



ThreatScape® App for Splunk Overview, Installation and Configuration

December 23, 2015



Description	3
System Requirements	3
ThreatScape App for Splunk Functionality	3
ThreatScape Cyber Threat Intelligence and Indicators	3
Threat Intelligence Indicator Fields and Splunk CIM Compliance	5
ThreatScape App for Splunk ALIASFIELD Entries	6
ThreatScape App for Splunk Index and Sourcetypes.....	6
IOC Dashboard	7
Creating Correlations Using iSIGHT Threatscape Intel Data in Splunk	8
Workflow Actions:	12
Pivot Search.....	14
ThreatScape App for Splunk Acquisition, Installation and Configuration	16
Acquisition.....	16
Installation/Upgrade	16
Configuration	25

Description

The ThreatScape App for Splunk facilitates the delivery of iSIGHT Partners ThreatScape Indicators to our customers' Splunk instances. Once consumed by a Splunk instance, the ThreatScape Indicators are treated as additional Splunk source types and can be used in search, correlation, reporting, and visualization workflows in the same manner as other data.

System Requirements

The ThreatScape App for Splunk shares the requirements of a properly installed Splunk instance and has been fully tested on the following platforms under the Splunk Enterprise 6.2.7 and 6.3.1 Free Edition:

OS Platforms
CentOS 64 Bit Server 7
CentOS 64 Bit Server 6.6
Ubuntu 64 Bit Server 14.04 LTS

ThreatScape App for Splunk Functionality

The functionality of the ThreatScape App for Splunk is underpinned by the ThreatScape API 2; the ThreatScape API is the repository from which the ThreatScape App for Splunk retrieves its data, after which Splunk users rely on the Splunk engine to leverage the ThreatScape API Data. As such, an understanding of the ThreatScape Cyber Threat Indicators and its delivery mechanism (i.e., the ThreatScape API) is fundamental for the efficient integration of ThreatScape API data into Splunk operations.

ThreatScape Cyber Threat Intelligence and Indicators

ThreatScape Cyber Threat Intelligence and Indicators as delivered by the ThreatScape API can best be understood in the context of threat indicators as a whole. There are many sources of threat indicators – commercial feeds, open-source lists, proprietary honeypots, etc. – and threat data can be obtained from any or all of these sources. What differentiates the iSIGHT Partners indicators from others is that the indicators are truly intelligence-based; all indicators delivered by the API have been observed by iSIGHT Partners intelligence researchers and analysts during the course of their collections and research, and all of these indicators have context in the form of intelligence reporting.

Additionally, the iSIGHT Partners API delivers vulnerabilities and two types of indicators. The first type, Indications and Warnings (I&Ws) are *any* indicators that iSIGHT Partners researchers and analysts discover during their research. The second type, Indicators of Compromise (IOCs), is confirmed as having been used in an actual attack. I&Ws are useful for security researchers who are looking for trends and as much intelligence as possible, whereas IOCs are most suited for Security Operators who want to minimize false positives.

The Venn diagram below shows the relationship among the different types of indicators:

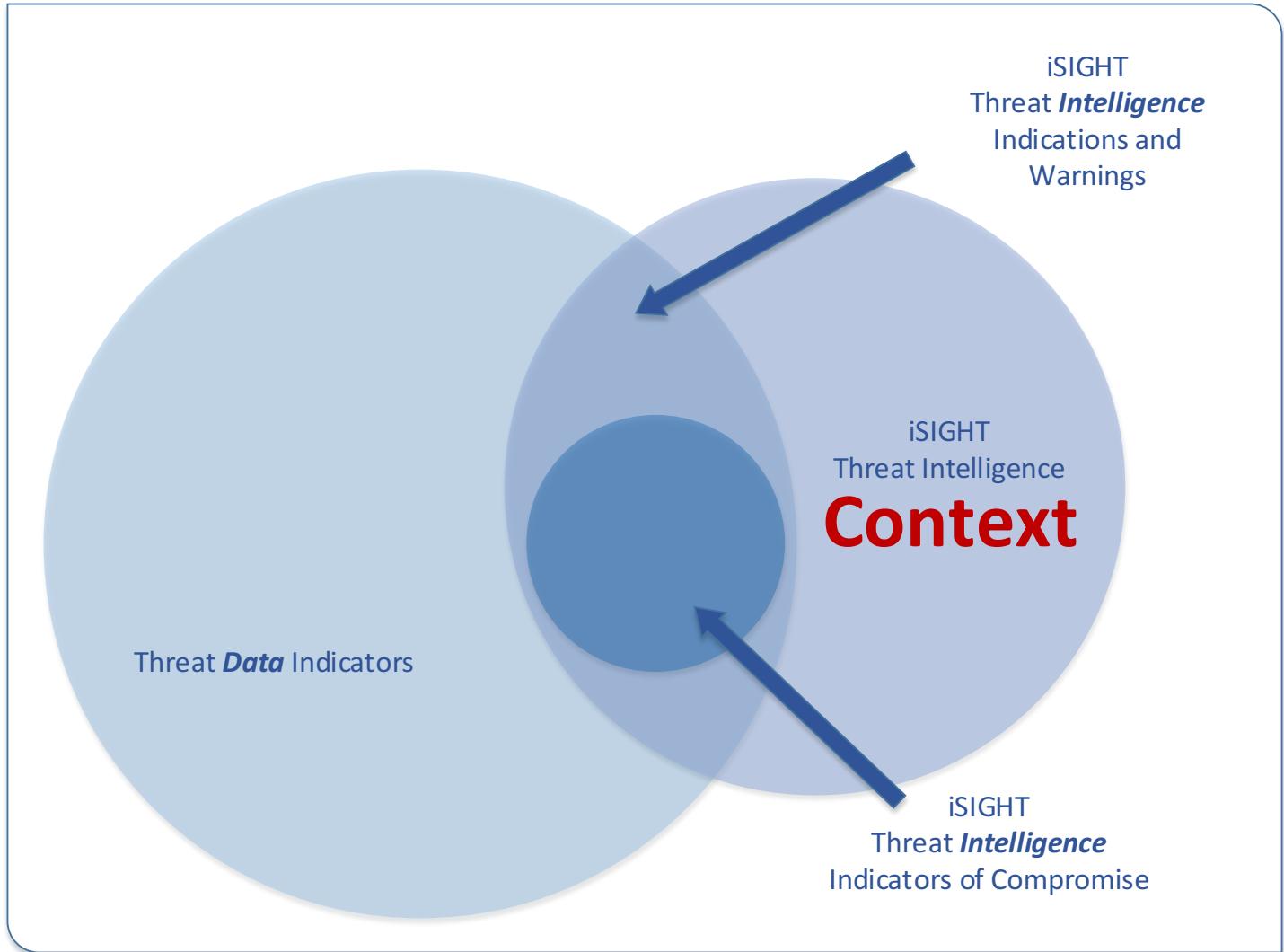


Diagram 1: Relationship Among Indicators Types

Threat Intelligence Indicator Fields and Splunk CIM Compliance

The ThreatScape App for Splunk downloads records containing the following fields from the ThreatScape API:

ThreatScape	fileType	productType	senderName
asn	fuzzyHash	Protocol	sha1
cidr	ip	publishDate	sha256
description	Language	Recipient	sourceDomain
domain	md5	registrantE-mail	sourcelp
domainTimeOfLookup	networkIdentifier	registrantName	Subject
e-mailIdentifier	networkName	Registry	Title
fileIdentifier	networkType	reportId	url
fileName	packer	reportLink	userAgent
fileSize	Port	senderAddress	webLink
attackingEase	cpe	cvelds	cveOriginalReleaseDate
cvssBaseScore	cvssTemporalScore	exploitInTheWild	mitigations

There are a few features of the ThreatScape API that must be covered to maximize the use of the API data in Splunk:

1. Because the ThreatScape API delivers machine intelligence to a variety of products, the API uses generic field names that are not by themselves Splunk Common Information Model (CIM) compliant. This fact is overcome with the use of Splunk *FIELDALIAS* mappings within the ThreatScape App for the Splunk *props.conf* file located at:

/opt/splunk/etc/apps/iSIGHTPartners_ThreatScape_App/default

Splunk operators are of course free to modify this *props.conf* file to define any additional aliases that are required for their environments or they can use the Splunk *rename* command in the search dialog to achieve similar results.

2. ThreatScape API network-related fields are intentionally non-directional, as this provides the most flexibility in searching disparate data sets. For example, an "ip" address indicator can, depending on the search requirements, either be a source address or a destination address. For this reason, the ThreatScape API "ip" and "port" fields are aliased to *both* corresponding CIM compliant "src" and "dest" fields.
3. Despite the aliased field names, each of the native field names remains available for searching. This is particularly useful when searching for known hashes of a certain type.

ThreatScape App for Splunk ALIASFIELD Entries

The following is a list of ALIASFIELD entries used for Splunk CIM compliance:

```
[host::ThreatScape® API]
#Direct Field Mappings
FIELDALIAS-file_cat = fileType AS category
FIELDALIAS-dest_domain = domain AS dest
FIELDALIAS-dest_ip = ip AS dest_ip
FIELDALIAS-dest_port = port AS dest_port
FIELDALIAS-hash_fuzzy = fuzzyHash AS file_hash
FIELDALIAS-hash_md5 = md5 AS file_hash
FIELDALIAS-hash_sha1 = sha1 AS file_hash
FIELDALIAS-hash_sha256 = sha256 AS file_hash
FIELDALIAS-file_name = fileName AS file_name
FIELDALIAS-http_user_agent = userAgent AS http_user_agent
FIELDALIAS-registry_obj_cat = registry AS object_category
FIELDALIAS-src_domain = domain AS src
FIELDALIAS-source_domain = sourceDomain AS src
FIELDALIAS-src_ip = ip AS src_ip
FIELDALIAS-source_ip = sourceIp AS src_ip
FIELDALIAS-src_port = port AS src_port
FIELDALIAS-transport = protocol AS transport
#Aggregate Field Mappings
FIELDALIAS-dest_all_ip = dest_ip AS dest
FIELDALIAS-src_all_ip = src_ip AS src
EVAL-file_hash = mvappend(md5, sha256, sha1)
#New Mappings
FIELDALIAS-cveIds = cveIds as cve
FIELDALIAS-cvssBaseScore = cvssBaseScore as cvss
FIELDALIAS-cvssTemporalScore = cvssTemporalScore AS cvss
```

ThreatScape App for Splunk Index and Sourcetypes

As described in the previous sections, the ThreatScape API contains vulnerabilities and two types of intelligence indicators: I&Ws and IOCs. All intelligence indicators and vulnerabilities data is saved in the same index named "isightpartners." I&Ws, IOCs and vulnerabilities are defined as the Splunk sourcetypes "isight_indicators", "isight_iocs" and "isight_vulnerabilities" respectively. This approach allows for maximum search flexibility, although it does mean that the index will have duplicate data. Duplicate data can be minimized by selecting one source type or the other during configuration (see below for more details).

