IDEFENSE INTELGRAPH 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

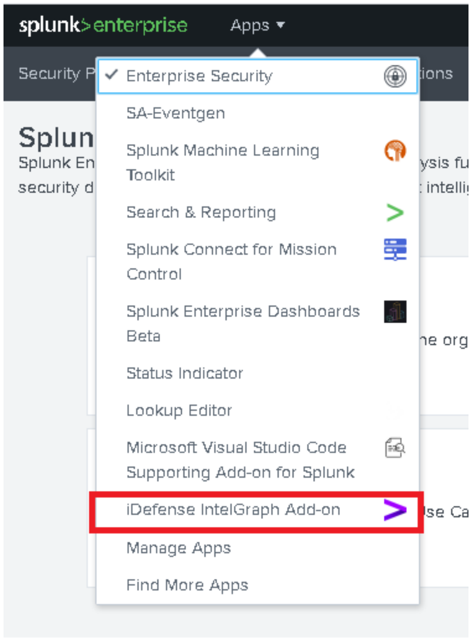
Current Add On Version	Supported Version of Splunk Enterprise
3.0	8.1, 8.0, 7.3

- 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.

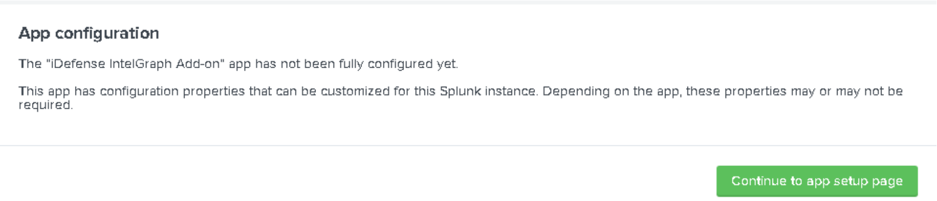
Installation and Configuration

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.**

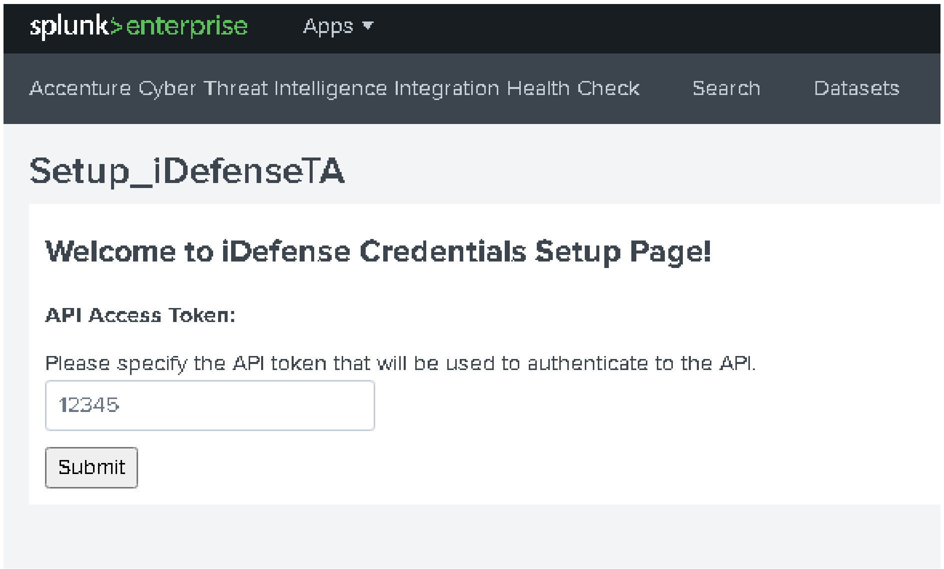


App configuration

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.

