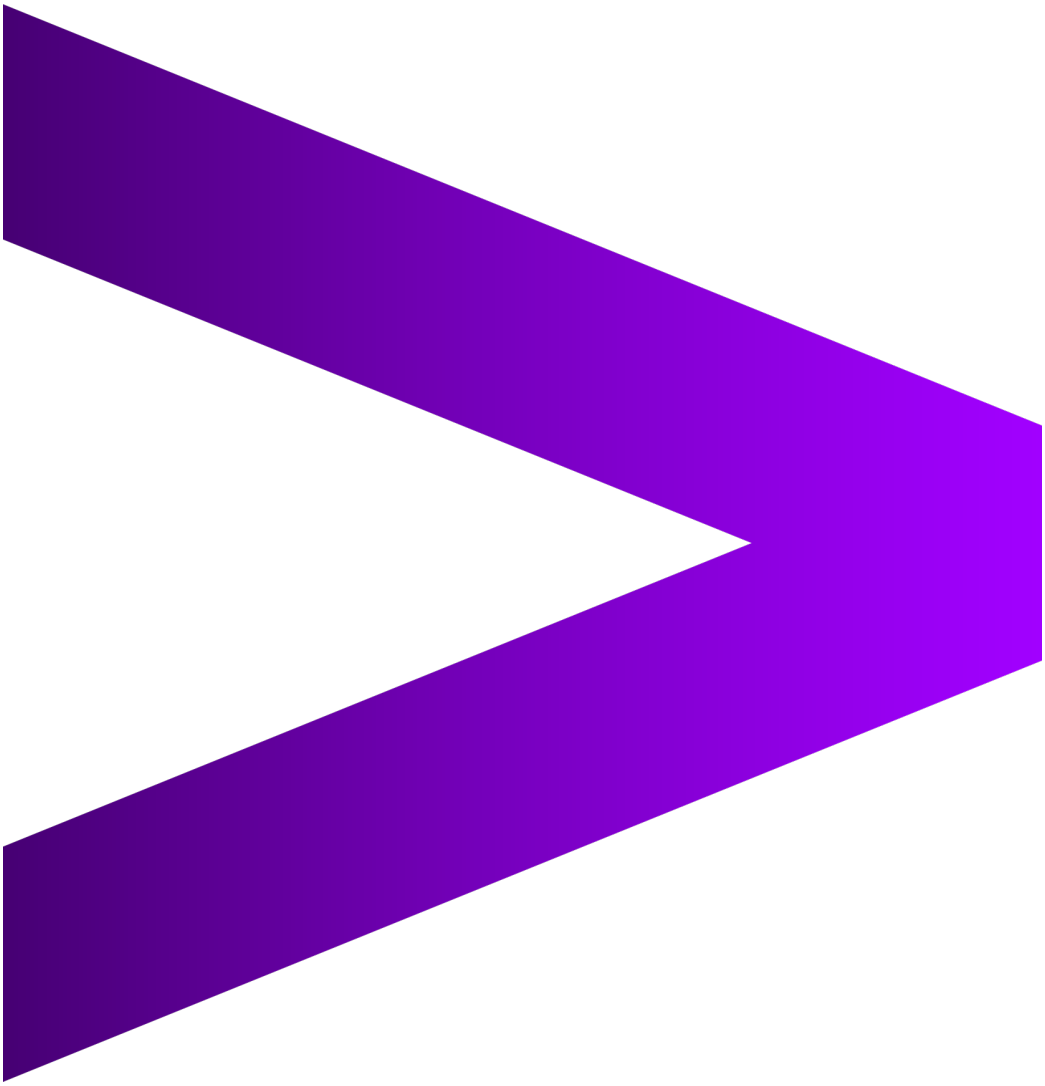
ACTI ADD-ON FOR SPLUNK

ACCENTURE CYBER THREAT INTELLIGENCE



Accenture Security

Table of Contents

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

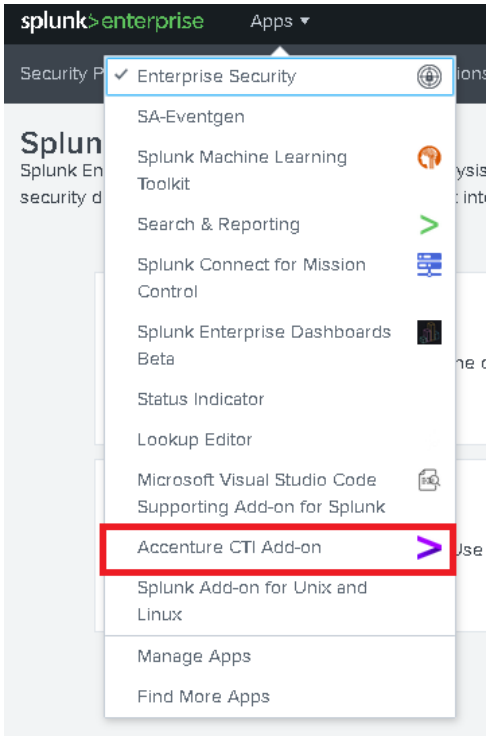
Current Add On Version	Supported Version of Splunk Enterprise
3.0.0	8.1, 8.0, 7.3
3.1.0	8.1, 8.0, 7.3

- 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.

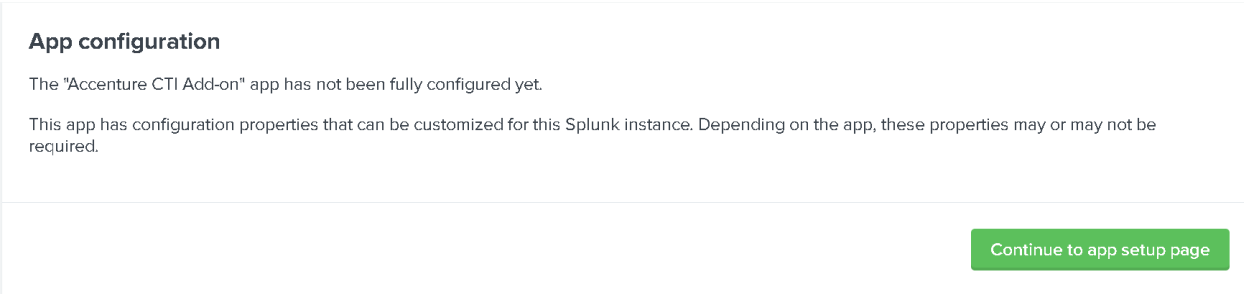
