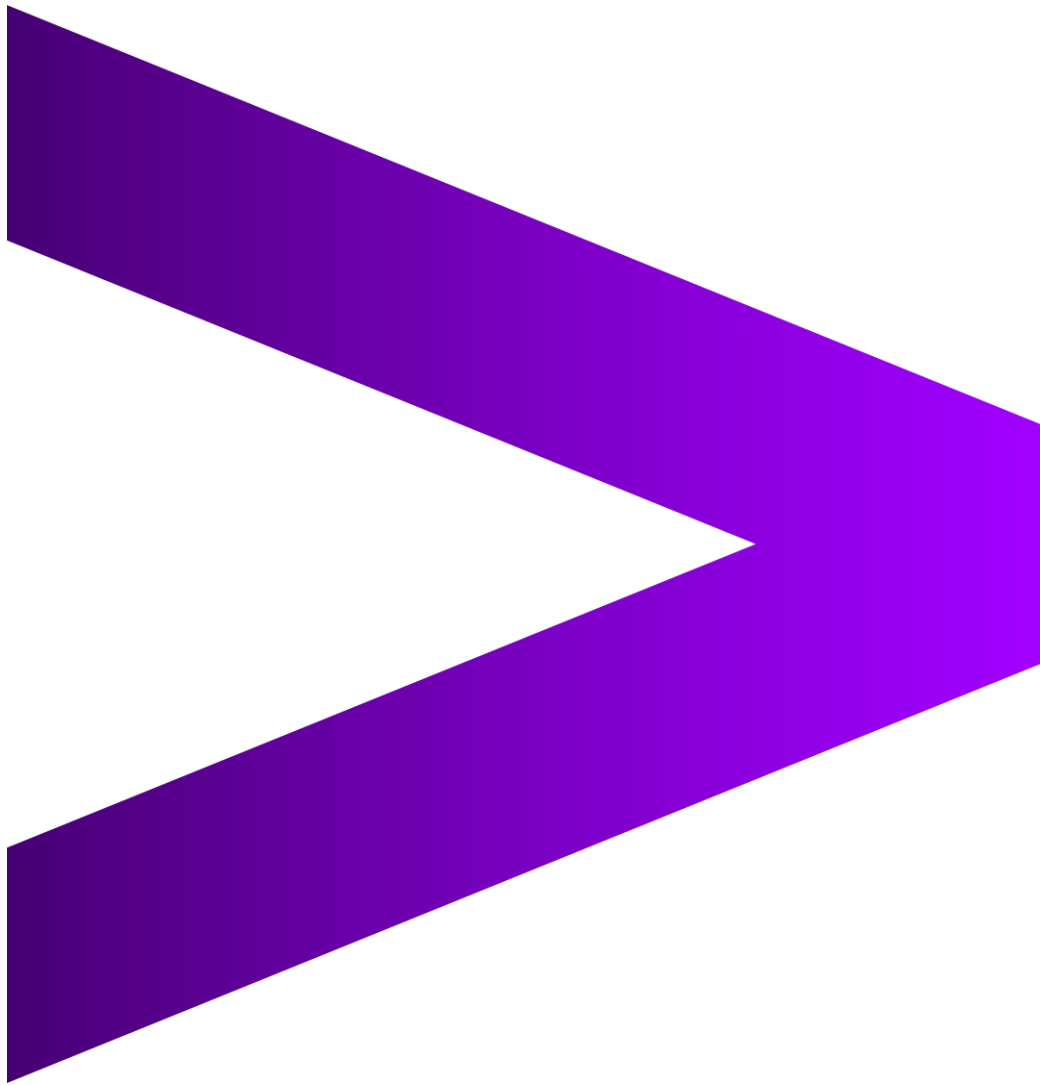


**IDEFENSE INTELGRAPH**  
**ADD-ON FOR SPLUNK**  
**ACCENTURE CYBER THREAT**  
**INTELLIGENCE**



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

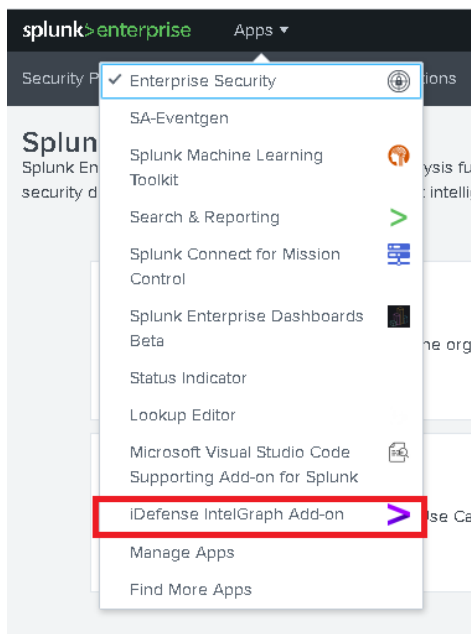
Current Add On Version	Supported Version of Splunk Enterprise
2.3.0	<a href="#">8.1</a> , <a href="#">8.0</a> , <a href="#">7.3</a>

- The add-on must be installed on the Search Head.
- Splunk 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 "iDefense IntelGraph 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