- 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

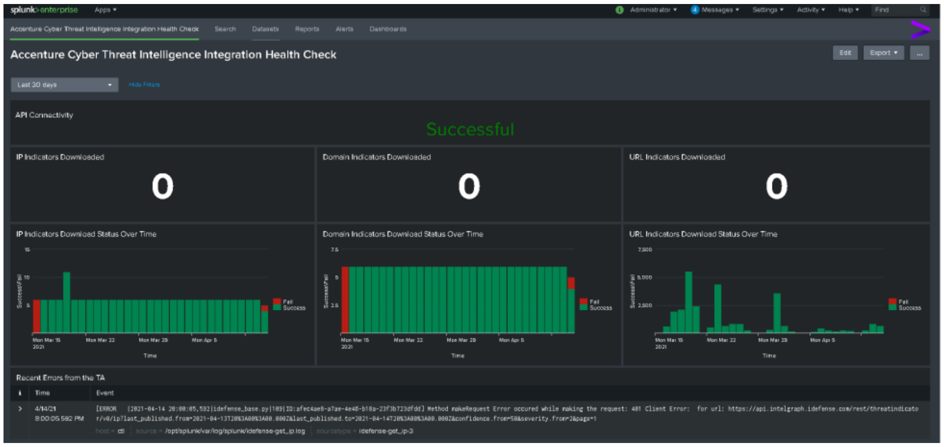
Welcome to iDefense Credentials Setup Page!

API Access Token:

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

12345

- 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 Cyber Threat Intelligence Integration Health Check

API Connectivity: Successful

IP Indicators Downloaded	Domain Indicators Downloaded	URL Indicators Downloaded
0	0	0

IP Indicators Download Status Over Time
Domain Indicators Download Status Over Time
URL Indicators Download Status Over Time
Success/Fail
Fail
Success
Mon Mar 15 2021
Mon Mar 22
Mon Mar 29
Mon Apr 5
Time
10
5
2.5
5,000
2,500
7,500

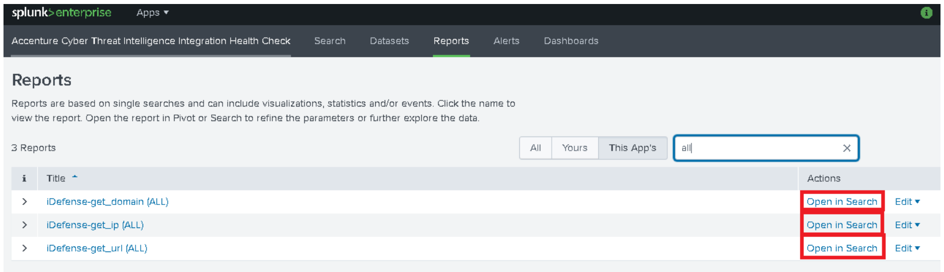
Recent Errors from the TA

```
i  Time          Event
>  4/14/21       [ERROR   |2021-04-14 20:00:05,592|idefense_base.py|109|ID:afec4ae8-a7ae-4e46-b18a-23f3b723dfdd] Method makeRequest Error occured while making the request: 401 Client Error:  for url: https://api.intelgraph.idefense.com/rest/threatindicato
   8:00:05.592 PM r/v0/ip?last_published.from=2021-04-13T20%3A00%3A00.000Z&last_published.to=2021-04-14T20%3A00%3A00.000Z&confidence.from=50&severity.from=2&page=1
                 host = ctl   source = /opt/splunk/var/log/splunk/idefense-get_ip.log   sourcetype = idefense-get_ip-3
```

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)



splunk>enterprise
Apps ▾
Accenture Cyber Threat Intelligence Integration Health Check
Search
Datasets
Reports
Alerts
Dashboards

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.