Installation and Configuration

Installation

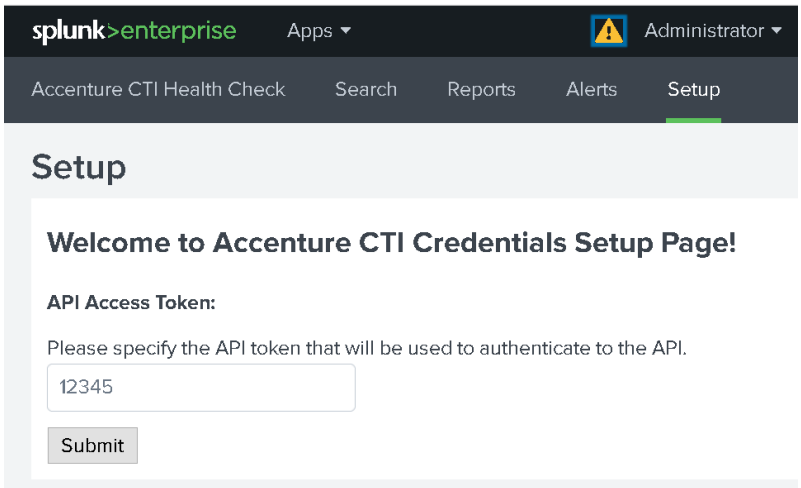
- Generate API token from IG portal at the user profile page. The token must have at least the "iGraph Read API Threat Indicator" role.
- Install the add-on from Splunkbase into the Splunk Search Head containing Splunk ES.
- Once installed, click on the "Apps" drop-down menu, then on the iDefense Intelgraph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



