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 6

Change Intelligence Download Frequency 6

Adding Accenture CTI Notable Review Fields to Splunk ES 7

Configure Threat Intelligence Retention 8

Contents **9**

Threat Intelligence KV Store 9

Macros for Data Enrichment 10

Accenture CTI Integration Health Check Dashboard 11

Correlation Search/Alert: iDefense Threat Match 12

Troubleshooting **13**

Where to find the Logs for this Add-On 13

Changing Log Level 14

Health Check Dashboard 15

Splunk Mission Control **15**

Getting the add-on ready for Splunk Mission Control 15

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

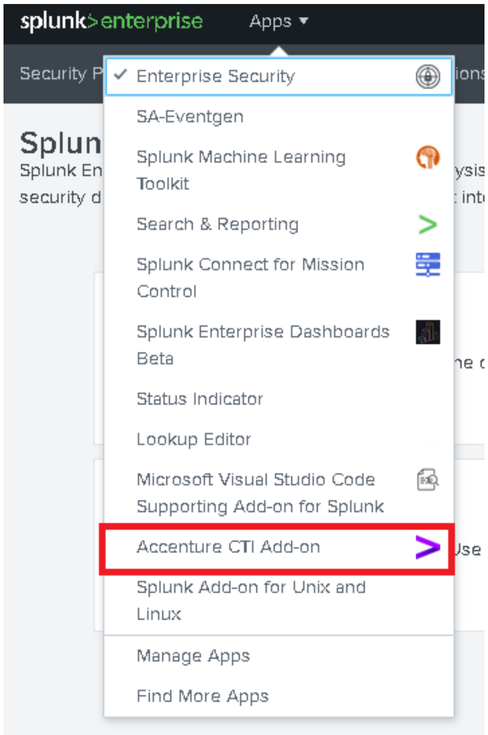
Current Add On Version	**Supported Version of Splunk Enterprise**
3.0.0	8.1, 8.0, 7.3
3.1.0	8.2, 8.1, 8.0
3.2.0	8.2, 8.1, 8.0

- 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.

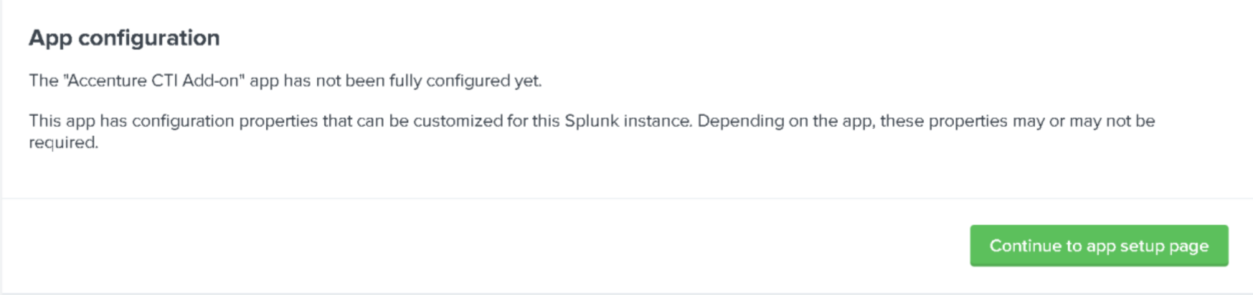
Installation and Configuration

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.


splunk>enterprise
Apps
Security P
Enterprise Security
SA-Eventgen
Splunk Machine Learning Toolkit
Search & Reporting
Splunk Connect for Mission Control
Splunk Enterprise Dashboards Beta
Status Indicator
Lookup Editor
Microsoft Visual Studio Code Supporting Add-on for Splunk
Accenture CTI Add-on
Splunk Add-on for Unix and Linux
Manage Apps
Find More Apps

- Then click on Continue to App Setup Page.

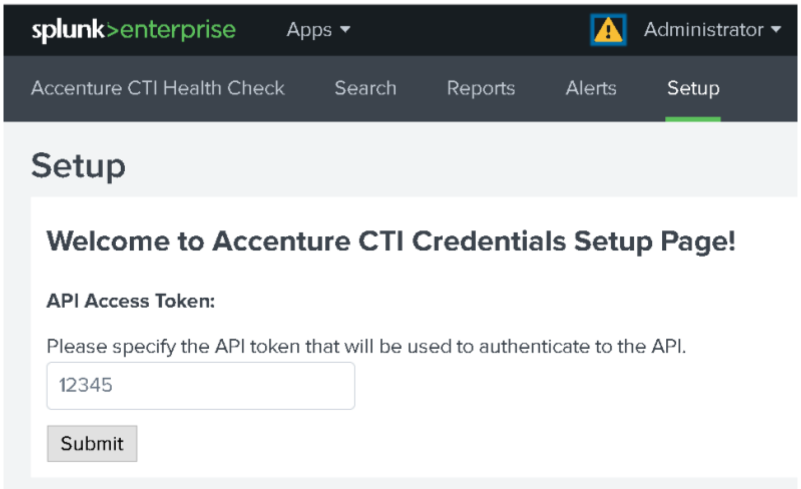


App configuration

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.