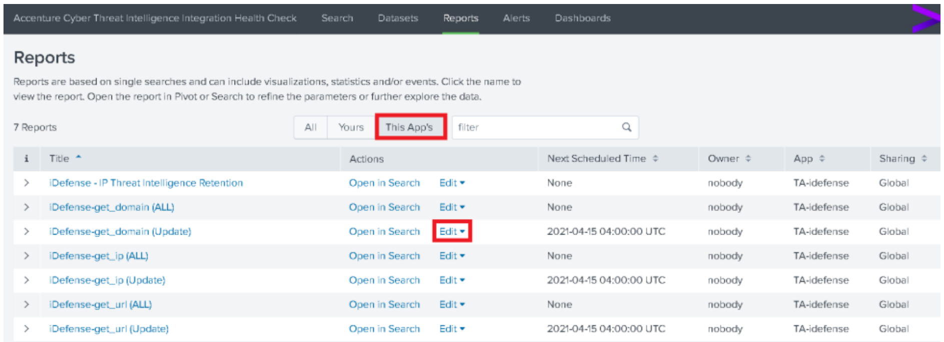
3 Reports

i	Title ▴	Actions	
>	iDefense-get_domain (ALL)	Open in Search	Edit ▾
>	iDefense-get_ip (ALL)	Open in Search	Edit ▾
>	iDefense-get_url (ALL)	Open in Search	Edit ▾

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.



Accenture Cyber Threat Intelligence Integration Health Check
Search
Datasets
Reports
Alerts
Dashboards

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.

7 Reports

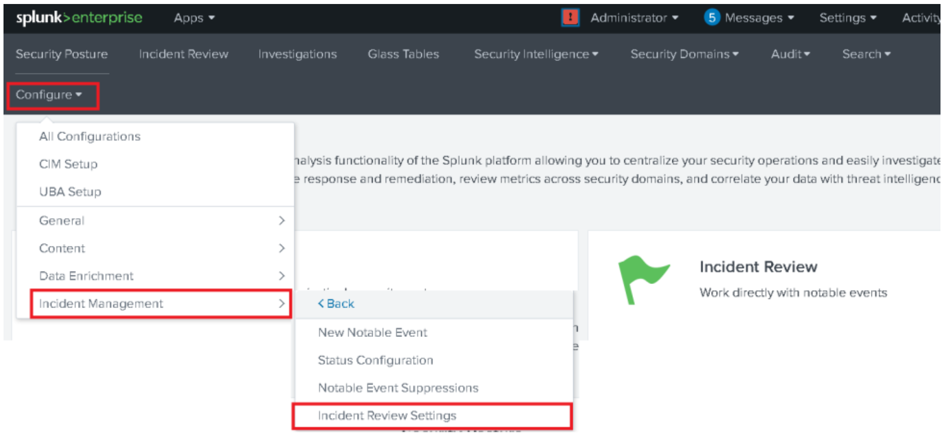
i	Title ▴	Actions		Next Scheduled Time ⇕	Owner ⇕	App ⇕	Sharing ⇕
>	iDefense - IP Threat Intelligence Retention	Open in Search	Edit ▾	None	nobody	TA-idefense	Global
>	iDefense-get_domain (ALL)	Open in Search	Edit ▾	None	nobody	TA-idefense	Global
>	iDefense-get_domain (Update)	Open in Search	Edit ▾	2021-04-15 04:00:00 UTC	nobody	TA-idefense	Global
>	iDefense-get_ip (ALL)	Open in Search	Edit ▾	None	nobody	TA-idefense	Global
>	iDefense-get_ip (Update)	Open in Search	Edit ▾	2021-04-15 04:00:00 UTC	nobody	TA-idefense	Global
>	iDefense-get_url (ALL)	Open in Search	Edit ▾	None	nobody	TA-idefense	Global
>	iDefense-get_url (Update)	Open in Search	Edit ▾	2021-04-15 04:00:00 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