Accenture Cyber Threat Intelligence Integration Health Check
Search
Datasets

## Setup\_iDefenseTA

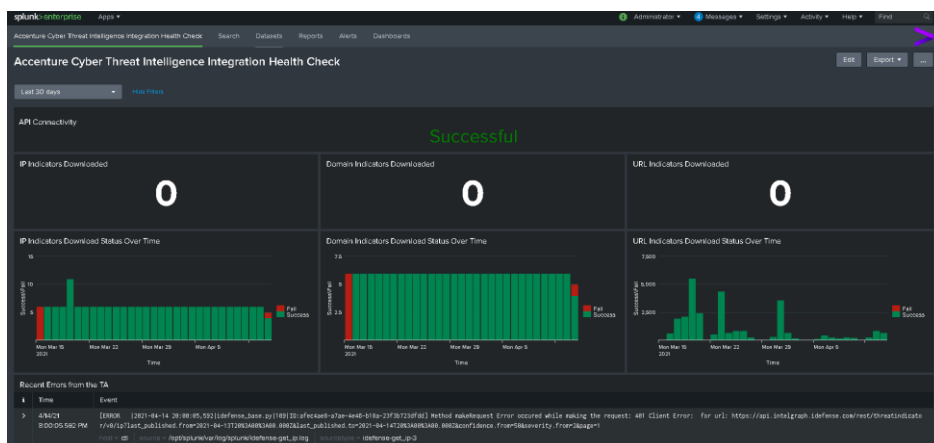
### Welcome to iDefense Credentials Setup Page!

**API Access Token:**

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



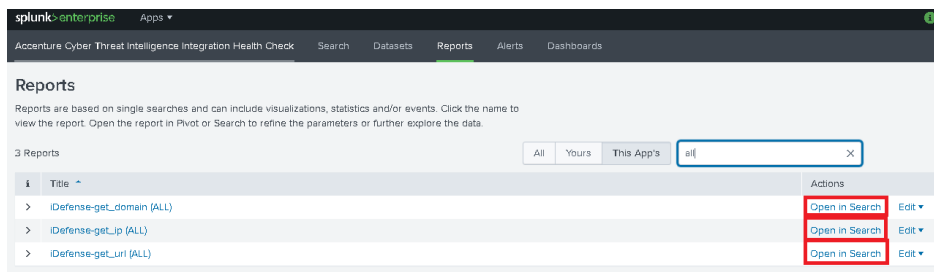
- Clicking on the app should now present the Health Check Dashboard. Connectivity to the API server should show as successful in the Health Check Dashboard.