IOC Dashboard

This dashboard will search iSIGHT reporting for the indicators users specify. When results are generated, user may click "Report ID" values to visit the MySIGHT portal and view the entire report.

Dashboard components:

The screenshot shows the Splunk web app header with 'splunk' and 'App: iSIGHT Partners'. Below the header, there are tabs for 'Matched Indicators', 'IOC Dashboard' (which is selected), 'Statistics', and 'Search'. On the right side of the header is the 'iSIGHTPARTNERS' logo. The main content area is titled 'IOC Dashboard' and contains the following fields:

- A time range dialog set to 'Last 30 days'.
- An input field for 'Enter one or more IOCs of any type, or a string of text. Use comma(,) as a separator for multiple IOCs.' containing '5.199.171.34,mecuwiqmb.com'.
- A dropdown for 'Specify the IOC ID as either Attacker,Compromised or All. Leave default to see all IOCs regardless of ID.' set to 'All'.
- A green 'Submit' button.

Figure-1 (IOC Dashboard)

In the above Figure-1, you see the normal Splunk web app header and the first row of form inputs.

1. The first option is a time range dialog, and this will drive how far back into reporting users wish to search (time is based on a report's publish date)
2. Enter IOCs. This can be any indicator type, in any sequence separated by a delimiter comma (,).
3. Since IOCs are tagged as Attacker and Compromised, user can select either of these options or all.
4. Clicking the "Submit" button to launch the search, the following response data is returned.

The screenshot shows the same Splunk web app header and tabs as Figure-1. The main content area is titled 'IOC Dashboard' and displays the following results:

IOCs Searched For:		Matching Reports (IOCs were found in raw text of the reports below)
search_iocs	<1m ago	Report ID: 15-00014452 Report Title: Indicator Report: TorrentLocker Activity Report (Dec. 9 to 16, 2015) Publish Date: 12/16/15 15:06:00
195.14.104.139		
toenocovo.org		

Figure-2 (IOC Dashboard Results)

Creating Correlations Using iSIGHT Threatscape Intel Data in Splunk

There are few sample searches that come bundled with iSIGHT Threatscape App for Splunk as shown below:

Search name	RSS feed	Scheduled time	Display view	Owner	App
Histogram of delay in seconds	None	report_builder_display	No owner	iSIGHTPartners_ThreatScape_App	
Mail delivery time	None	report_builder_display	No owner	iSIGHTPartners_ThreatScape_App	
⚡ Matched Domain	2015-12-15 12:00:00 EST	None	No owner	iSIGHTPartners_ThreatScape_App	
⚡ Matched File Hash md5	2015-12-15 02:20:00 EST	None	No owner	iSIGHTPartners_ThreatScape_App	
⚡ Matched File Hash sha1	2015-12-15 02:30:00 EST	None	No owner	iSIGHTPartners_ThreatScape_App	
⚡ Matched File Hash sha256	2015-12-15 03:00:00 EST	None	No owner	iSIGHTPartners_ThreatScape_App	
⚡ Matched IP	2015-12-15 04:00:00 EST	None	No owner	iSIGHTPartners_ThreatScape_App	
⚡ Matched URL	2015-12-16 00:00:00 EST	None	No owner	iSIGHTPartners_ThreatScape_App	

Figure-3 (Searches, reports and alerts)

This section is accessible from: **Settings -> Knowledge -> Searches, Reports and Alerts.**

Users can create a new search, by selecting the “New” button in the top left, or they can clone or modify existing searches. This example shows a rule being modified, but the dialog is the same for all functions:

Search

```
index=isightpartners [search index=source db  
earliest= -5m |fields domain] | stats count by domain
```

Description

Matched Domain

Time range

Start time

Finish time

Time specifiers: y, mon, d, h, m, s
[Learn more](#)

Acceleration

Accelerate this search

Summary range

1 Month ▾

Schedule and alert

Schedule this search

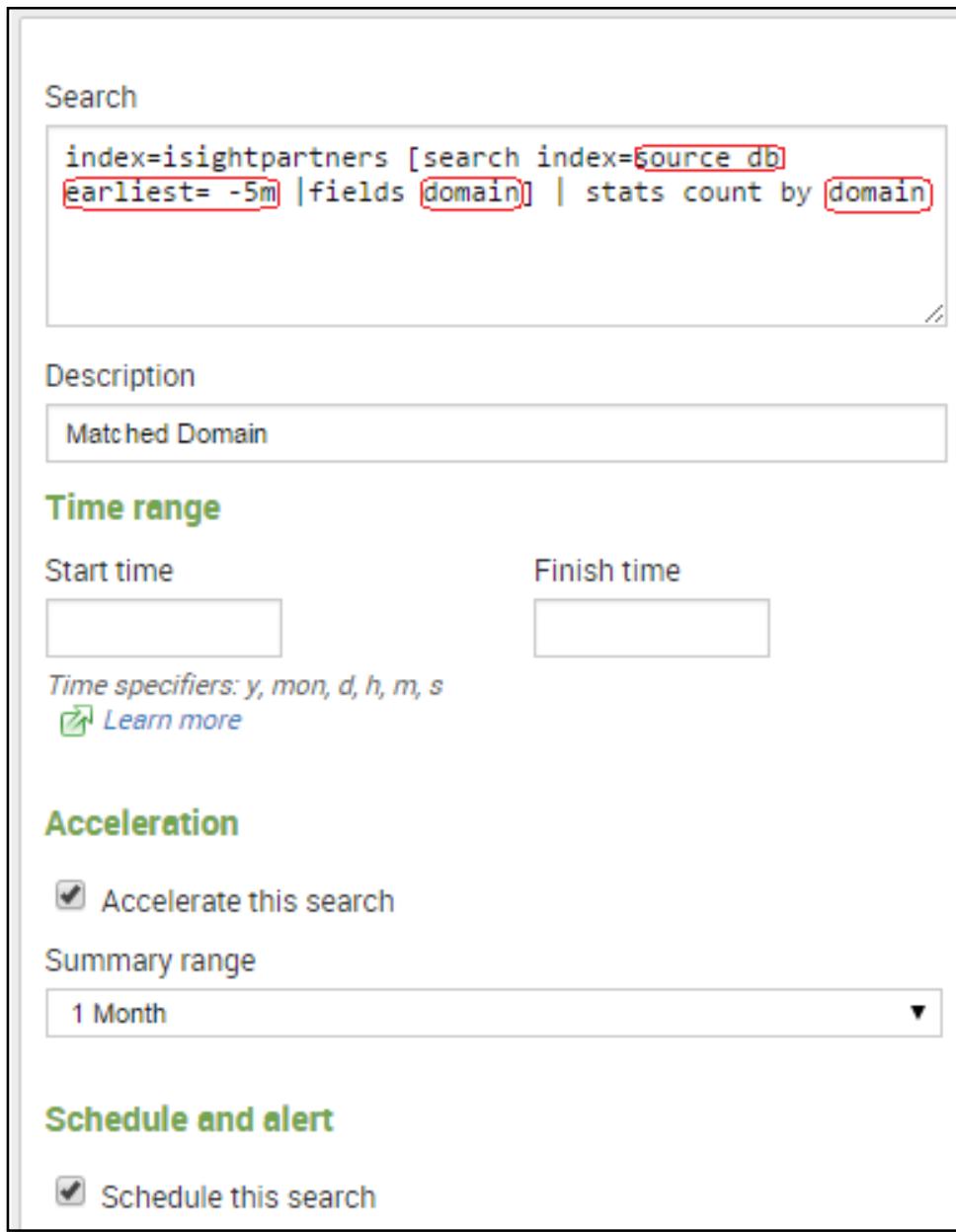


Figure-4 (Edit search window)

In the above Figure-4, **source_db** can be replaced with any custom index which is to be matched with index of **isightpartners**. User can also provide any supported CIM fields like *fields domain*, *fields ip*, *fields md5* etc. Description is for referencing the Search.

So, in case a user has one or more index created in Splunk, the same can be used for correlation (instead of source_db that is mentioned in the search query screen shown above)

Schedule and alert

Schedule this search

Schedule type *

Cron

Cron schedule

`*/5 * * * *`

*Enter a cron-style schedule.
For example '*/5 * * * *' (every 5 minutes) or '0 21 * * *' (every day at 9 PM).*

Schedule Window

0

*Sets an optional window of time (in minutes) within which a report can start.
Improves efficiency when there are many concurrently scheduled reports.*

Alert

Condition

always

To enable all the alert conditions, disable summary indexing.

Alert mode

Once per search

Throttling

After triggering the alert, don't trigger it again for

Expiration *

After 24 hours

How long Splunk keeps a record of each triggered alert.

Severity *

Medium

Figure-5 (Edit search window contd)

This job can be scheduled as cron job as shown in Figure-5, this schedule can be specified the highlighted text box.

Note: Scheduled cron job time should be equal to earliest time ('earliest' value used in search query shown in Figure-4 above) to avoid duplication.