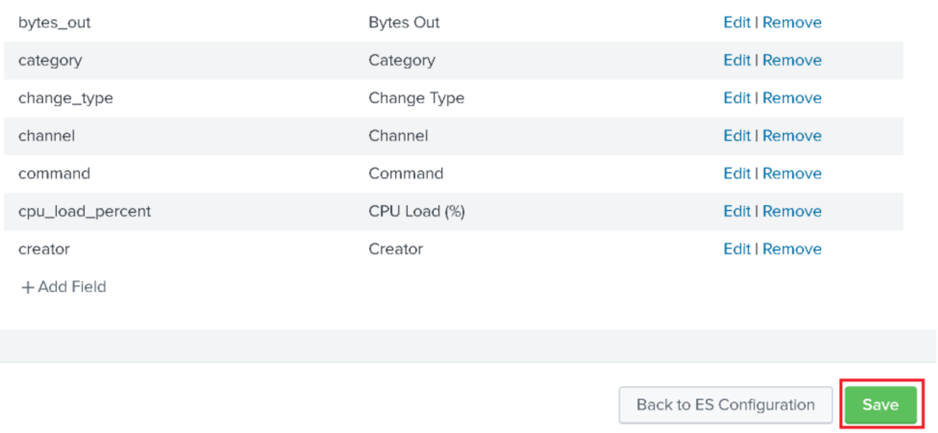
Work directly with notable events

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

Field	Label
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	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

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

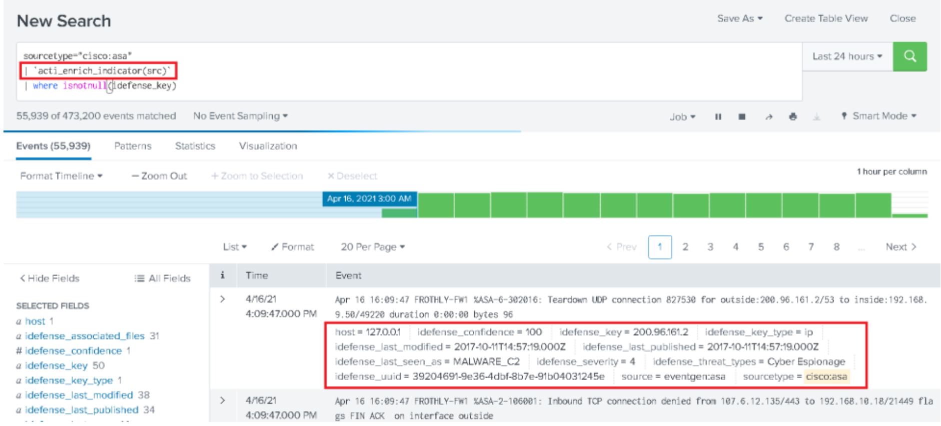
Check this link for more information on the Splunk's threat intel framework.

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:



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

55,939 of 473,200 events matched

SELECTED FIELDS
- a host 1
- a idefense_associated_files 31
- # idefense_confidence 1
- a idefense_key 50
- a idefense_key_type 1
- a idefense_last_modified 38
- a idefense_last_published 34

i	Time	Event

›	4/16/21 4:09:47.000 PM	Apr 16 16:09:47 FROTHLY-FW1 %ASA-6-302016: Teardown UDP connection 827530 for outside:200.96.161.2/53 to inside:192.168.9.50/49220 duration 0:00:00 bytes 96
		host = 127.0.0.1 | idefense_confidence = 100 | idefense_key = 200.96.161.2 | idefense_key_type = ip
		idefense_last_modified = 2017-10-11T14:57:19.000Z | idefense_last_published = 2017-10-11T14:57:19.000Z
		idefense_last_seen_as = MALWARE_C2 | idefense_severity = 4 | idefense_threat_types = Cyber Espionage
		idefense_uuid = 39204691-9e36-4dbf-8b7e-91b04031245e | source = eventgen:asa | sourcetype = cisco:asa