## 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:

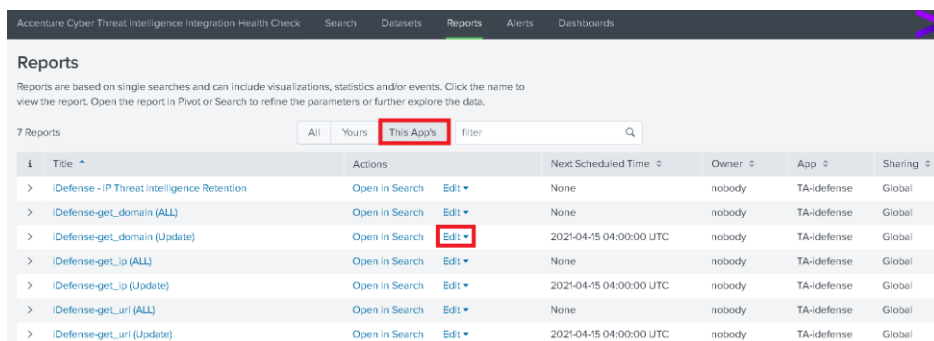
- iDefense-get\_domain (ALL)
- iDefense-get\_url (ALL)
- iDefense-get\_ip (ALL)



## 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.

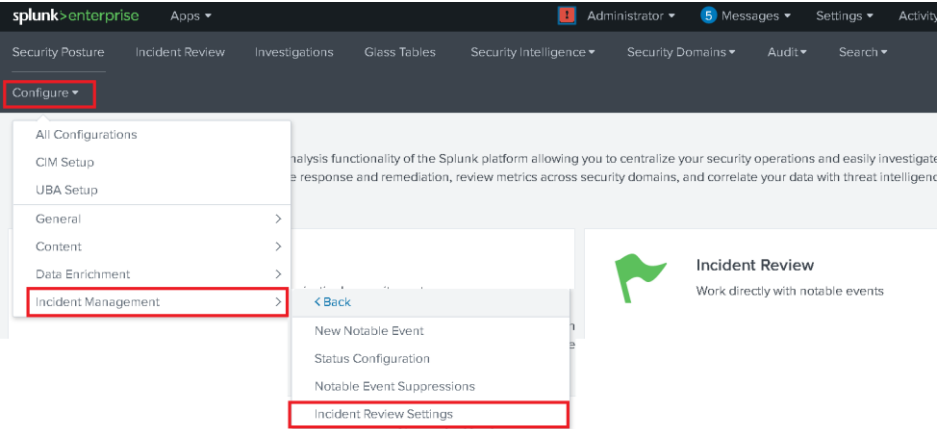


- Click on Edit > Edit Schedule for the Intel type that you wish to update the download frequency. Then change the CRON schedule as necessary.

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
idefense_key_type	ACTI Key Type
idefense_key	ACTI Indicator
idefense_threat_campaigns	ACTI Threat Campaigns Test
idefense_threat_types	ACTI Threat Types
idefense_uuid	ACTI UUID
idefense_severity	ACTI Severity
idefense_malware_family	ACTI Malware Family
idefense_last_seen_as	ACTI Last SeenAs

idefense_associated_files	ACTI Associated Files
idefense_last_seen	ACTI Last Seen
idefense_last_published	ACTI Last Published
idefense_last_modified	ACTI Last Modified
idefense_confidence	ACTI Confidence Score

- 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:

- idefense\_threatindicator\_ip
- idefense\_threatindicator\_domain
- idefense\_threatindicator\_url

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



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 the Splunk's Threat Intelligence Framework. The data gets stored into the following KV stores that are within Splunk ES:

- ip\_intel
- http\_intel

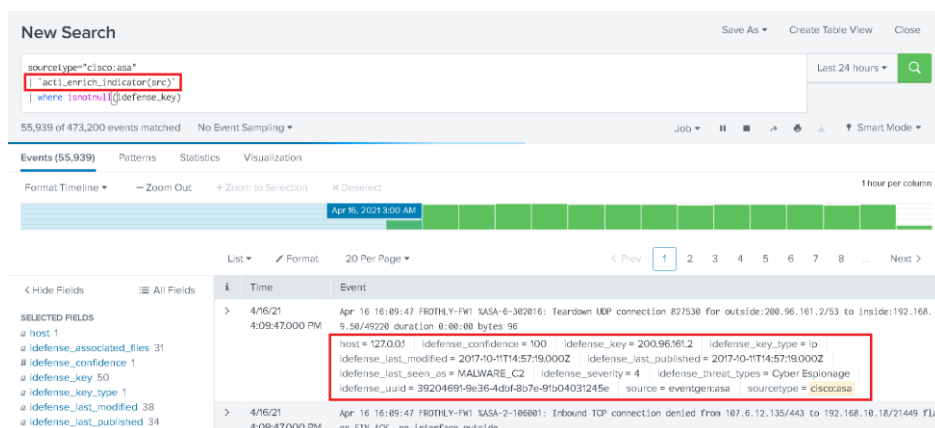
Check this [link](#) for more information on the Splunk's threat intel framework.