Alert actions

Send email
 Enable
[Click to edit email action](#)

Add to RSS
 Enable
The RSS link is available in Settings > Searches, reports, and alerts.

Run a script
 Enable

List in Triggered Alerts
 Enable
Triggered Alerts are available in Activity located in the upper right navigation.

Summary indexing

Enable
Enabling summary indexing will set the alert condition to 'always'.

Select the summary index
isight_matches

Only indexes that you can write to are listed.

Add fields

type	=	matched_domain	Delete
	=		Delete

Add another field

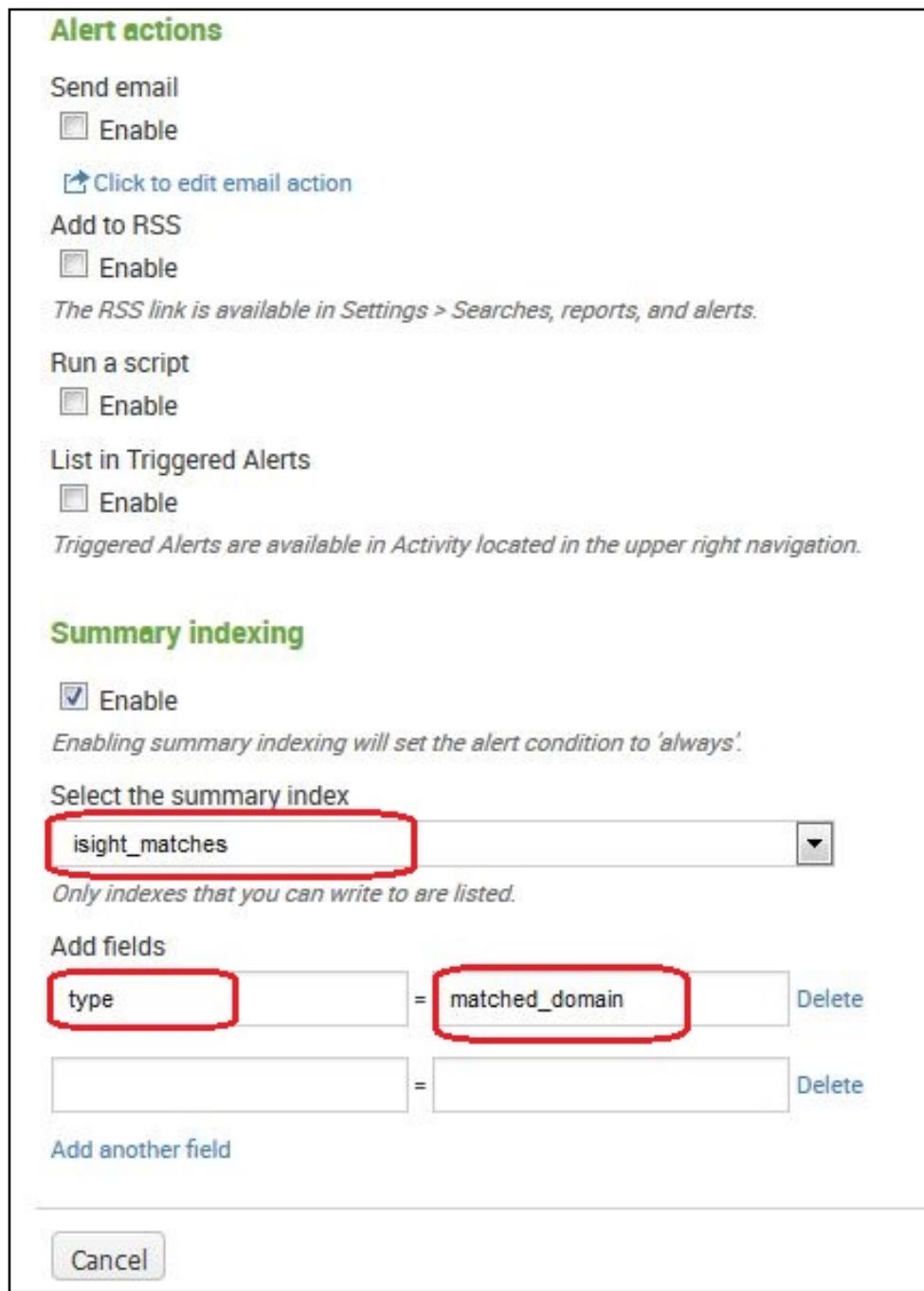


Figure-6 (Edit search window cont'd)

The ThreatScape App provides the option of summary indexing for the correlation of customer data. With summary indexing, users can extract precise information based on search strings queried frequently. Each

time Splunk Enterprise runs these searches, it saves the results into a summary index that the user designates. Users can then run searches and reports on this significantly smaller (and thus more responsive) summary index.

By default, ThreatScape App uses **isight_matches** as the summary index. User can run searches and reports on this summary index for matched results. Users can however create their own summary index instead of default. Figure-6 shows the configuration of summary indexing.

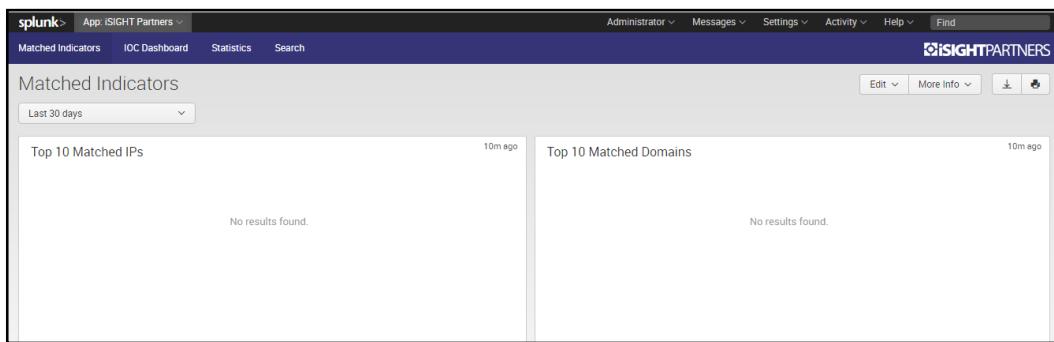
To classify the search result separately a field **type** is added with value **matched_domain**.

Example Rules/Correlations

1. Find correlation of passiveDNS data from internal log file with iSIGHT IOCs.
 - a. Rule helps with discovery of exfiltration in organization. Needs passiveDNS logs as comparison input.
 - b. `index=isightpartners sourcetype=isight_iocs | rename domain as pDNSDomain | join pDNSDomain [search sourcetype=passiveDNS NOT (Recursion OR Response)] | table _time, sourcetype, queryHost, pDNSDomain, ip, reportId, webLink, title, ThreatScape | dedup pDNSDomain`
 - c. This is a great indicator to detect where or not there is outbound communication with a bad actor. Business problem = Exfiltration. Address with DLP.
2. Find correlation of data in index ‘test_index’ that are not in iSIGHT iocs.
 - a. The event data from this index may share at least one common field. You can use the values of this field to search for events in **test** index based on a value that is not in sourcetype= isight_iocs.
 - b. `index=test_index NOT [search index=isightpartners sourcetype=isight_iocs| fields ip] | stats count by ip | dedup ip`
 - c. This helps ascertaining that there are no known indicators of compromise with regard to the given set of data.

Matched Indicators

Once the required correlations are created as defined in the above section, the ‘Matched indicator’ section in the app offers a quick view of top/relevant matches between customer and iSIGHT data. This is further customizable by the Admin, so as to show relevant data as per preferences. In case the relevant customer data index and correlation is not setup, the tab will display blank panels(as shown below).



Workflow Actions:

The ThreatScape App provides three types of workflow actions:

1. Search against iSIGHT Partners indicators
2. Pivot search against iSIGHT Partners indicators
3. View report on MySIGHT portal

Workflow actions appear in menus associated with events in search results. To select event-level workflow actions, expand an event in your search results and click **Event Actions**, as shown in the figure below. This is an example of "Search/Pivot Search/View report," an event-level workflow action that, when clicked, displays the new tab with the appropriate search/pivot search strings and results.

View report redirects the user to the MySIGHT Portal report page.

The screenshot shows a Splunk search results page. On the left, there's a sidebar with 'Selected Fields' and 'Interesting Fields' lists. The main area shows a table with columns for 'Time' and 'Event'. An event is selected, displaying its raw JSON data. A context menu is open over this event, with 'Event Actions' highlighted. The menu options include: 'Indicators SHA1 = null', 'Pivot Search against iSIGHT Partners Indicators SHA256 = null', 'Pivot Search against iSIGHT Partners Indicators URL = null', 'Search against iSIGHT Partners Indicators Domain = jeluganusog.eu', 'Search against iSIGHT Partners Indicators File Hash = null', 'Search against iSIGHT Partners Indicators IP = 31.170.178.179', and 'Search against iSIGHT Partners Indicators MD5 = null'. Below the table, there's a search bar and a footer with the URL '10.201.50.11:8000/en-US/app/iSIGHTPartners_ThreatScape_App/search?q=search index%3D"iisightpartners" ip!%3Dnull ip%3D"31.170.178.179"&earliest=1447765098&latest=145035709'.