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



Setup

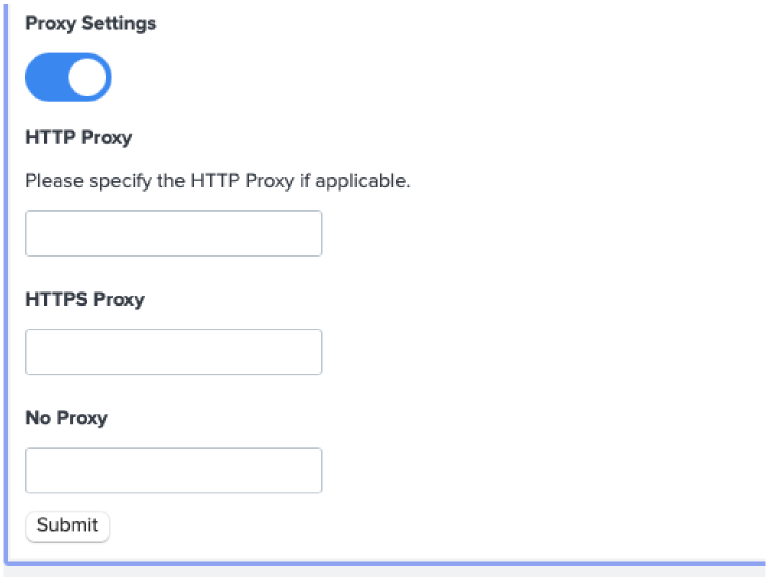
Welcome to Accenture CTI Credentials Setup Page!

API Access Token:

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

12345

- If you need to configure proxy, provide the proxy parameters in the same page:



Proxy Settings

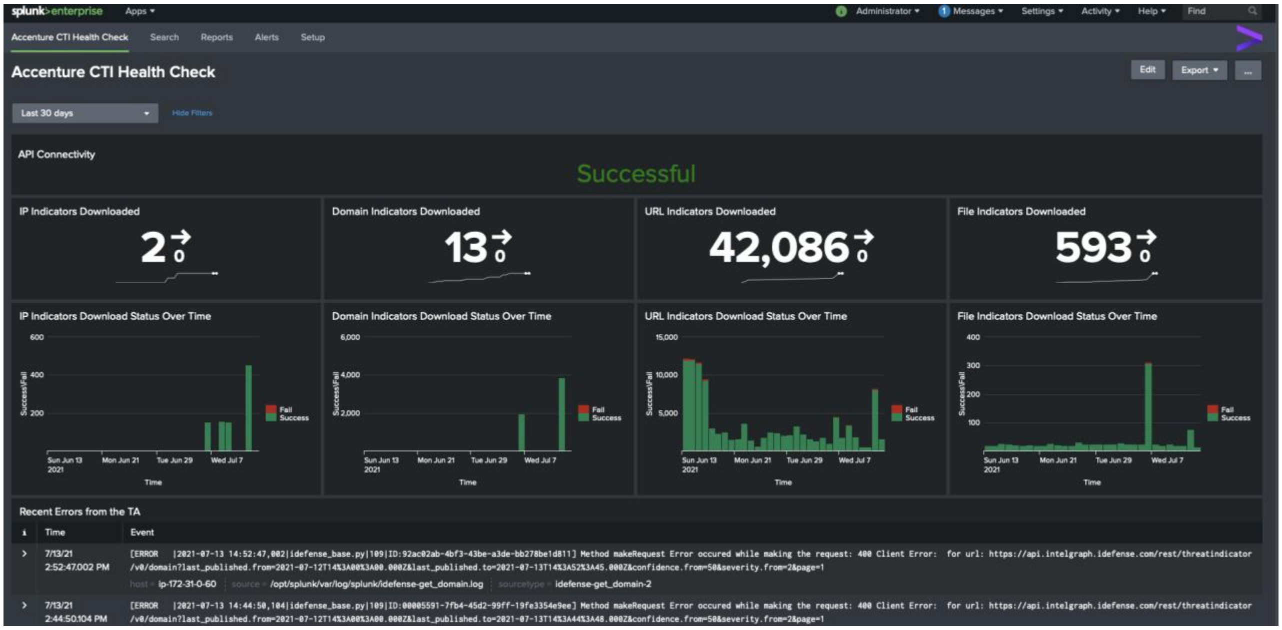
HTTP Proxy

Please specify the HTTP Proxy if applicable.

HTTPS Proxy

No Proxy

- 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.



Accenture CTI Health Check

API Connectivity

Successful

IP Indicators Downloaded	Domain Indicators Downloaded	URL Indicators Downloaded	File Indicators Downloaded
2 → 0	13 → 0	42,086 → 0	593 → 0