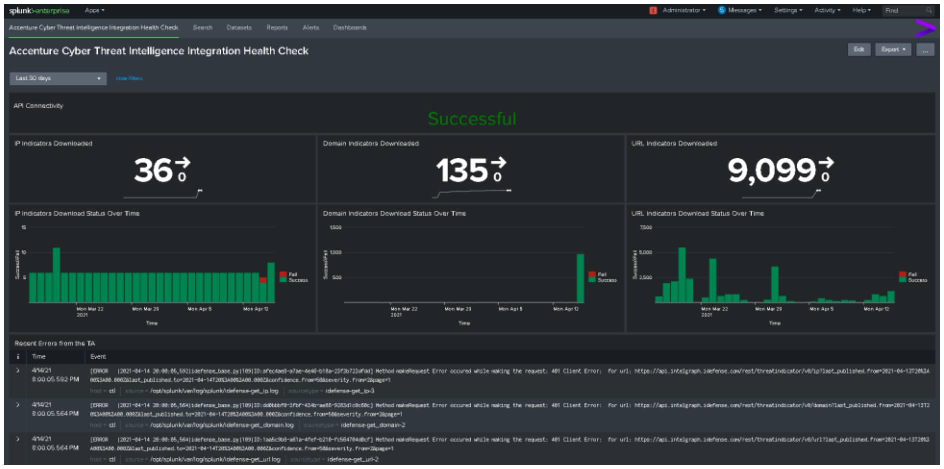
›	4/16/21 4:09:47.000 PM	Apr 16 16:09:47 FROTHLY-FW1 %ASA-2-106001: Inbound TCP connection denied from 107.6.12.135/443 to 192.168.10.18/21449 flags FIN ACK on interface outside

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 Health Check Dashboard appears as follows:

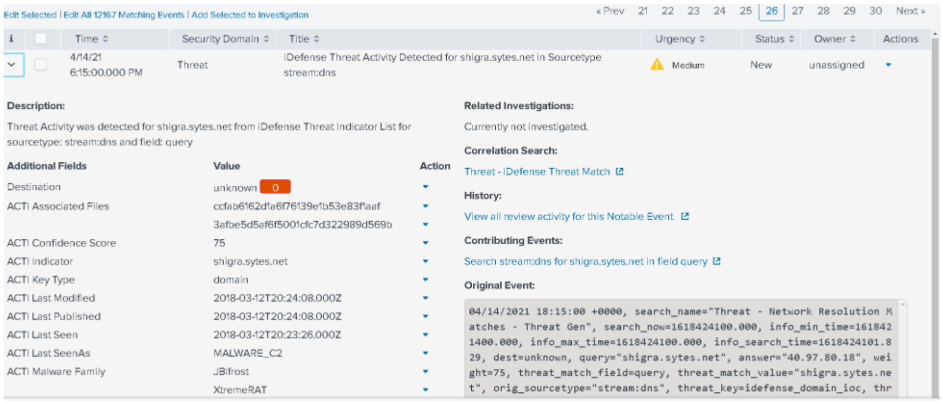


Recent Errors from the TA

i	Time	Event
›	4/14/21 8:00:05.592 PM	[ERROR |2021-04-14 20:00:05,592|idefense_base.py|109|ID:afec4ae8-a7ae-4e46-b18a-22f3b723dfdd] Method makeRequest Error occured while making the request: 401 Client Error: for url: https://api.intelgraph.idefense.com/rest/threatindicator/v0/ip?last_published.from=2021-04-13T20%2A00%3A00.000Z&last_published.to=2021-04-14T20%3A00%2A00.000Z&confidence.from=50&severity.from=2&page=1 host = ctl | source = /opt/splunk/var/log/splunk/idefense-get_ip.log | sourcetype = idefense-get_ip-3
›	4/14/21 8:00:05.564 PM	[ERROR |2021-04-14 20:00:05,564|idefense_base.py|109|ID:dd0bbbf0-3fbf-434b-ae85-9283d1c0c60c] Method makeRequest Error occured while making the request: 401 Client Error: for url: https://api.intelgraph.idefense.com/rest/threatindicator/v0/domain?last_published.from=2021-04-13T20%3A00%2A00.000Z&last_published.to=2021-04-14T20%2A00%3A00.000Z&confidence.from=50&severity.from=2&page=1 host = ctl | source = /opt/splunk/var/log/splunk/idefense-get_domain.log | sourcetype = idefense-get_domain-2
›	4/14/21 8:00:05.564 PM	[ERROR |2021-04-14 20:00:05,564|idefense_base.py|109|ID:1aa6c9b8-a61a-4fef-b210-fc564704d0cf] Method makeRequest Error occured while making the request: 401 Client Error: for url: https://api.intelgraph.idefense.com/rest/threatindicator/v0/url?last_published.from=2021-04-13T20%3A00%3A00.000Z&last_published.to=2021-04-14T20%3A00%2A00.000Z&confidence.from=50&severity.from=2&page=1 host = ctl | source = /opt/splunk/var/log/splunk/idefense-get_url.log | sourcetype = idefense-get_url-2