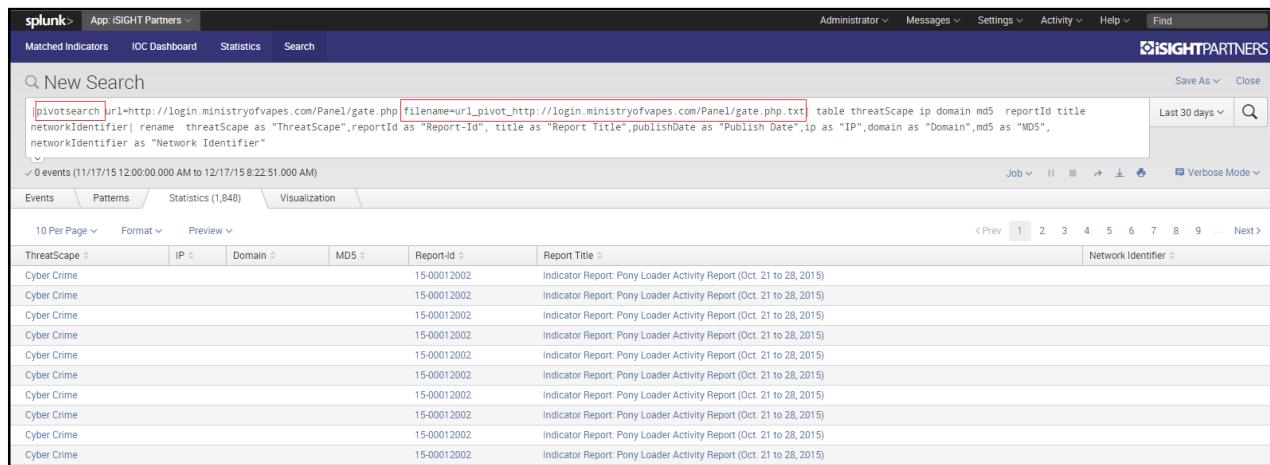
Figure-7 (Workflow actions)

These workflow actions for search/pivot search are available for 6 types of indicators: IP, Domain, SHA1, SHA256, MD5, URL and FileHash.

Pivot Search

Pivot search functionality is provided to retrieve additional indicators related to a given indicator, within the Splunk interface. It is provided as a part of the workflow actions described above and can be performed by introducing the custom search command “pivotsearch”. The following figure shows an example of pivot search command for a URL indicator and the results.

When clicked, the pivot search command will be executed. With the below search query, the result is also saved as a file (name specified in the search query) under apps bin directory. Pivoting on matching indicators (inside and outside the organization) extend the observable and actionable information. An IP can pivot to a domain owned by architects of specific malware which can identify intent and capability thus guiding a particular mitigation response.



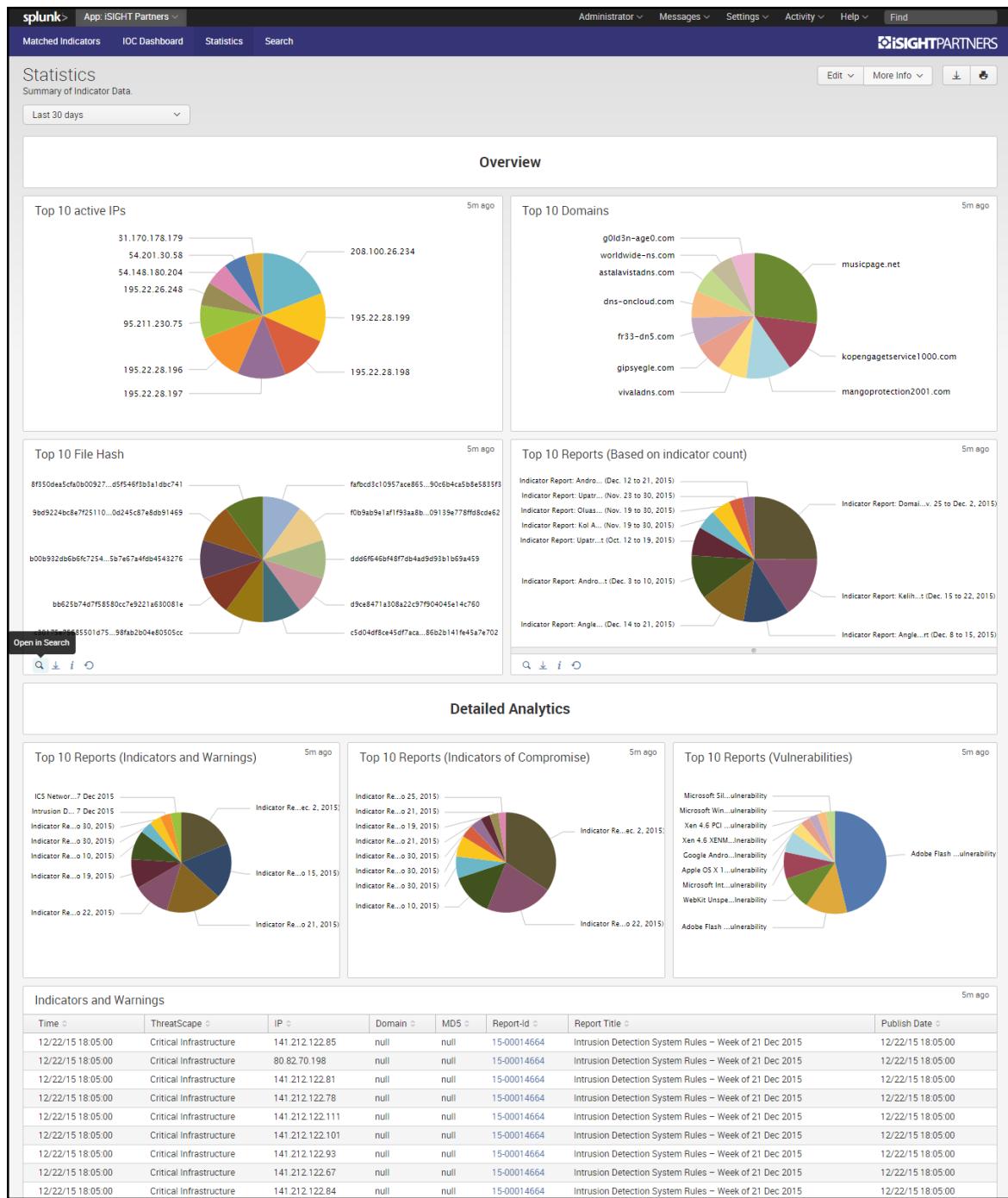
The screenshot shows the Splunk interface with the following details:

- Search Bar:** Contains the search command: `pivotsearch url=http://login.ministryofvapes.com/Panel/gate.php [filename=url_pivot_http://login.ministryofvapes.com/Panel/gate.php.txt]`. This command is highlighted with a red box.
- Results Panel:** Shows 0 events found between 11/17/15 12:00:00.000 AM and 12/17/15 8:22:51.000 AM.
- Table Headers:** ThreatScape, IP, Domain, MD5, Report-Id, Report Title.
- Table Data:** A list of 15 entries, all labeled "Cyber Crime" under ThreatScape, with various Report-Id and Report Title values.

Figure-8 (Pivot search command)

Statistics

The app offers a visual interface to quickly look at the top indicators (IPs, Domains, File Hash, etc.) and interact with this data. The page uses predefined search queries to pull the relevant data into the panels and this can be further customized to suit user preferences. The user also has the option of accessing the search query through the ‘search’ icon in the ribbon as well as exporting the results in the preferred format (CSV, XML, JSON)



ThreatScape App for Splunk Acquisition, Installation and Configuration

Acquisition

The ThreatScape App for Splunk is available from Splunk's splunkbase at:

<https://splunkbase.splunk.com/app/2764>

The ThreatScape App for Splunk can also be obtained directly from within the Apps page of Splunk (search for "ThreatScape") or from your iSIGHT Partners point of contact. Keep in mind that before using the ThreatScape App for Splunk, you will need a set of ThreatScape API keys¹.



Installation/Upgrade

If the ThreatScape App for Splunk is acquired through the Splunk admin browser, the app will automatically install following Splunk standard prompting. **In the case of an upgrade it is recommended to run the provided script prior to the upgrade to avoid duplicate indexing of data.**

If the ThreatScape App for Splunk is obtained as a file from your iSIGHT Partners Point of Contact or if it is downloaded from Splunk's splunkbase, you will need to install the file from the Splunk admin browser using the following steps:

1. From the Splunk home page, navigate to the Splunk App page.

¹ If you do not have an iSIGHT Partners ThreatScape API account, please request that we contact you by visiting the following site: <http://www.isightpartners.com/act-today/request-consultation/>

The screenshot shows the Splunk 6.2.3 home page at the URL 192.168.169.130:8000/en-US/app/launcher/home. A blue arrow points to the 'splunk>' logo in the top left corner. The main content area is titled 'Explore Splunk Enterprise' and features four sections: 'Add Data', 'Splunk Apps', 'Splunk Docs', and 'Splunk Answers'. Each section includes an icon, a title, and a brief description. A large modal window is open in the center, showing three small charts (bar, line, and area) and a 'Close' button.