IP Indicators Download Status Over Time

Domain Indicators Download Status Over Time

URL Indicators Download Status Over Time

File Indicators Download Status Over Time

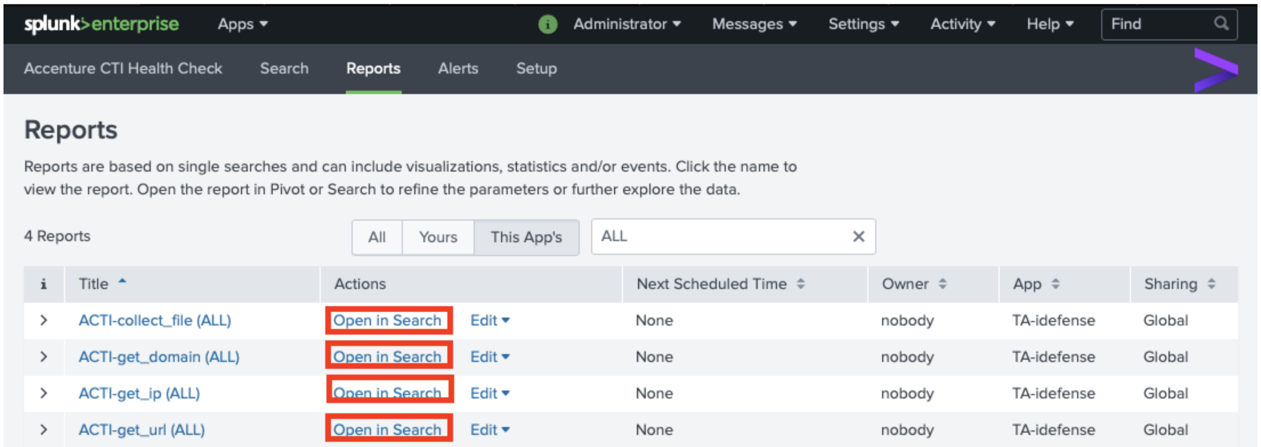
Recent Errors from the TA

```
i  Time          Event
>  7/13/21       [ERROR   |2021-07-13 14:52:47,002|idefense_base.py|109|ID:92ac02ab-4bf3-43be-a3de-bb278be1d811] Method makeRequest Error occured while making the request: 400 Client Error:  for url: https://api.intelgraph.idefense.com/rest/threatindicator
   2:52:47.002 PM /v0/domain?last_published.from=2021-07-12T14%3A00%3A00.000Z&last_published.to=2021-07-13T14%3A52%3A45.000Z&confidence.from=50&severity.from=2&page=1
                 host = ip-172-31-0-60 | source = /opt/splunk/var/log/splunk/idefense-get_domain.log | sourcetype = idefense-get_domain-2
>  7/13/21       [ERROR   |2021-07-13 14:44:50,104|idefense_base.py|109|ID:00005591-7fb4-45d2-99ff-19fe3354e9ee] Method makeRequest Error occured while making the request: 400 Client Error:  for url: https://api.intelgraph.idefense.com/rest/threatindicator
   2:44:50.104 PM /v0/domain?last_published.from=2021-07-12T14%3A00%3A00.000Z&last_published.to=2021-07-13T14%3A44%3A48.000Z&confidence.from=50&severity.from=2&page=1
```

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)



Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

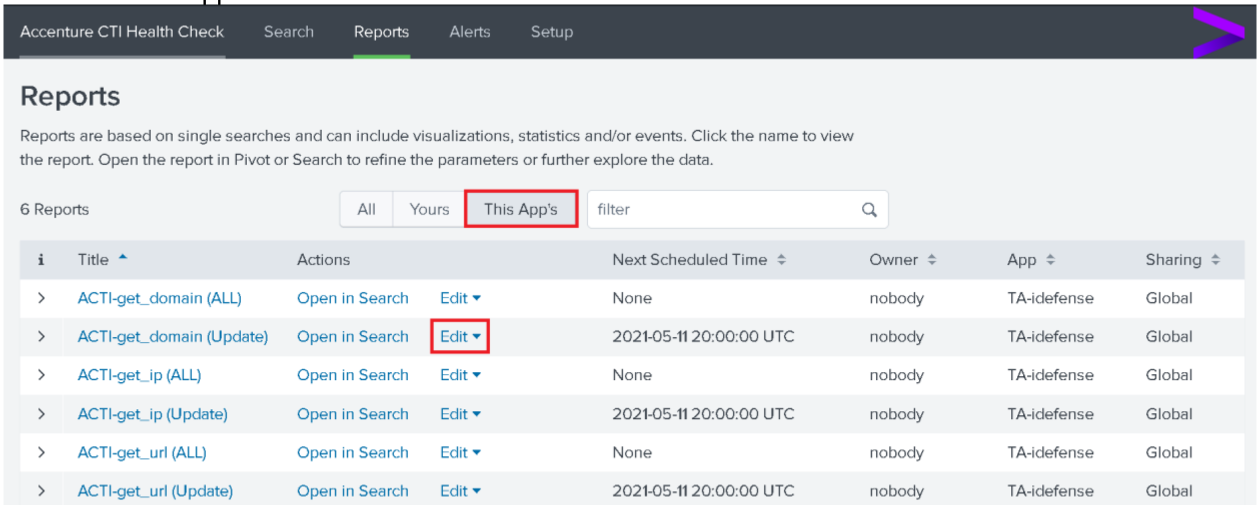
4 Reports

i	Title ▴	Actions		Next Scheduled Time ⇕	Owner ⇕	App ⇕	Sharing ⇕
>	ACTI-collect_file (ALL)	Open in Search	Edit ▾	None	nobody	TA-idefense	Global
>	ACTI-get_domain (ALL)	Open in Search	Edit ▾	None	nobody	TA-idefense	Global
>	ACTI-get_ip (ALL)	Open in Search	Edit ▾	None	nobody	TA-idefense	Global
>	ACTI-get_url (ALL)	Open in Search	Edit ▾	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.



Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

6 Reports

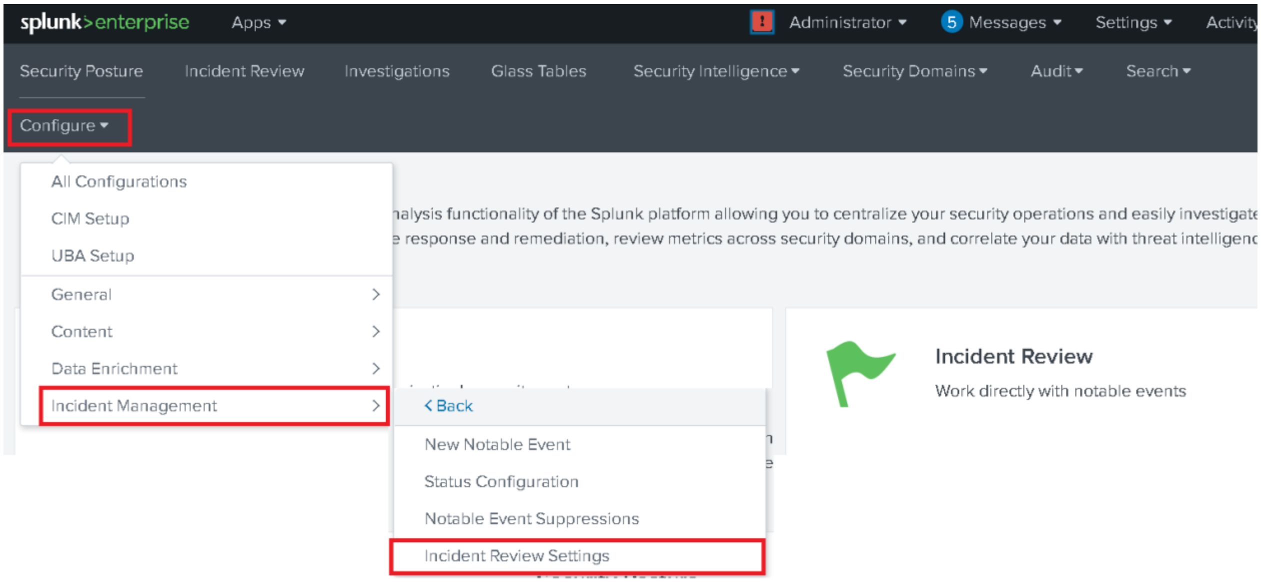
i	Title ▴	Actions		Next Scheduled Time ⇕	Owner ⇕	App ⇕	Sharing ⇕
>	ACTI-get_domain (ALL)	Open in Search	Edit ▾	None	nobody	TA-idefense	Global
>	ACTI-get_domain (Update)	Open in Search	Edit ▾	2021-05-11 20:00:00 UTC	nobody	TA-idefense	Global
>	ACTI-get_ip (ALL)	Open in Search	Edit ▾	None	nobody	TA-idefense	Global
>	ACTI-get_ip (Update)	Open in Search	Edit ▾	2021-05-11 20:00:00 UTC	nobody	TA-idefense	Global
>	ACTI-get_url (ALL)	Open in Search	Edit ▾	None	nobody	TA-idefense	Global
>	ACTI-get_url (Update)	Open in Search	Edit ▾	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.



nalysis functionality of the Splunk platform allowing you to centralize your security operations and easily investigate
e response and remediation, review metrics across security domains, and correlate your data with threat intelligenc

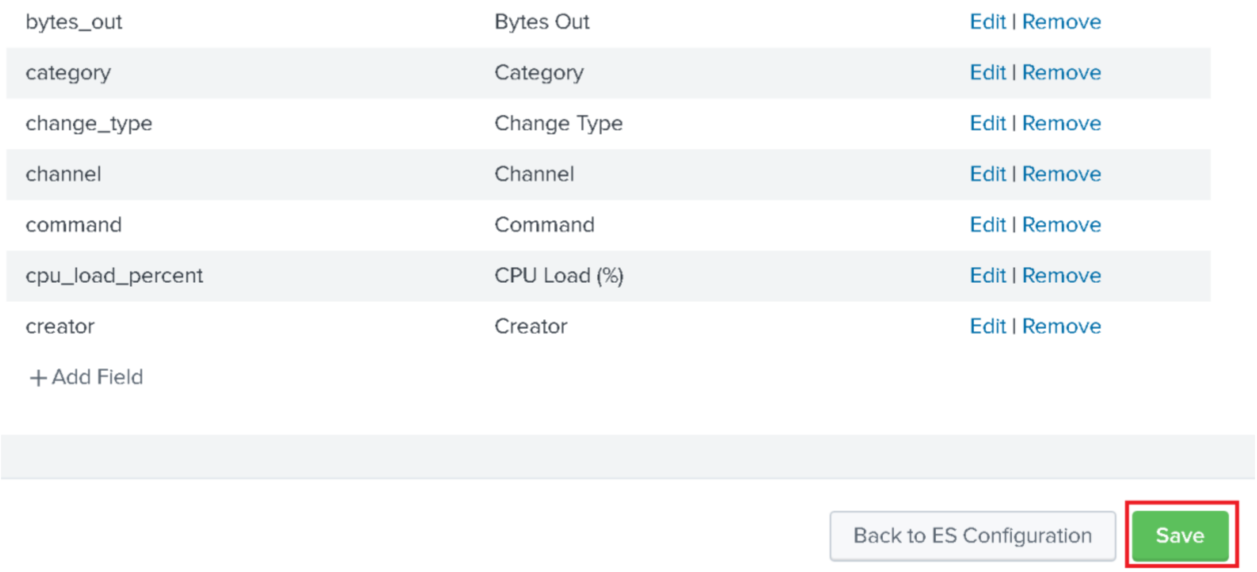
Incident Review

Work directly with notable events

- 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

Configure Threat Intelligence Retention

There are two sets of threat intelligence retention management. One is used manage alerting from IOCs that are older than defined threshold, and the other is used to remove IOCs from the system, after a certain time has passed.