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:



Edit Selected | Edit All 12167 Matching Events | Add Selected to Investigation

« Prev 21 22 23 24 25 26 27 28 29 30 Next »

i	□	Time	Security Domain	Title	Urgency	Status	Owner	Actions
	□	4/14/21 6:15:00.000 PM	Threat	iDefense Threat Activity Detected for shigra.sytes.net in Sourcetype stream:dns	⚠ Medium	New	unassigned	

Description:

Threat Activity was detected for shigra.sytes.net from iDefense Threat Indicator List for sourcetype: stream:dns and field: query

Additional Fields	Value	Action
Destination	unknown 0	
ACTI Associated Files	ccfab6162d1a6f76139e1b53e83f1aaf	
	3afbe5d5af6f5001cfc7d322989d569b	
ACTI Confidence Score	75	
ACTI Indicator	shigra.sytes.net	
ACTI Key Type	domain	
ACTI Last Modified	2018-03-12T20:24:08.000Z	
ACTI Last Published	2018-03-12T20:24:08.000Z	
ACTI Last Seen	2018-03-12T20:23:26.000Z	
ACTI Last SeenAs	MALWARE_C2	
ACTI Malware Family	JBifrost	
	XtremeRAT	

Related Investigations:

Currently not investigated.

Correlation Search:

Threat - iDefense Threat Match

History:

View all review activity for this Notable Event

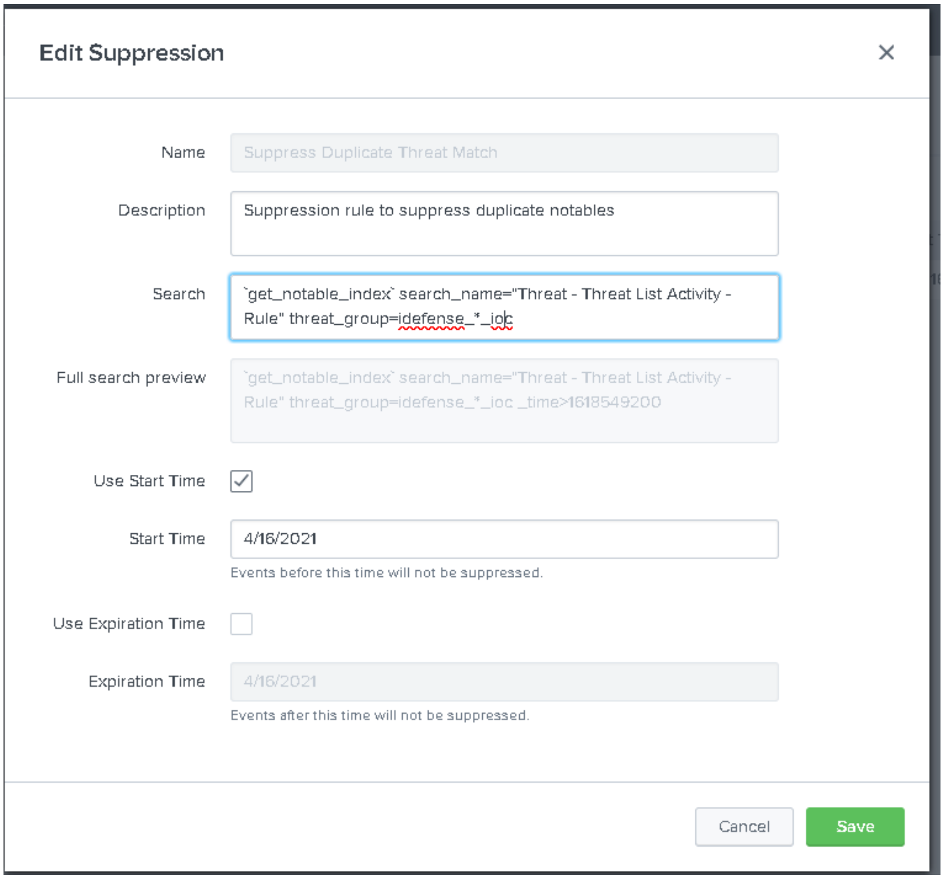
Contributing Events:

Search stream:dns for shigra.sytes.net in field query

Original Event:

```
04/14/2021 18:15:00 +0000, search_name="Threat - Network Resolution M
atches - Threat Gen", search_now=1618424100.000, info_min_time=161842
1400.000, info_max_time=1618424100.000, info_search_time=1618424101.8
29, dest=unknown, query="shigra.sytes.net", answer="40.97.80.18", wei
ght=75, threat_match_field=query, threat_match_value="shigra.sytes.ne
t", orig_sourcetype="stream:dns", threat_key=idefense_domain_ioc, thr
```

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.

Troubleshooting

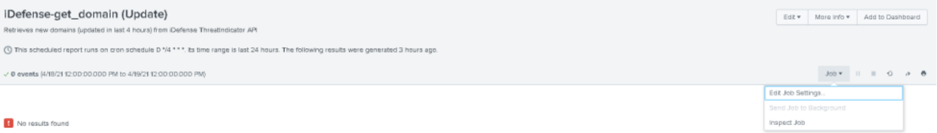
Where to find the Logs for this Add-On

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.



iDefense-get_domain (Update)

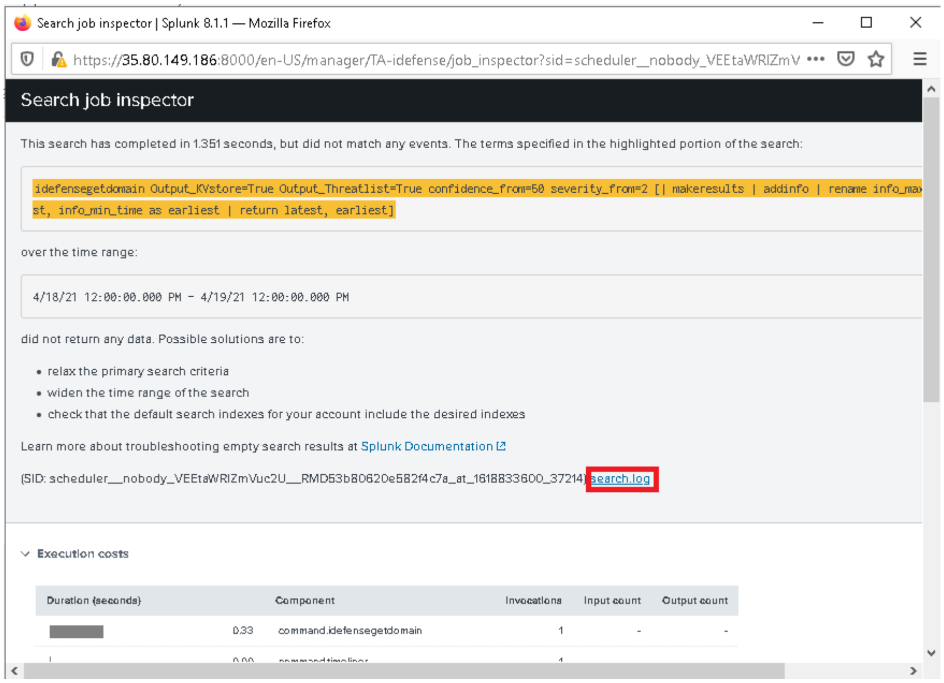
Retrieves new domains (updated in last 4 hours) from iDefense ThreatIndicator API

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.



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_VEEtaWRlZmV

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_VEEtaWRlZmVuc2U__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 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.