splunk> splunk>

Administrator Messages Settings Activity Help Find

Apps splunk>

Explore Splunk Enterprise

Add Data

Splunk Apps

Splunk Docs

Splunk Answers

Search & Reporting

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

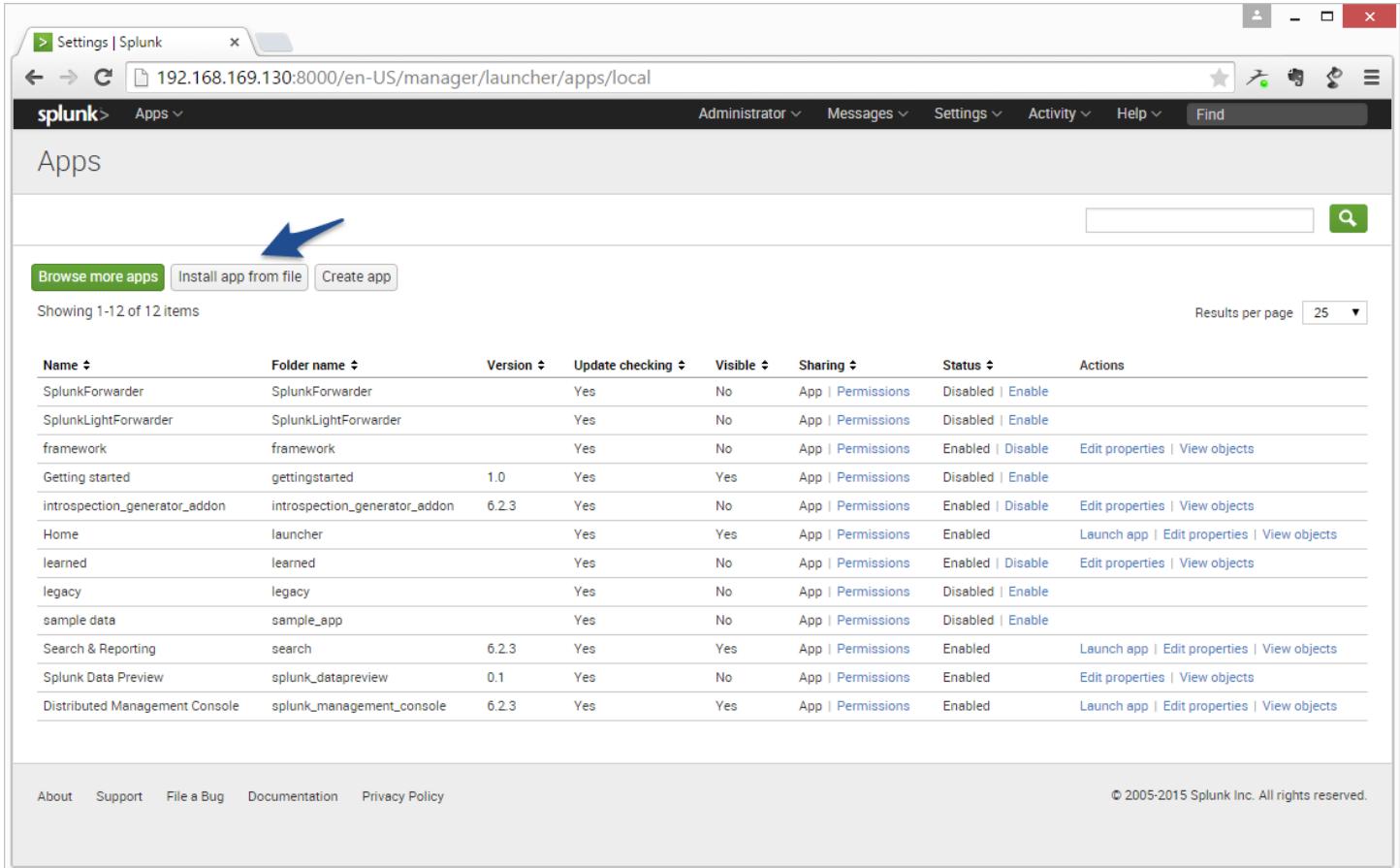
Apps and add-ons extend the capabilities of Splunk Enterprise.

Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

Have questions about how to do something with Splunk products? Get answers fast.

Close

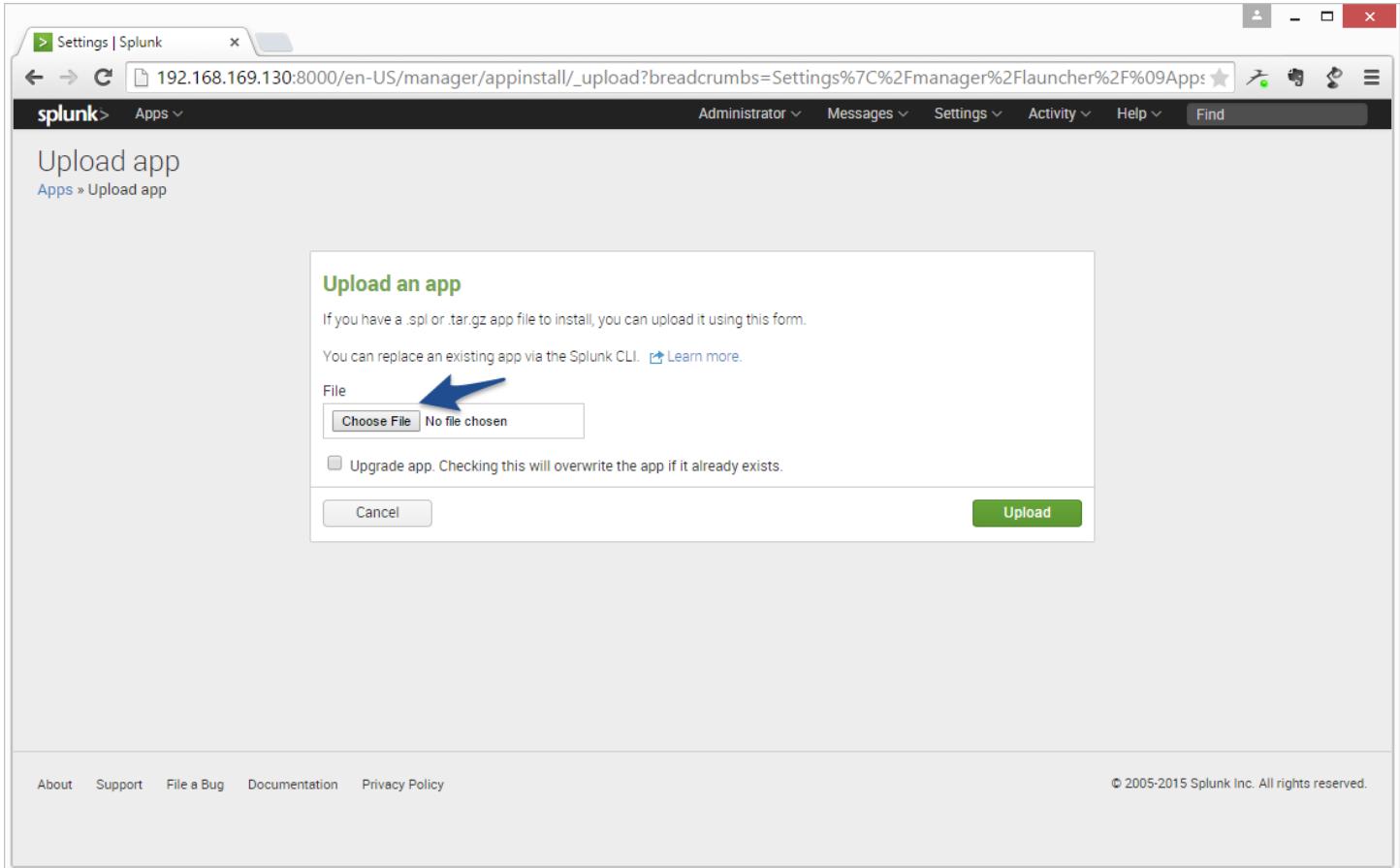
2. Select the button labeled "Install app from file."



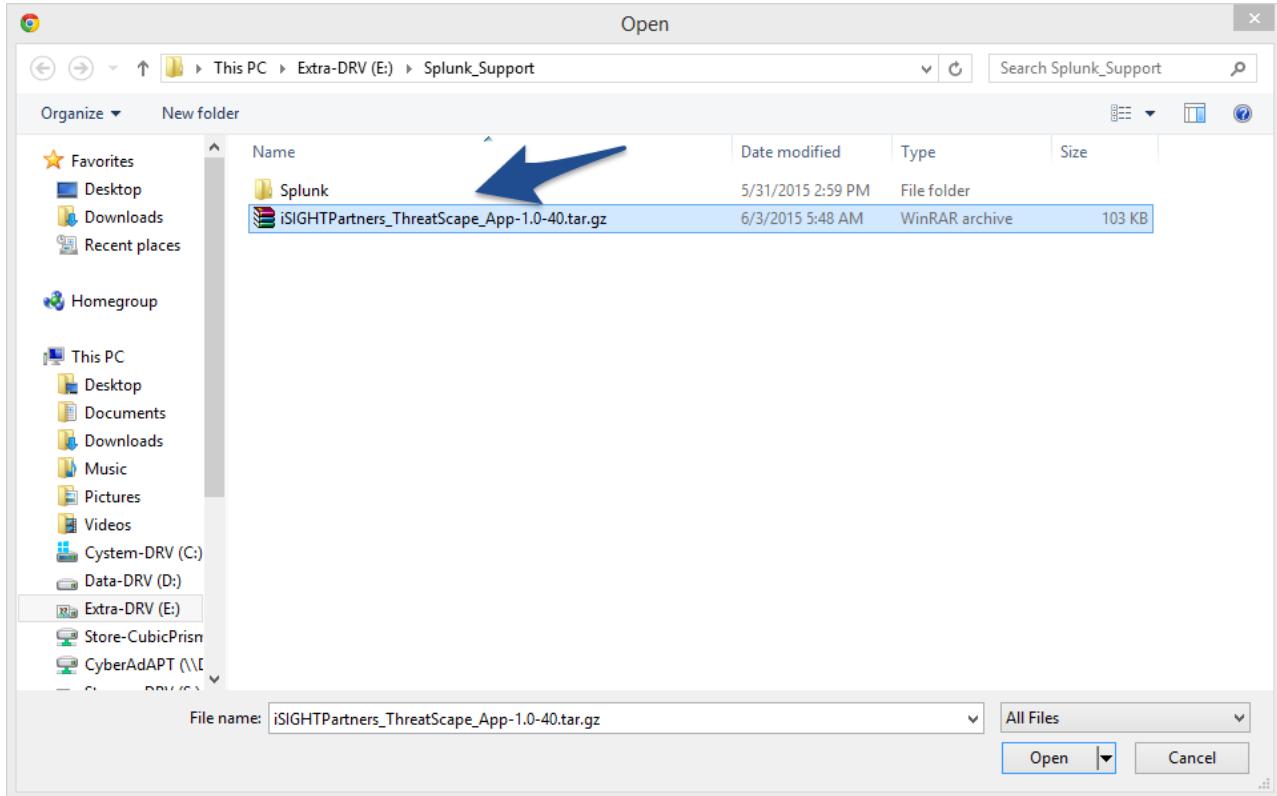
The screenshot shows the Splunk Settings interface with the URL `192.168.169.130:8000/en-US/manager/launcher/apps/local`. The page title is "Settings | Splunk". The top navigation bar includes links for "Administrator", "Messages", "Settings", "Activity", "Help", and "Find". Below the navigation is a search bar and a "Results per page" dropdown set to 25. The main content area is titled "Apps" and displays a table of 12 items. The table columns are: Name, Folder name, Version, Update checking, Visible, Sharing, Status, and Actions. The "Actions" column contains links like "Edit properties" and "View objects". At the bottom of the table, there are buttons for "Browse more apps", "Install app from file" (which has a blue arrow pointing to it), and "Create app". The footer contains links for "About", "Support", "File a Bug", "Documentation", and "Privacy Policy", along with a copyright notice: "© 2005-2015 Splunk Inc. All rights reserved."