Retention Management for Threat Match Alerts

The IOCs are removed from the Splunk Threat Intelligence KV store, to avoid alerts from old IOCs that are no longer relevant. Following aging criteria is used to remove the IOCs.

- Cyber Espionage: 2 years
- IOCs associated with Threat Groups: 120 Days
- IOCs associated with Threat Campaigns: 120 Days
- Default: 60 Days

Following queries run once a day, to enforce aging criteria:

- ACTI_File_Splunk_TI_Retention
- ACTI_IP-Domain_Splunk_TI_Retention
- ACTI_URL_Splunk_TI_Retention

The aging criteria explained above can be modified, if desired with following lookups:

- acti_ti_retention

Retention Management for ACTI IOCs

The IOCs are removed from the ACTI KV stores and Splunk system completely, after they have aged 5 years from the last_published date. Following saved search, that runs every day, purges older IOCs:

- ACTI_Internal_Retention

The aging criteria for retention can also be configured by modifying the search above.

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
- acti_threatindicator_file

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

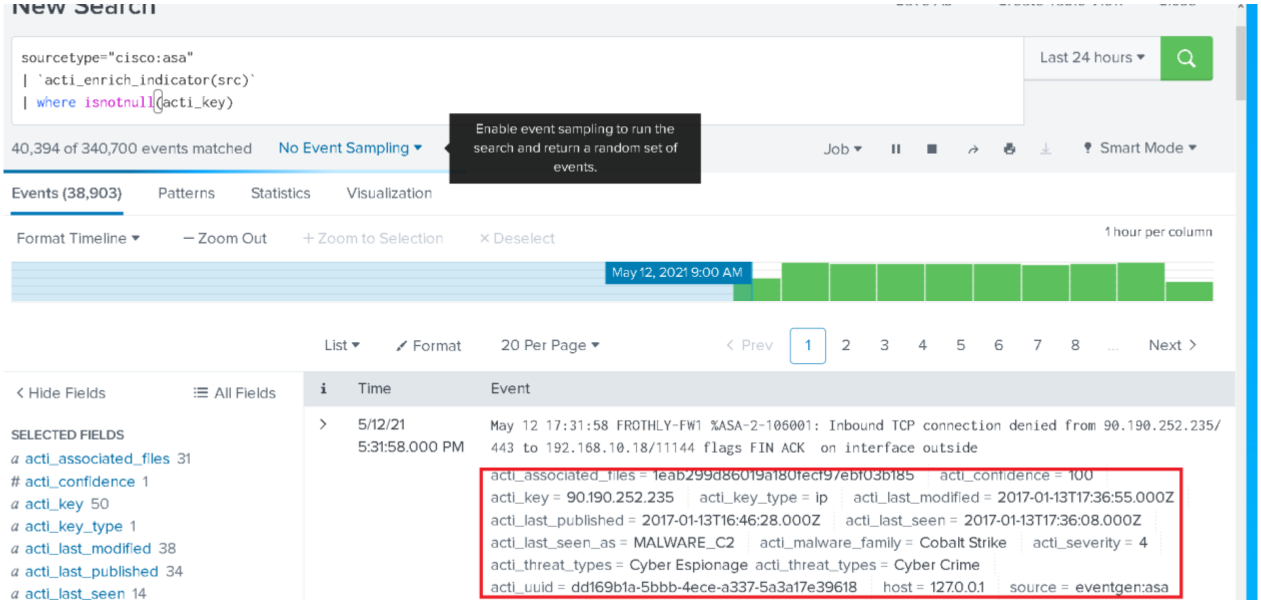
Check this link for more information on the Splunk's threat intel framework.

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:



```
sourcetype="cisco:asa"
| `acti_enrich_indicator(src)`
| where isnotnull(acti_key)
```

40,394 of 340,700 events matched

No Event Sampling

SELECTED FIELDS
a acti_associated_files 31
# acti_confidence 1
a acti_key 50
a acti_key_type 1
a acti_last_modified 38
a acti_last_published 34
a acti_last_seen 14

5/12/21
5:31:58.000 PM

```
May 12 17:31:58 FROTHLY-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
```