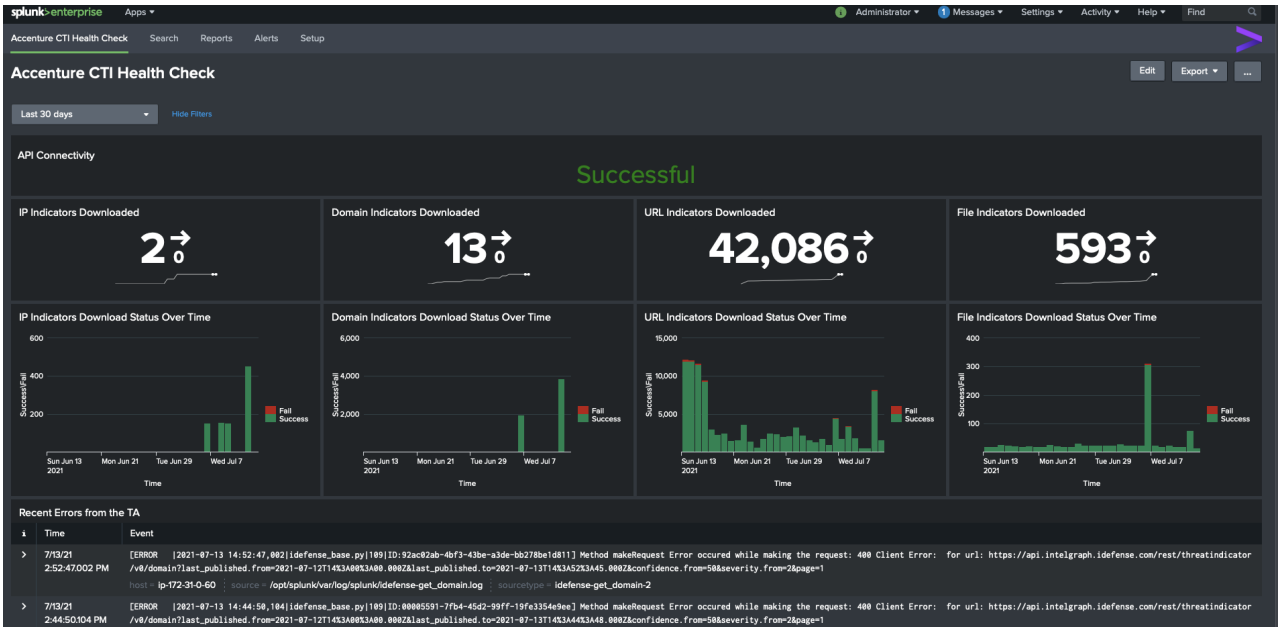
- Then click on Continue to App Setup Page.



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



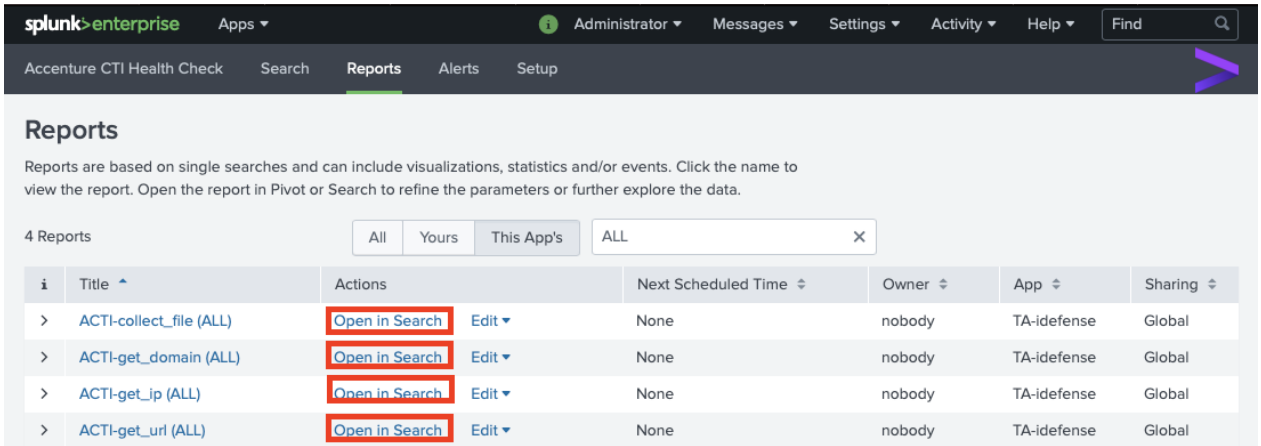
- Clicking on the app should now present the Health Check Dashboard. Connectivity to the API server should show as successful in the Health Check Dashboard.