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
framework	framework		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Getting started	gettingstarted	1.0	Yes	Yes	App Permissions	Disabled Enable	
introspection_generator_addon	introspection_generator_addon	6.2.3	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
legacy	legacy		Yes	No	App Permissions	Disabled Enable	
sample data	sample_app		Yes	No	App Permissions	Disabled Enable	
Search & Reporting	search	6.2.3	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Splunk Data Preview	splunk_datapreview	0.1	Yes	No	App Permissions	Enabled	Edit properties View objects
Distributed Management Console	splunk_management_console	6.2.3	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects

3. Select the button labeled "Choose File."



4. Navigate to the ThreatScape App for Splunk file on your local system and select the button labeled "Open".



NOTE: ThreatScape App Upgrade:

To upgrade the ThreatScape App, the user needs to enable the upgrade checkbox as shown below in Figure-6. This will help the user to NOT setup another instance of the app

IMPORTANT NOTE (Please read carefully before updating the App):

Due to a documented issue in the original version of the ThreatScape App, there may be some duplicate data indexing present that needs to be addressed prior to upgrade. To solve this issue, the user can choose **one of the 3 approaches** listed below (**need to be implemented prior to upgrading the app**):

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

No file chosen

Upgrade app. Checking this will overwrite the app if it already exists.

The options to avoid duplicate data indexing issue (as described above) are :

Approach 1 - Scripted:

The user can achieve the same results from approach 1, by running the python script available at the link given below, just before upgrade of the ThreatScape App.

The script is available at:

https://github.com/iSIGHTPartners/iSIGHT-connectors/blob/master/Splunk%20Upgrade/splunk_pre_upgrade.py

Note: This script execution is a one time activity for the release 1.1 and will not be needed for future releases.

Approach 2 - Manual:

Go to splunk app local directory (\$SPLUNK_HOME/etc/apps/iSIGHTPartners_App/local).

Open file iSIGHTPartners_ThreatScape_App.conf file.

At the end of file, paste the lines mentioned below:

```
[isight_iocs]
delay = <copy this value from $SPLUNK_HOME/etc/apps/iSIGHTPartners_App/bin/isight_iocs.conf>
last_exec = <copy this value from $SPLUNK_HOME/etc/apps/iSIGHTPartners_App/bin/isight_iocs.conf>

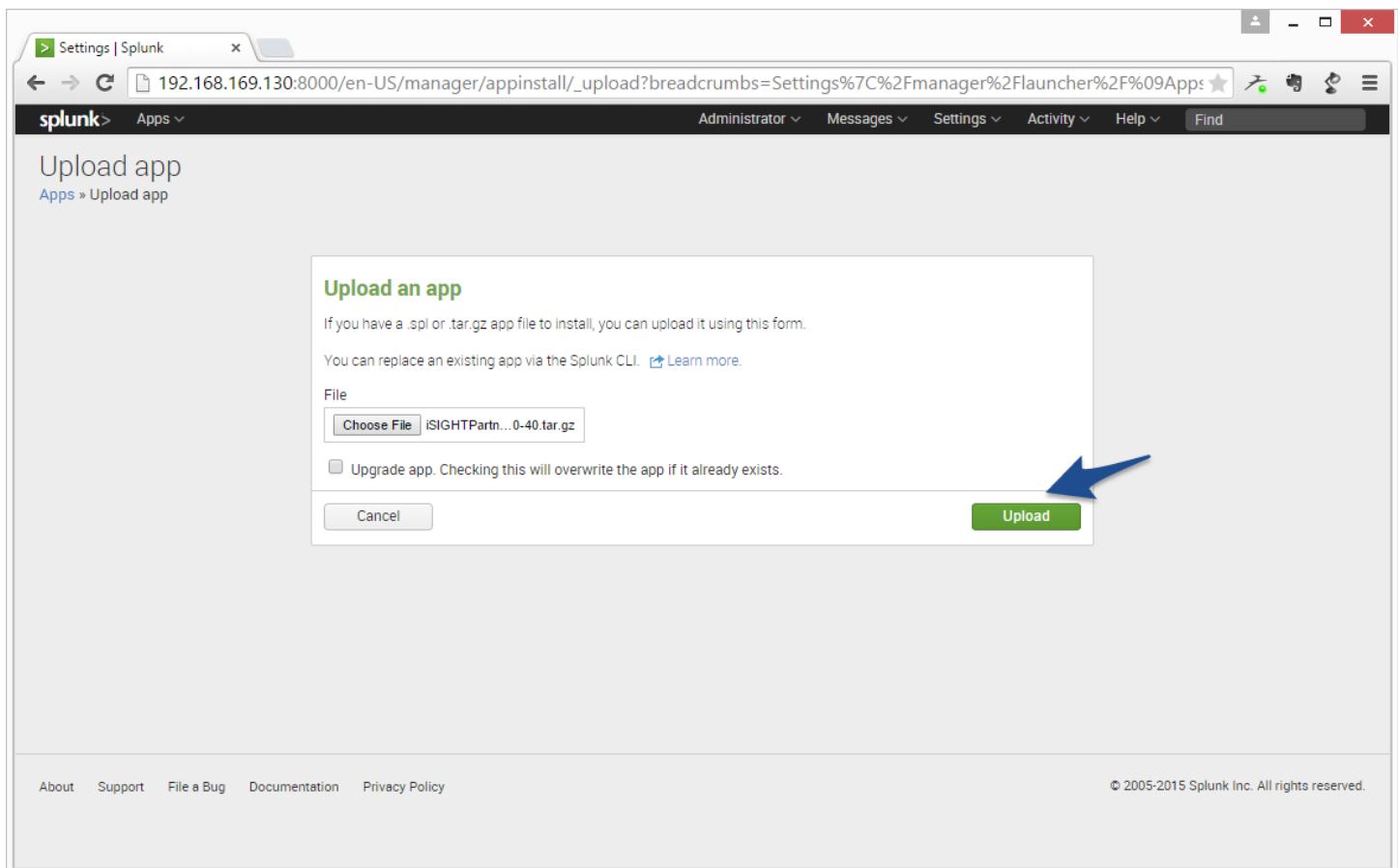
[isight_indicators]
last_exec = <copy this value from
$SPLUNK_HOME/etc/apps/iSIGHTPartners_App/bin/isight_indicators.conf>
delay = <copy this value from $SPLUNK_HOME/etc/apps/iSIGHTPartners_App/bin/isight_indicators.conf>
```

Remove all files from bin directory(\$SPLUNK_HOME/etc/apps/iSIGHTPartners_App/bin/).

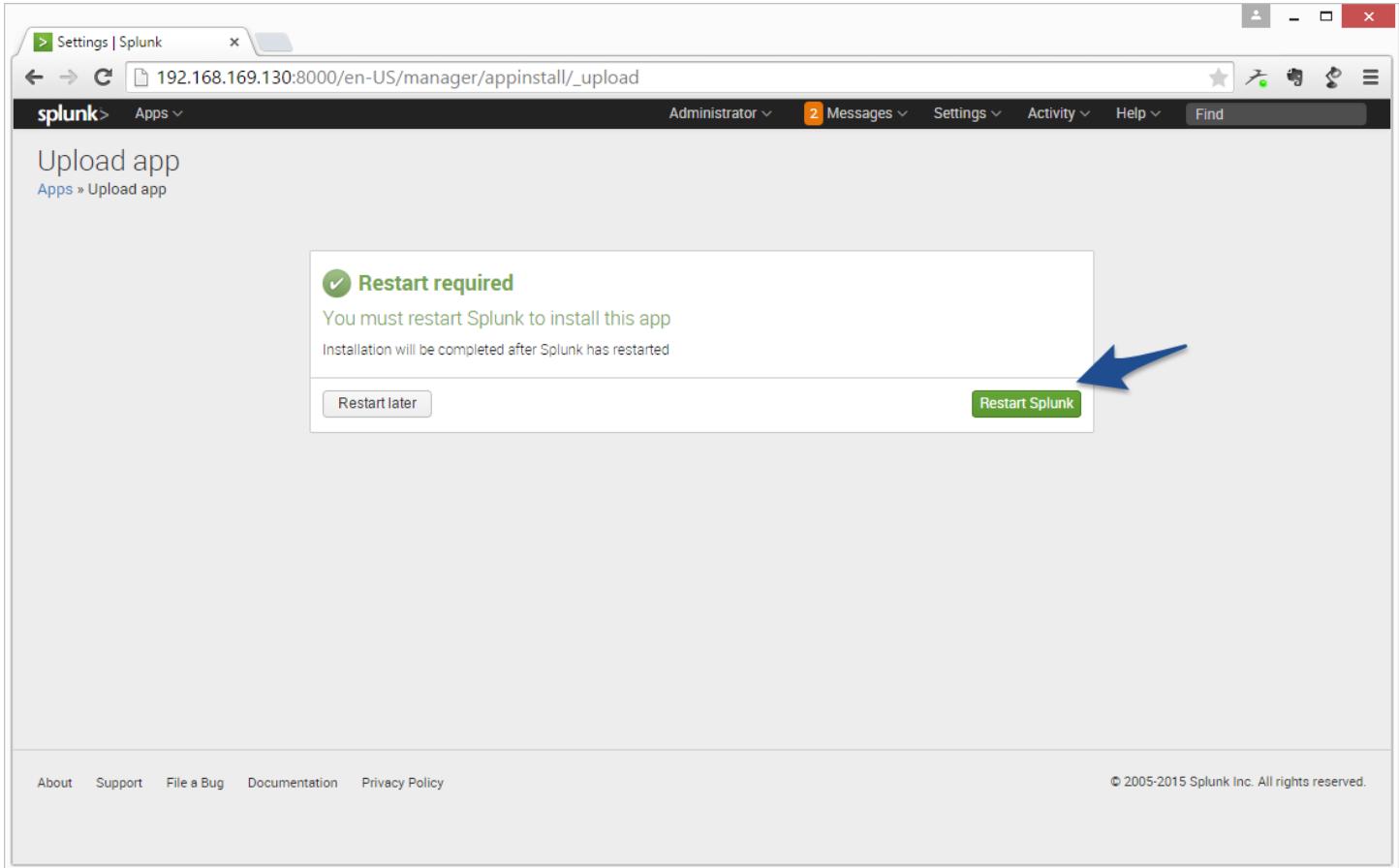
Approach 3 (uninstall before upgrade):

The above steps can be avoided by completely uninstalling the ThreatScape App and indexes and reinstalling the new version.