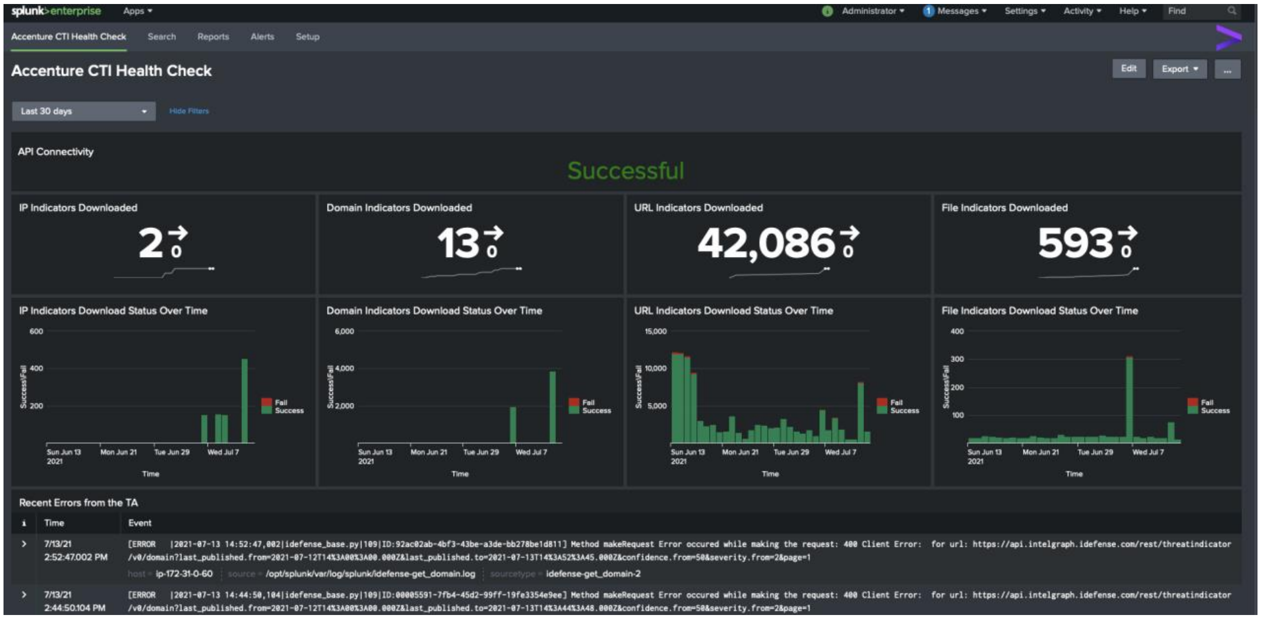
acti_associated_files = 1eab299d86019a180fecf97ebf03b185 acti_confidence = 100
acti_key = 90.190.252.235 acti_key_type = ip acti_last_modified = 2017-01-13T17:36:55.000Z
acti_last_published = 2017-01-13T16:46:28.000Z acti_last_seen = 2017-01-13T17:36:08.000Z
acti_last_seen_as = MALWARE_C2 acti_malware_family = Cobalt Strike acti_severity = 4
acti_threat_types = Cyber Espionage acti_threat_types = Cyber Crime
acti_uuid = dd169b1a-5bbb-4ece-a337-5a3a17e39618 host = 127.0.0.1 source = eventgen:asa

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:



7/13/21
2:52:47.002 PM

```
[ERROR  |2021-07-13 14:52:47,002|idefense_base.py|109|ID:92ac02ab-4bf3-43be-a3de-bb278be1d811] Method makeRequest Error occured while making the request: 400 Client Error:  for url: https://api.intelgraph.idefense.com/rest/threatindicator
/v0/domain?last_published.from=2021-07-12T14%3A00%3A00.000Z&last_published.to=2021-07-13T14%3A52%3A45.000Z&confidence.from=50&severity.from=2&page=1
```

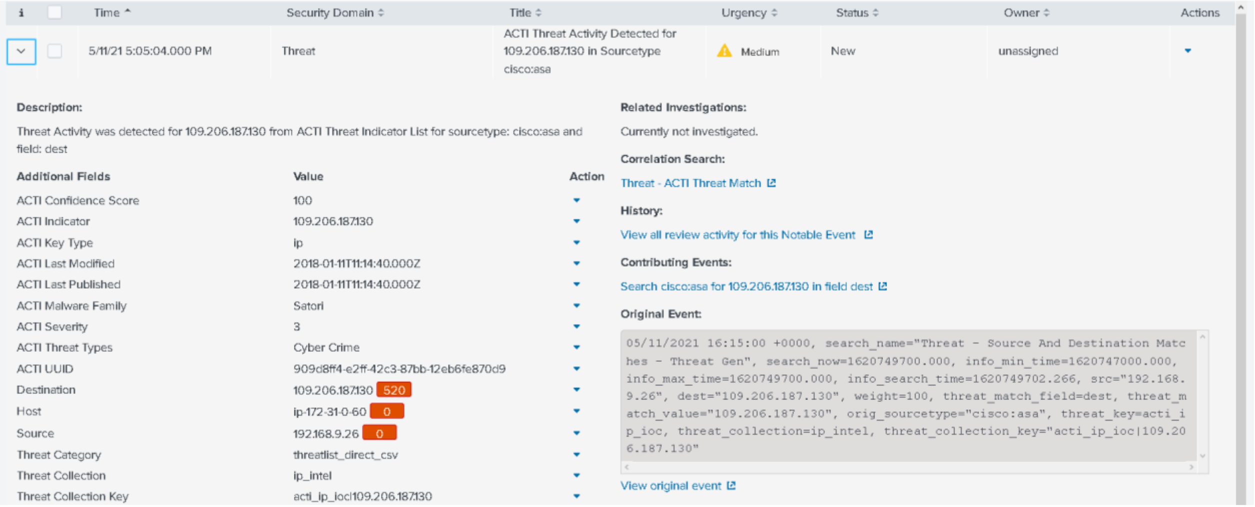
host = ip-172-31-0-60 source = /opt/splunk/var/log/splunk/idefense-get_domain.log sourcetype = idefense-get_domain-2