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:

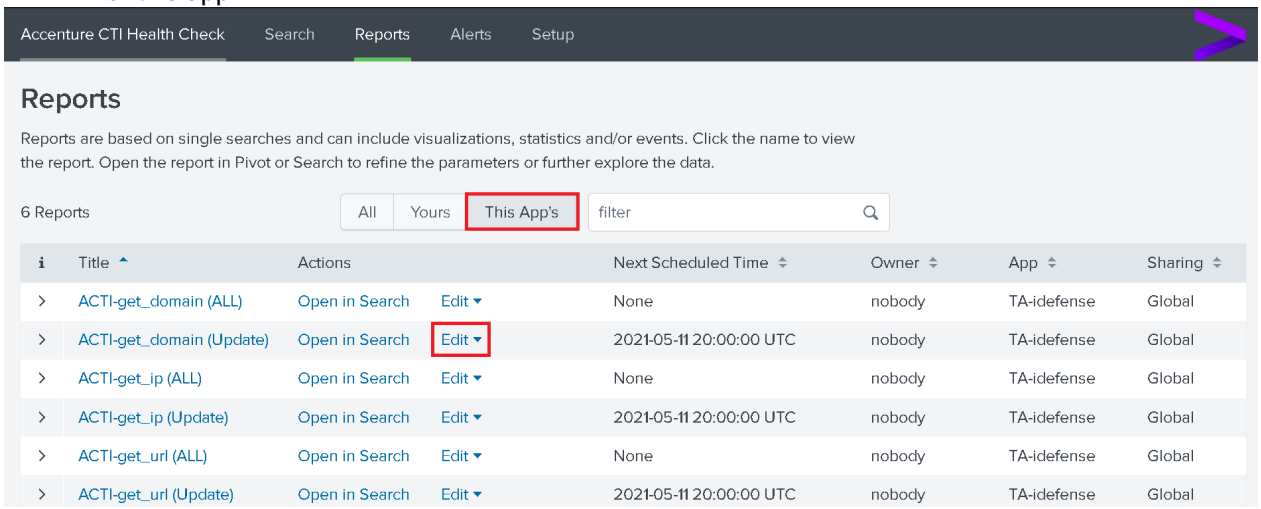
1. ACTI-get_url (ALL)
2. ACTI-get_ip (ALL)
3. ACTI-get_domain (ALL)
4. ACTI-collect_file(ALL)



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.

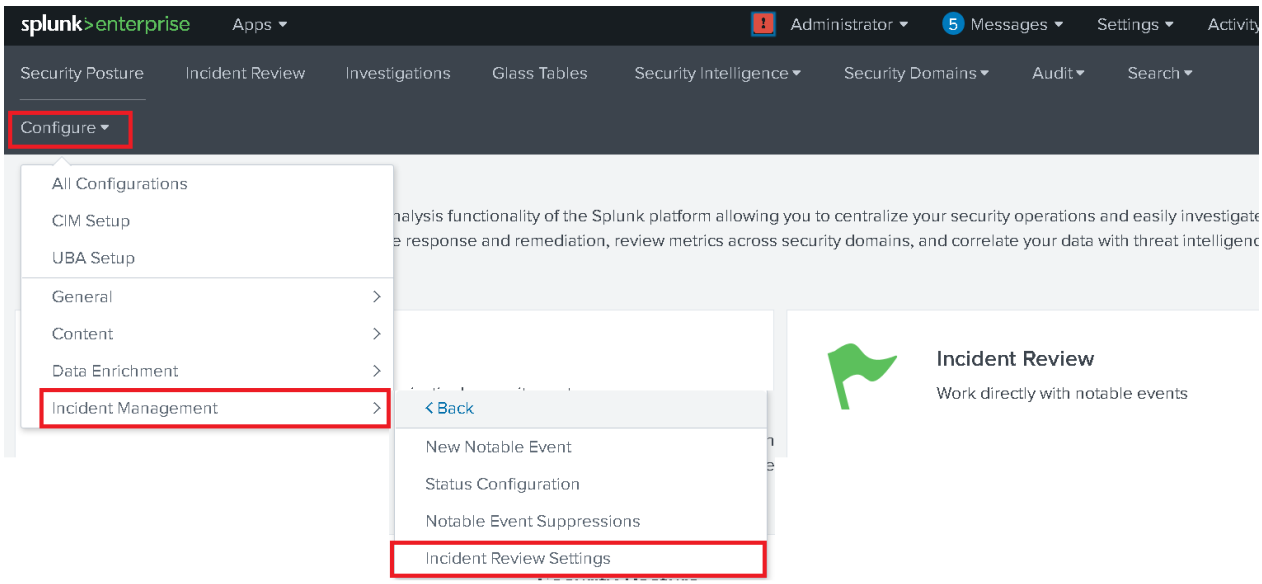


- Click on Edit > Edit Schedule for the Intel type that you wish to update the download frequency. Then change the CRON schedule as necessary.