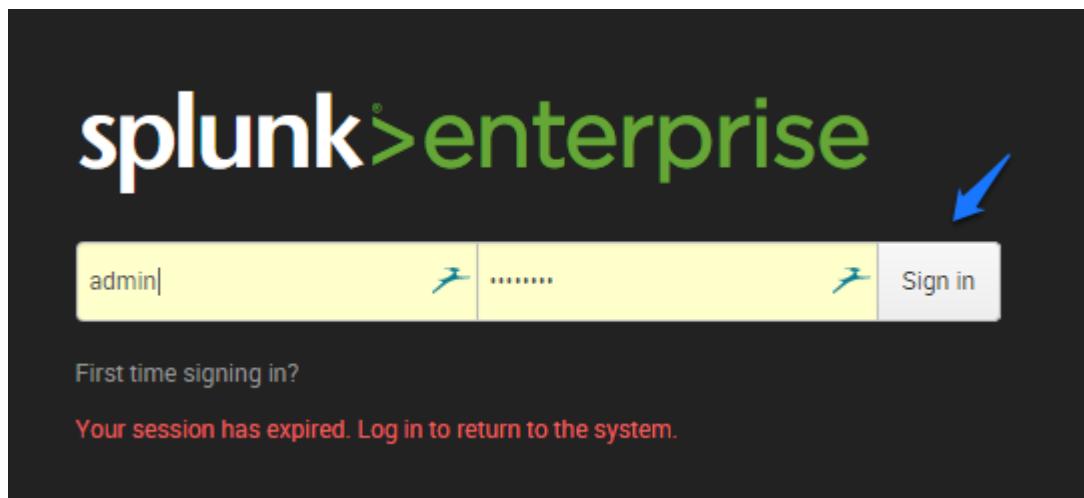
5. Select the button labeled "Upload."



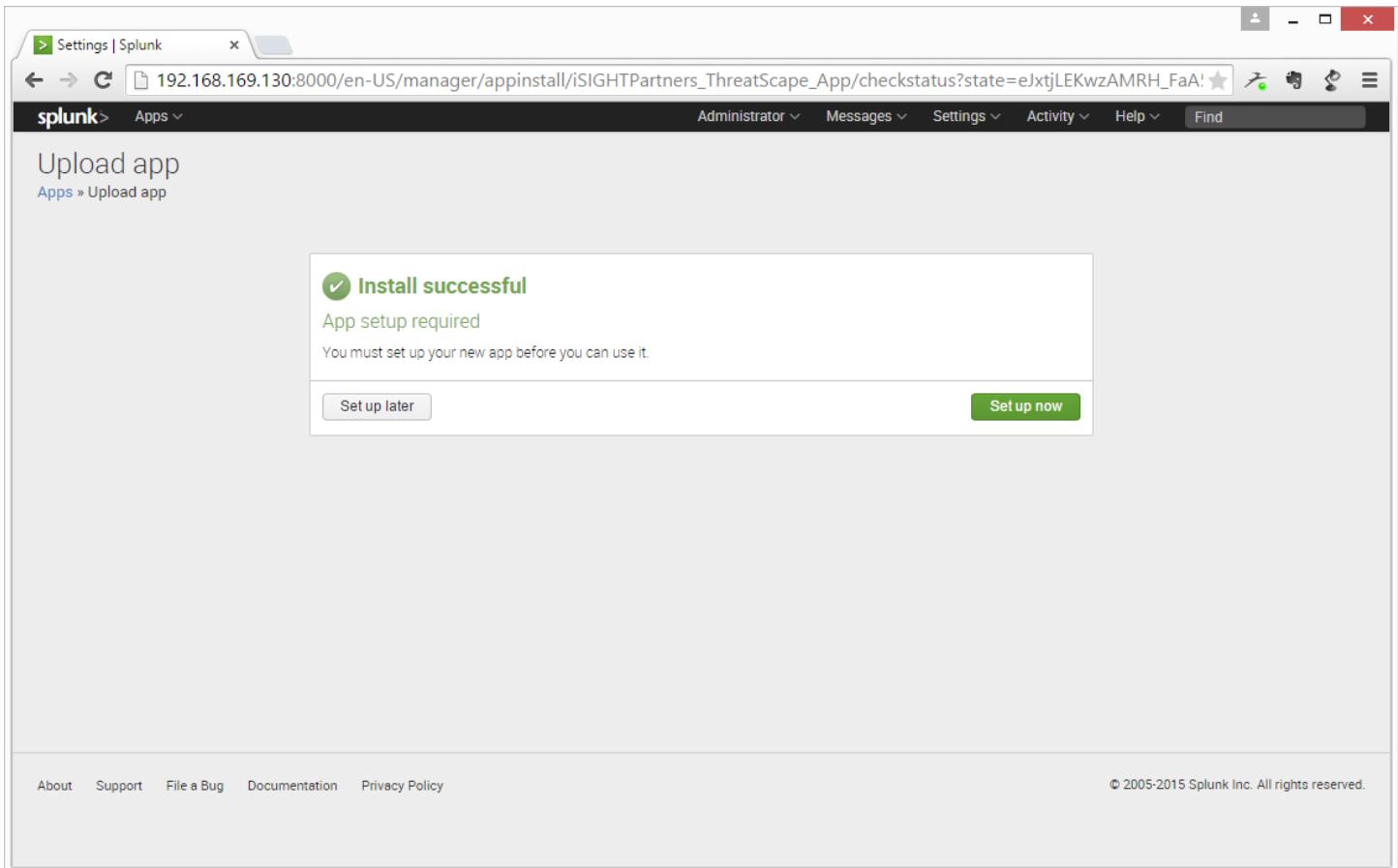
6. The ThreatScape App for Splunk is now installed! Select the button labeled "Restart Splunk."



7. And log back into Splunk.



8. A message is displayed that the ThreatScape App for Splunk has been installed. Select the button labeled "Set up now" to configure the ThreatScape App for Splunk.



Configuration

Configuration is required to allow the ThreatScape App for Splunk to retrieve ThreatScape API data. The following steps walk through the configuration process:

1. Copy and paste the Public API key (1) and the Private API key (2) into the respective fields. These keys are available with a subscription to the ThreatScape API and can be obtained from the account's customer engagement representative.
2. Enter the date from which you would like to retrieve indicators. This can be as far back as the API Keys subscription date.
3. Select the desired indicator feeds (IOCs, I&Ws and Vulnerabilities) available via the API. We recommend that you avoid duplicate data by selecting EITHER I&Ws (most suitable for researchers) OR the IOCs (most suitable for SOC operators because there will be fewer false positives, as these indicators are verified as having been used in an attack or a campaign). **If both feeds are selected to be retrieved, then while performing search, duplicate results can be avoided by specifying the appropriate source type ("isight_indicators" and "isight_iocs," respectively) within Splunk searches.**
4. Enable proxy server if the user needs to use the proxy for Threatscape API Communications by splunk. User needs to provide the proxy details by filling in the values of "Proxy host", "Proxy port", "Proxy user" and "Proxy password".
5. Select the button labeled "Save" to save the configuration options.

Welcome to the iSIGHT Partners ThreatScape® App for Splunk

The ThreatScape App for Splunk integrates ThreatScape intelligence - the most comprehensive, contextually rich, and actionable cyber threat intelligence available – into your Splunk instance. To realize the benefits of this integration, you will need both a public and private API key to enter into the fields below. If you would like more information on how you can integrate ThreatScape API data into Splunk, please visit here: <http://www.isightpartners.com/act-today/request-consultation/>

ThreatScape API Settings

Public Key

1

Private Key

1

Retrieve indicators from (mm/dd/yyyy)