## 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\$)

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. The search bar contains the query: `sourcetype="cisco:asa" | acti_enrich_indicator(indicator="192.168.1.1") | where !isnull(iddefense.key)`. The search results show 55,939 events. The table view displays the following data:

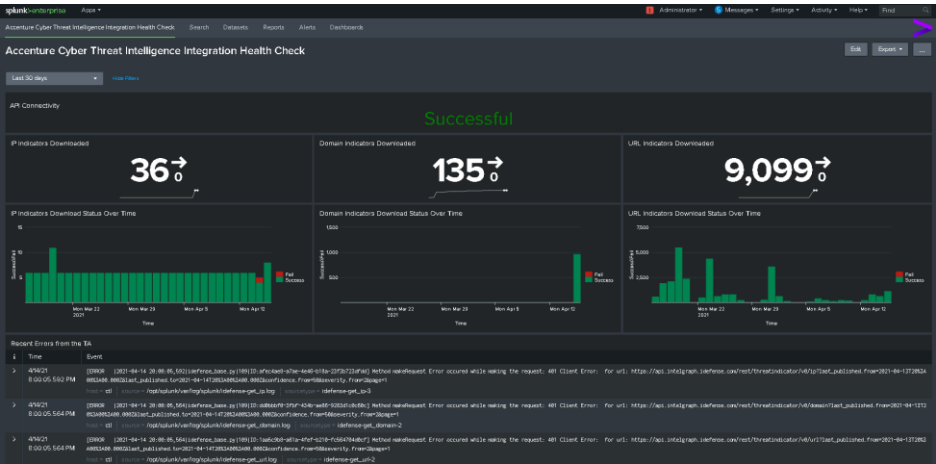
Time	Event
4/16/21 4:09:47.000 PM	Apr 16 16:09:47 PROTHLY-FW1 SASA-6-302016: Teardown UDP connection 827530 for outside:200.96.161.2/53 to inside:192.168.1.1/53 duration 0:00:00 bytes 96
4/16/21 4:09:47.000 PM	host = 127.0.0.1   iddefense_confidence = 100   iddefense_key = 200.96.161.2   iddefense_key_type = ip   iddefense_last_modified = 2017-10-11T14:57:19.000Z   iddefense_last_published = 2017-10-11T14:57:19.000Z   iddefense_last_seen_as = MALWARE_C2   iddefense_severity = 4   iddefense_threat_types = Cyber Espionage   iddefense_uuid = 39204691-9e36-4dbf-8b7e-9fb04031245e   source = eventgenasa   sourcetype = cisco:asa
4/16/21 4:09:47.000 PM	Apr 16 16:09:47 PROTHLY-FW1 SASA-2-106001: Inbound TCP connection denied from 107.6.12.135/443 to 192.168.10.18/21449 flags FIN ACK on interface outside

## 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:

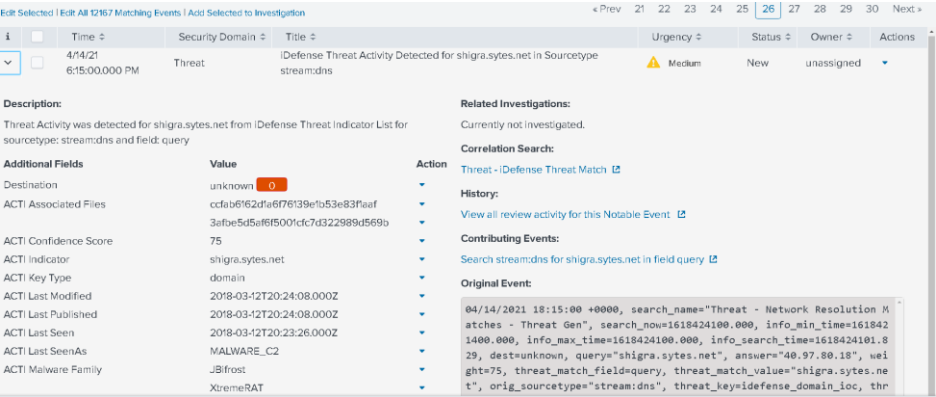
- API Connectivity: Shows the Connectivity Status to the ACTI API endpoints.
- IP, Domain, URL Indicators Download: Shows the number of indicators downloaded over the given time range.
- IP, Domain, URL Indicator Download Status: Shows each time the TA tried to pull indicators from ACTI and whether those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