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	Edit | Remove
category	Category	Edit | Remove
change_type	Change Type	Edit | Remove
channel	Channel	Edit | Remove
command	Command	Edit | Remove
cpu_load_percent	CPU Load (%)	Edit | Remove
creator	Creator	Edit | Remove

+ 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

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

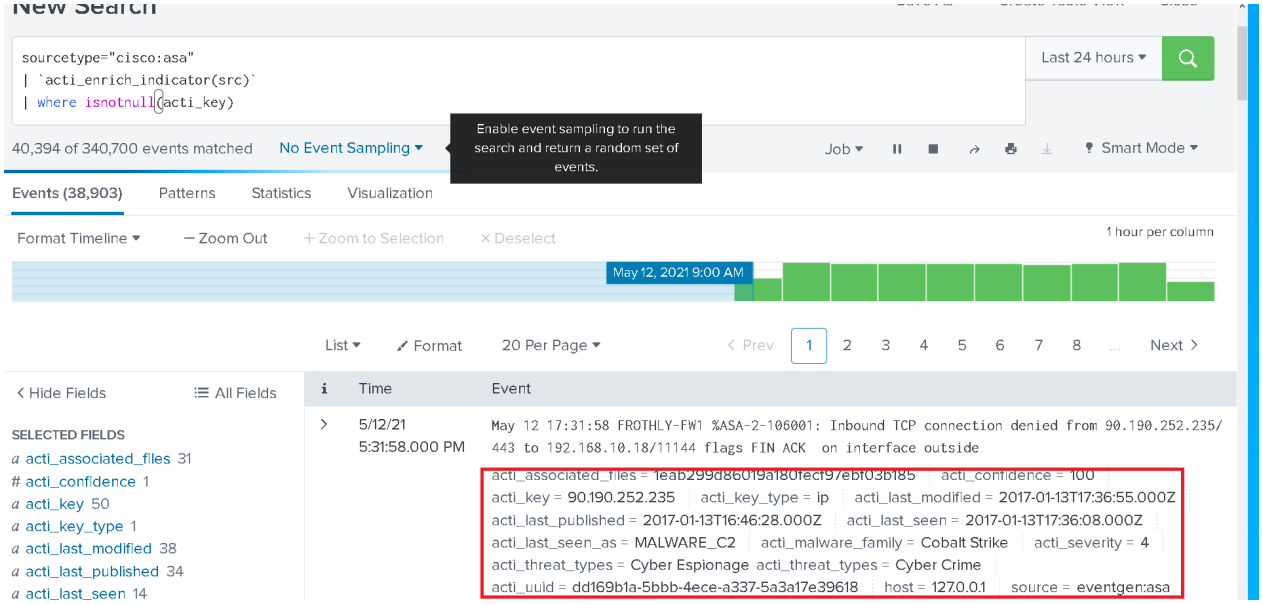
Check this link for more information on the Splunk's threat intel framework.

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:

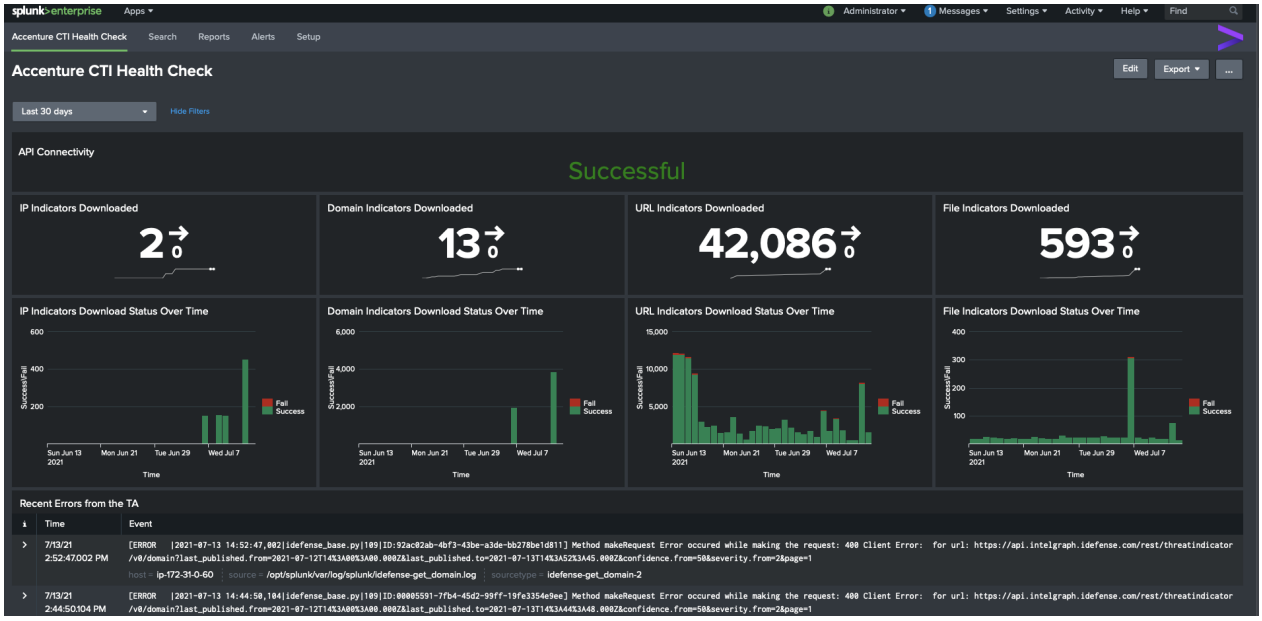


Accenture CTI Integration Health Check Dashboard

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:

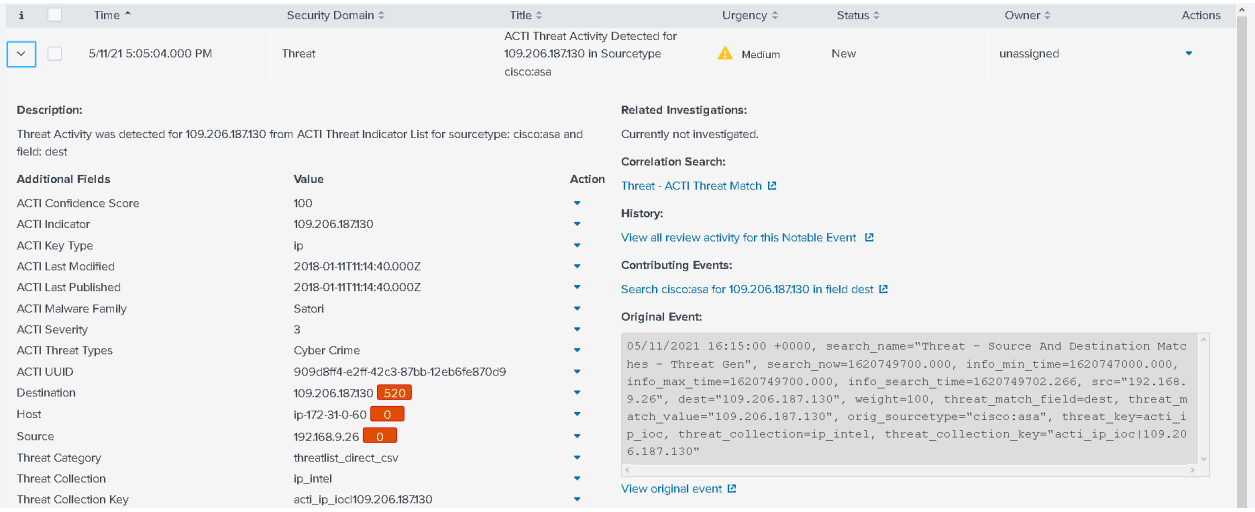
- API Connectivity: Shows the Connectivity Status to the ACTI API endpoints.
- IP, Domain, URL Indicators Download: Shows the number of indicators downloaded over the given time range.
- IP, Domain, URL Indicator Download Status: Shows each time the TA tried to pull indicators from ACTI and whether those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

The Health Check Dashboard appears as follows:

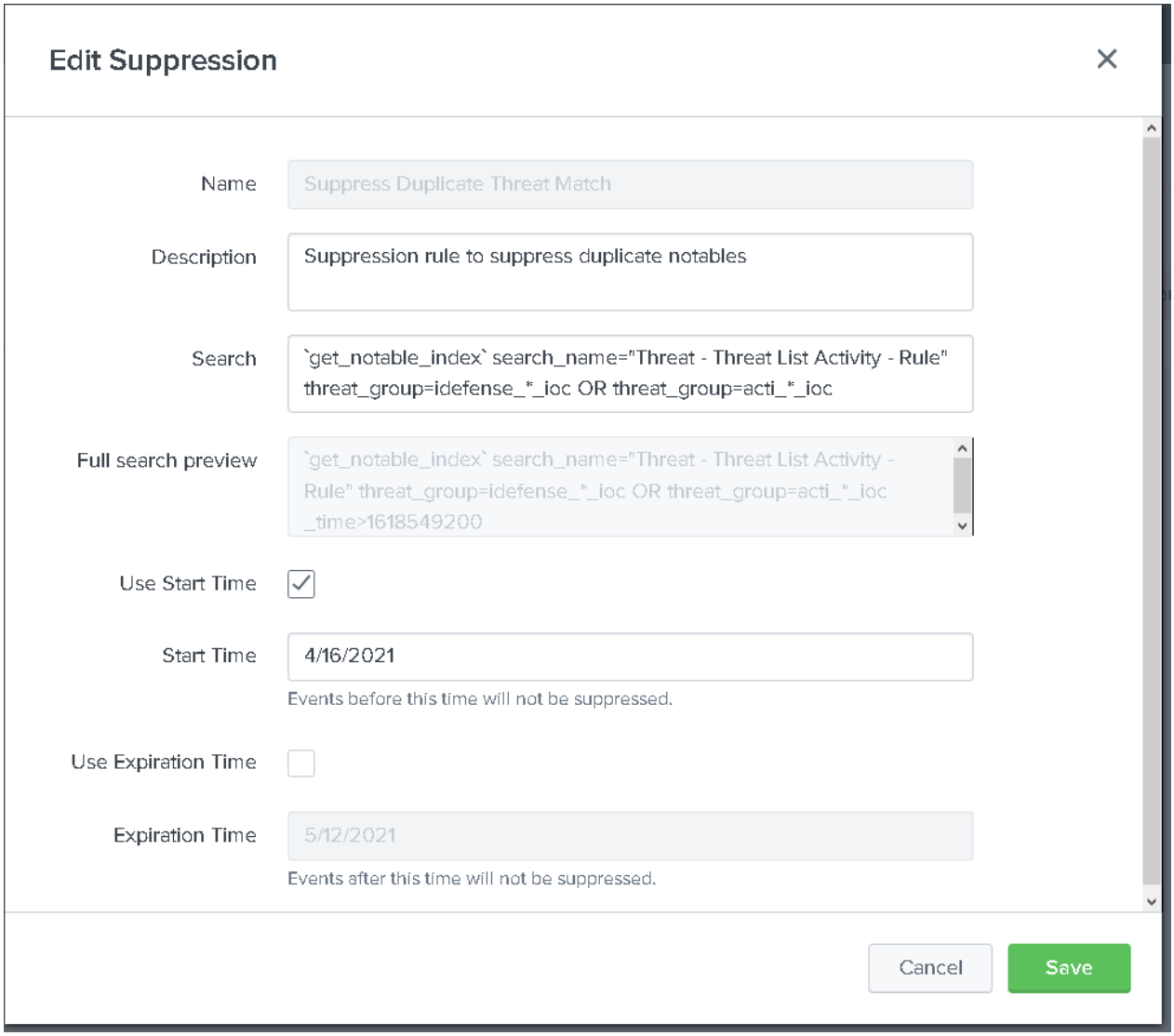


Correlation Search/Alert: iDefense Threat Match

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:



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:



Troubleshooting

Where to find the Logs for this Add-On

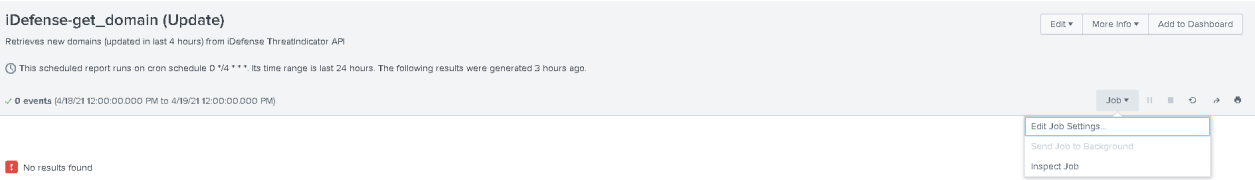
This add-on logs to the following locations:

- $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

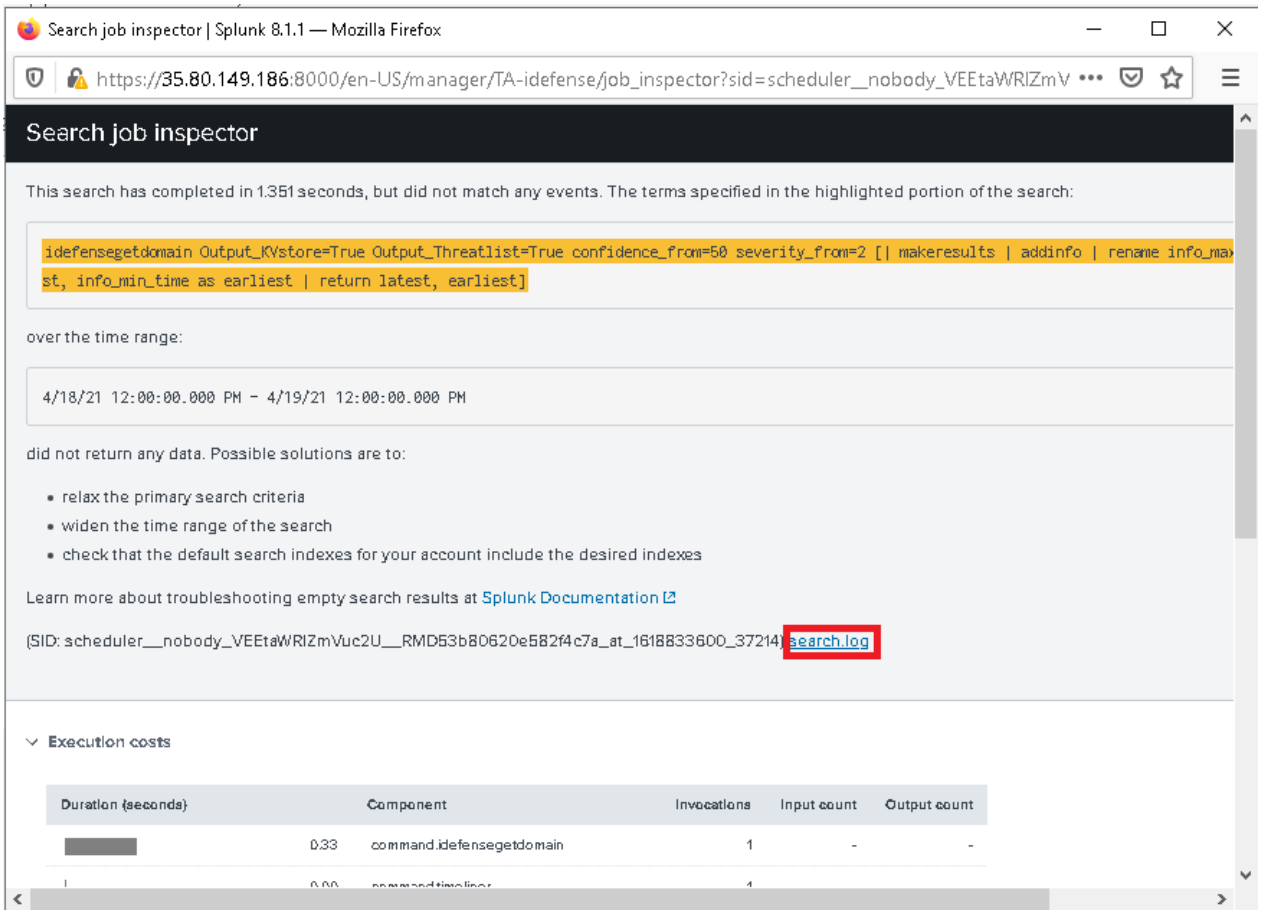
The logs for each run of a TI pull can also be viewed in the Search Head UI, by viewing the search log. To view this log for a TI download that was run recently, follow the steps below:

- 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.



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



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.