7/13/21
2:44:50.104 PM

```
[ERROR  |2021-07-13 14:44:50,104|idefense_base.py|109|ID:00005591-7fb4-45d2-99ff-19fe3354e9ee] Method makeRequest Error occured while making the request: 400 Client Error:  for url: https://api.intelgraph.idefense.com/rest/threatindicator
/v0/domain?last_published.from=2021-07-12T14%3A00%3A00.000Z&last_published.to=2021-07-13T14%3A44%3A48.000Z&confidence.from=50&severity.from=2&page=1
```

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
	□	5/11/21 5:05:04.000 PM	Threat	ACTI Threat Activity Detected for 109.206.187130 in Sourcetype cisco:asa	⚠ Medium	New	unassigned	

Description:

Threat Activity was detected for 109.206.187130 from ACTI Threat Indicator List for sourcetype: cisco:asa and field: dest

Additional Fields	Value	Action
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	909d8ff4-e2ff-42c3-87bb-12eb6fe870d9	
Destination	109.206.187130 520	
Host	ip-172-31-0-60 0	
Source	192168.9.26 0	
Threat Category	threatlist_direct_csv	
Threat Collection	ip_intel	
Threat Collection Key	acti_ip_iocl109.206.187130	

Related Investigations:

Currently not investigated.

Correlation Search:

Threat - ACTI Threat Match

History:

View all review activity for this Notable Event

Contributing Events:

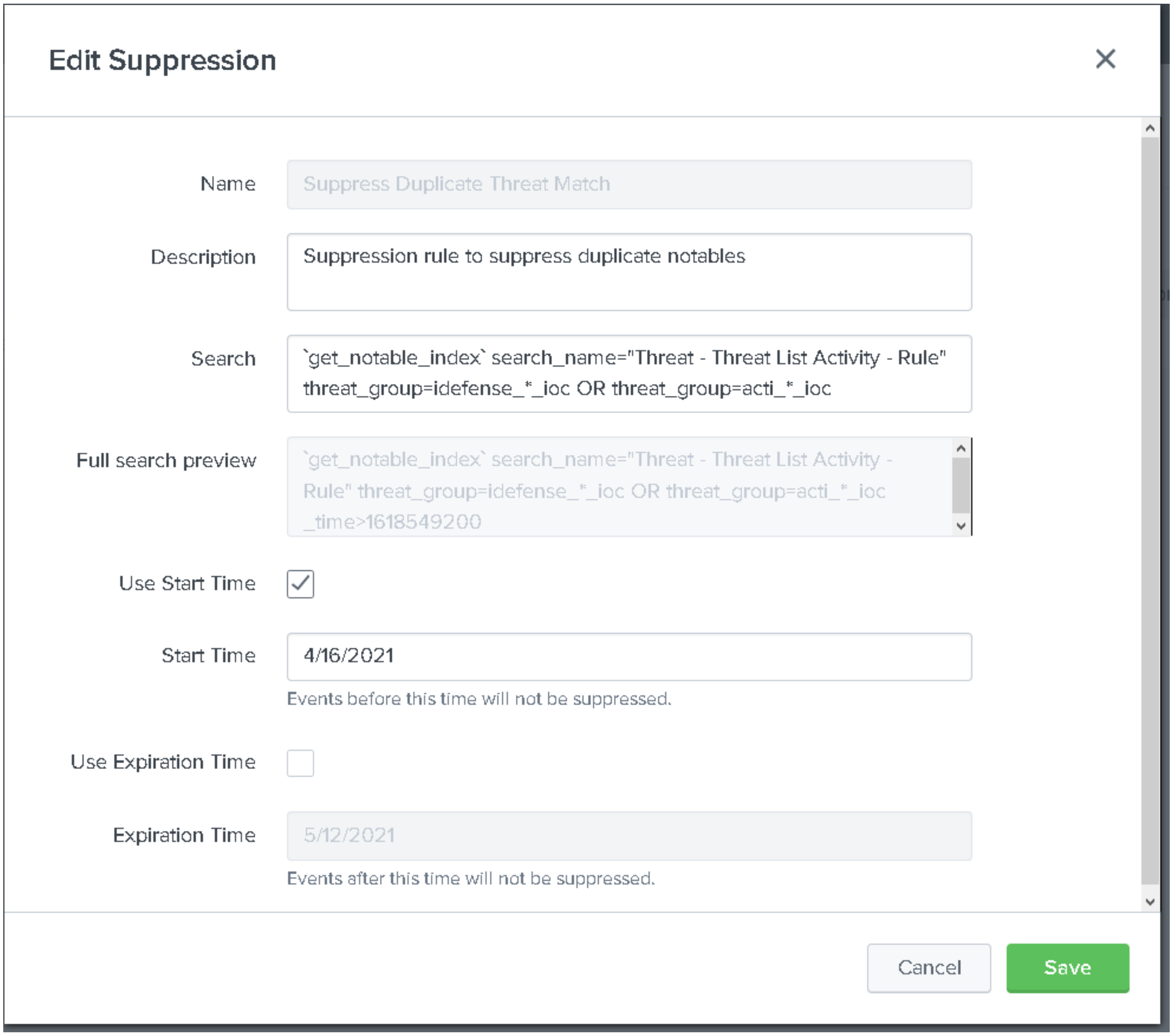
Search cisco:asa for 109.206.187130 in field dest

Original Event:

```
05/11/2021 16:15:00 +0000, search_name="Threat - Source And Destination Matc
hes - 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_m
atch_value="109.206.187.130", orig_sourcetype="cisco:asa", threat_key=acti_i
p_ioc, threat_collection=ip_intel, threat_collection_key="acti_ip_ioc|109.20
6.187.130"
```

View original event

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.