The 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:

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`

Full search preview

``get_notable_index` search_name="Threat - Threat List Activity - Rule" threat_group=idefense-*_ioc_time>1618549200`

Use Start Time

☒

Start Time

4/16/2021

Events before this time will not be suppressed.

Use Expiration Time

☐

Expiration Time

4/16/2021

Events after this time will not be suppressed.

Cancel

Save

## Troubleshooting

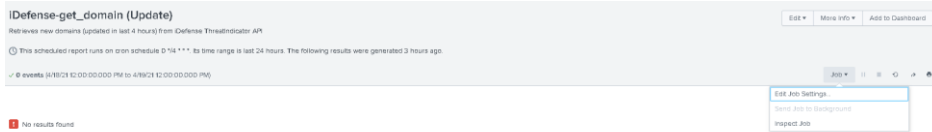
### Where to find the Logs for this Add-On

This add-on logs to the following locations:

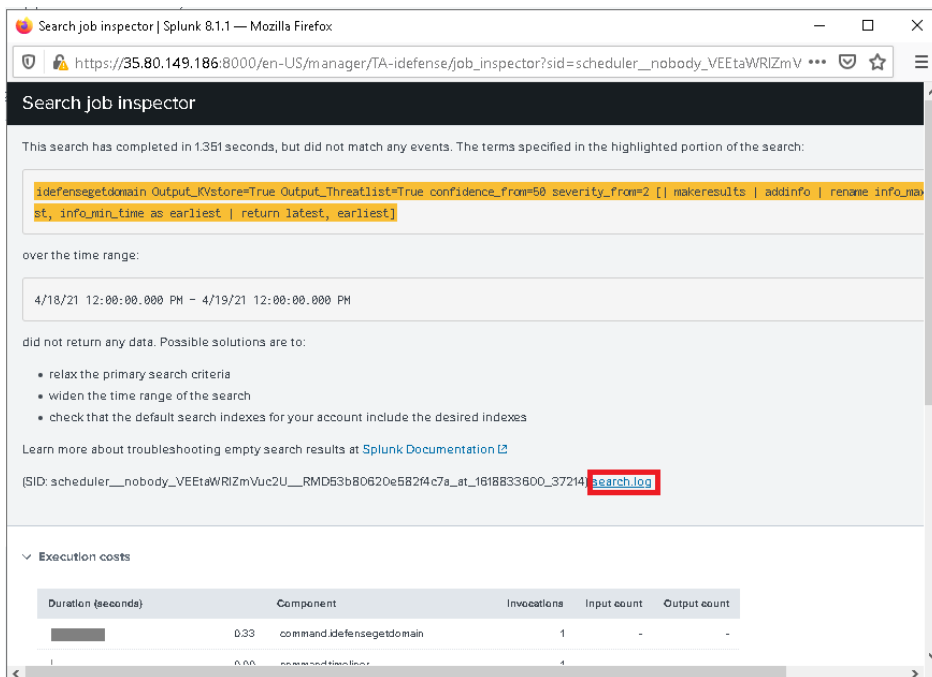
- \$SPLUNK\_HOME/var/log/idefense-get\_ip.log
- \$SPLUNK\_HOME/var/log/idefense-get\_domain.log
- \$SPLUNK\_HOME/var/log/idefense-get\_url.log
- \$SPLUNK\_HOME/var/log/idefense-validate.log

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 iDefense 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 iDefense Threat Match Correlation Search.