will ensure that the ACTI IntelGraph integration works with Splunk Mission Control Plugin for ACTI:

Complete the installation and requirement of this TA on all of the Splunk ES Search Heads.

Add ACTI Notable Fields in the Notable Review Settings.

Enable the ACTI Threat Match Correlation Search.