Troubleshooting

Where to find the Logs for this Add-On

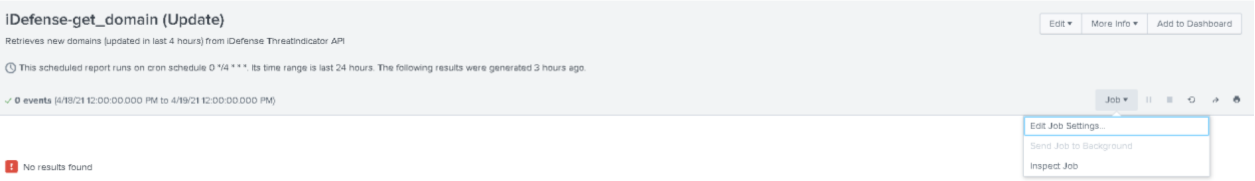
This add-on logs to the following locations:

- $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)

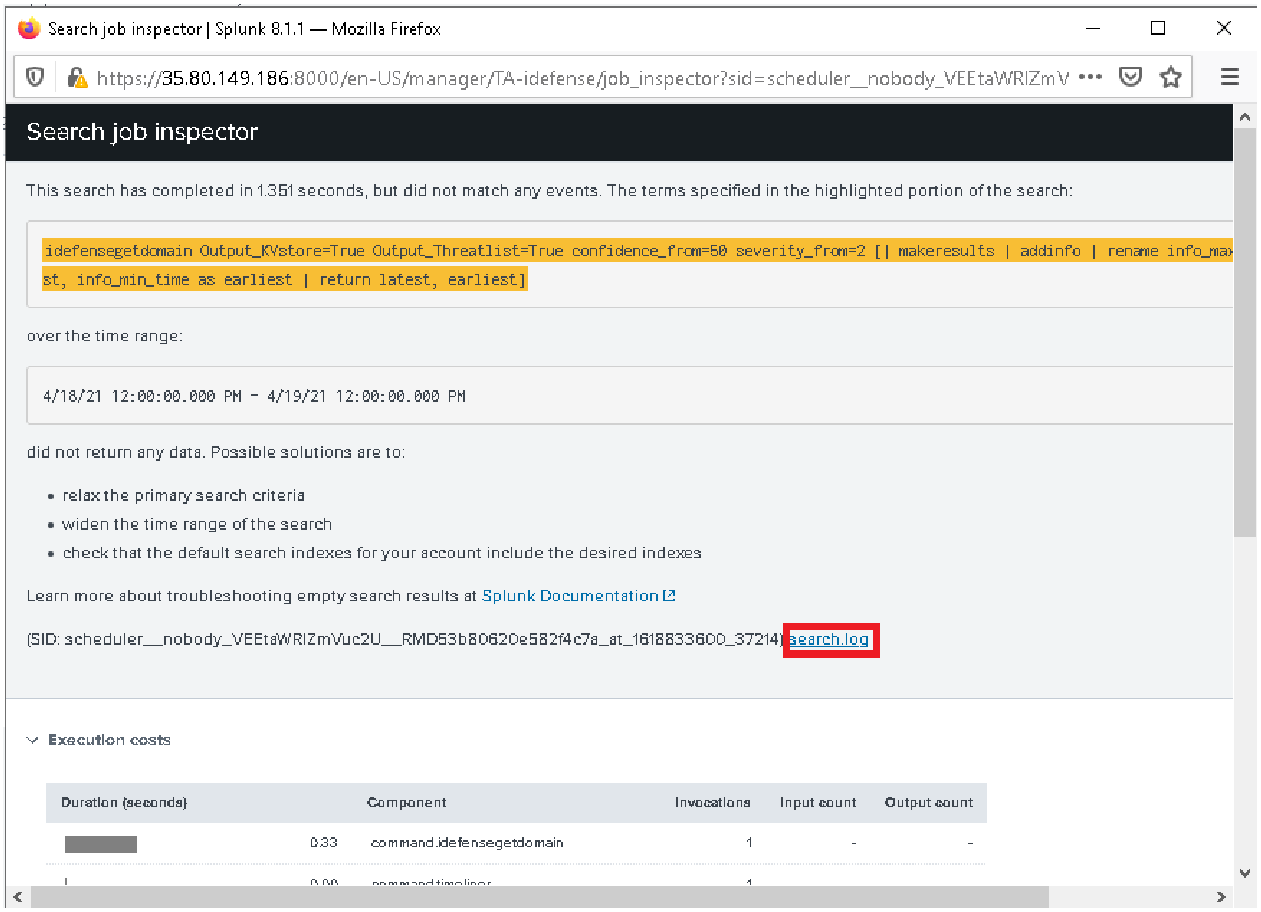
Retrieves new domains (updated in last 4 hours) from iDefense ThreatIndicator API

This scheduled report runs on cron schedule 0 */4 * * *. 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)

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.



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_max
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.timeliner	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.