2

Indicators and Warnings

Enable

Indicators of Compromise

Enable

Vulnerability Feed

Enable

Enable Proxy

Enable Proxy Server

Proxy Host

*Enter Proxy Host IP Address

3

Proxy Port

*Enter Proxy Port Number

4

Proxy User

(Optional) Enter Proxy User Name

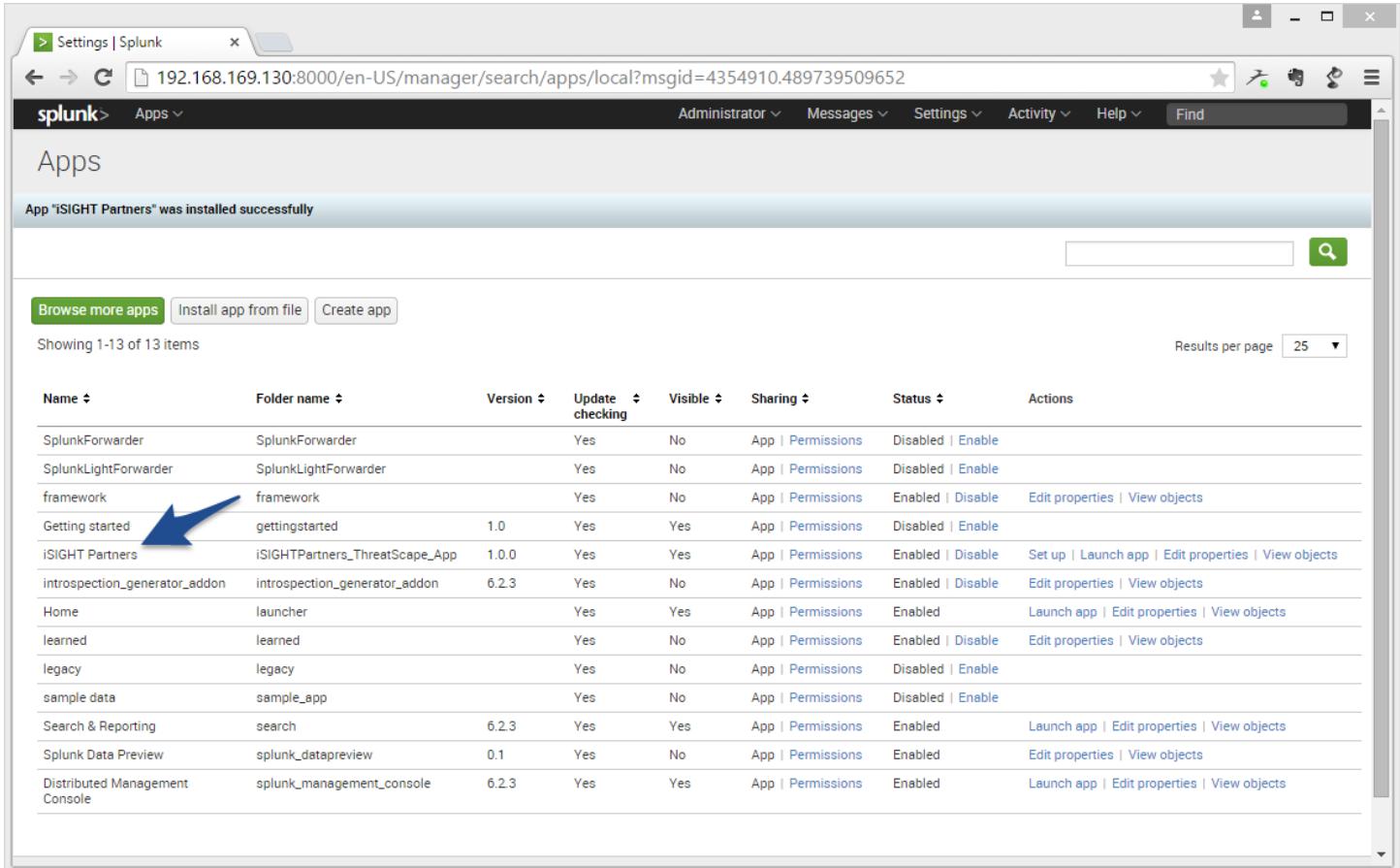
Proxy Pass

(Optional) Enter Proxy Password

Confirm password

5

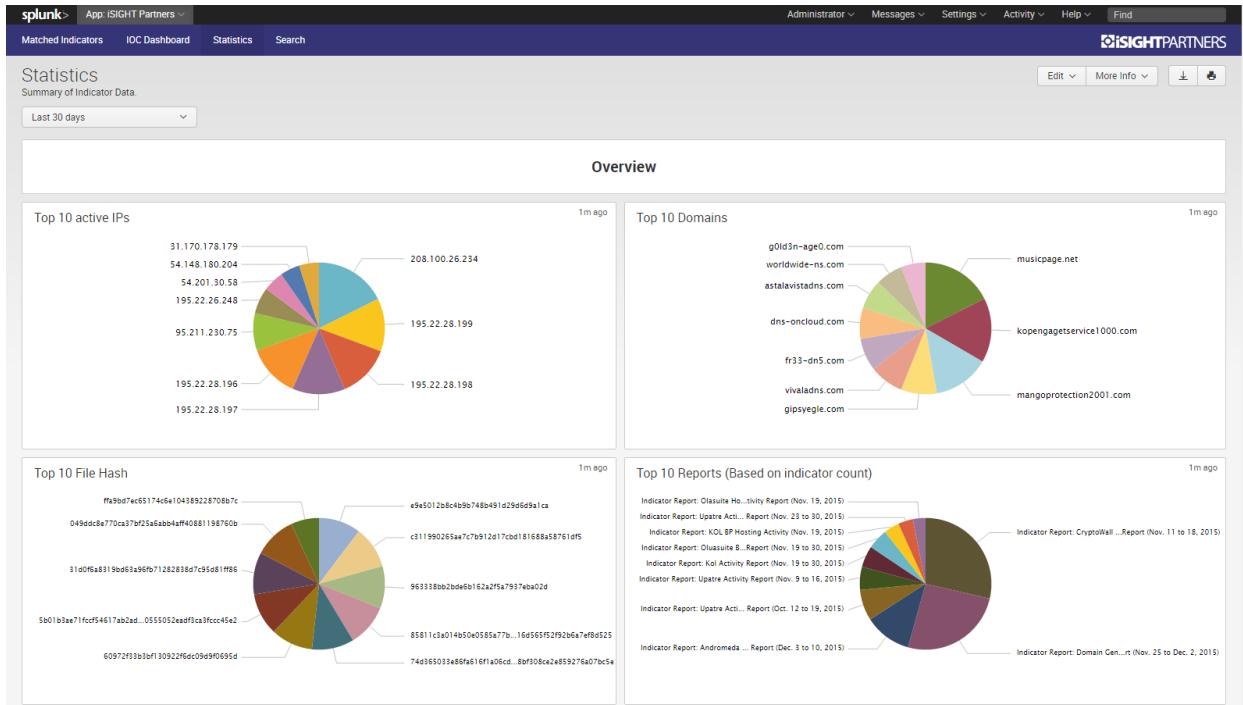
6. Validate that the ThreatScape App for Splunk installed and is enabled.



The screenshot shows the Splunk Apps interface. At the top, there is a message: "App 'iSIGHT Partners' was installed successfully". Below this, there are buttons for "Browse more apps", "Install app from file", and "Create app". A search bar is also present. The main area displays a table of installed apps, with 13 items shown per page. The table columns include Name, Folder name, Version, Update checking, Visible, Sharing, Status, and Actions. A blue arrow points to the "Getting started" row, which corresponds to the iSIGHT Partners app. The "Status" column for this row shows "Enabled | Enable".

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
framework	framework		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Getting started	gettingstarted	1.0	Yes	Yes	App Permissions	Disabled Enable	
iSIGHT Partners	iSIGHTPartners_ThreatScape_App	1.0.0	Yes	Yes	App Permissions	Enabled Disable	Set up Launch app Edit properties View objects
introspection_generatorAddon	introspection_generatorAddon	6.2.3	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
legacy	legacy		Yes	No	App Permissions	Disabled Enable	
sample data	sample_app		Yes	No	App Permissions	Disabled Enable	
Search & Reporting	search	6.2.3	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Splunk Data Preview	splunk_datapreview	0.1	Yes	No	App Permissions	Enabled	Edit properties View objects
Distributed Management Console	splunk_management_console	6.2.3	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects

7. Navigate to the ThreatScape App for Splunk dashboard and verify that API data is being retrieved.



8. It is also a good idea to make sure that the ThreatScape API data is available to be used in searches. This can be accomplished by pressing the "Search" menu option and executing a simple search (For example: `index=isightpartners (sourcetype="isight_indicators") |table, _time, reportId, title, webLink, sourcetype, ThreatScape, ip, networkIdentifier, productType`). The return should look something like this:

_time	reportId	title	webLink	sourcetype	ThreatScape	ip	networkIdentifier	productType
2015-12-15 18:21:00	15-00014406	Indicator Report: Madness Activity Report (Dec. 8 to 15, 2015)	https://mysight.isightpartners.com/report/full/15-00014406	isight_indicators	Cyber Crime	null	Attacker	MAL
2015-12-15 18:21:00	15-00014406	Indicator Report: Madness Activity Report (Dec. 8 to 15, 2015)	https://mysight.isightpartners.com/report/full/15-00014406	isight_indicators	Cyber Crime	31.170.162.63	Attacker	MAL
2015-12-15 18:21:00	15-00014406	Indicator Report: Madness Activity Report (Dec. 8 to 15, 2015)	https://mysight.isightpartners.com/report/full/15-00014406	isight_indicators	Cyber Crime	81.177.6.12	Attacker	MAL
2015-12-15 18:21:00	15-00014406	Indicator Report: Madness Activity Report (Dec. 8 to 15, 2015)	https://mysight.isightpartners.com/report/full/15-00014406	isight_indicators	Cyber Crime	104.219.248.47	Attacker	MAL
2015-12-15 18:21:00	15-00014406	Indicator Report: Madness Activity Report (Dec. 8 to 15, 2015)	https://mysight.isightpartners.com/report/full/15-00014406	isight_indicators	Cyber Crime	144.76.192.128	Attacker	MAL
2015-12-15 18:21:00	15-00014406	Indicator Report: Madness Activity Report (Dec. 8 to 15, 2015)	https://mysight.isightpartners.com/report/full/15-00014406	isight_indicators	Cyber Crime	null	Attacker	MAL
2015-12-15 18:21:00	15-00014406	Indicator Report: Madness Activity Report (Dec. 8 to 15, 2015)	https://mysight.isightpartners.com/report/full/15-00014406	isight_indicators	Cyber Crime	31.170.161.236	Attacker	MAL
2015-12-15 18:21:00	15-00014406	Indicator Report: Madness Activity Report (Dec. 8 to 15, 2015)	https://mysight.isightpartners.com/report/full/15-00014406	isight_indicators	Cyber Crime	null	Attacker	MAL
2015-12-15 15:14:00	15-00014320	LATENTBOT Malware: Introduction and Indicators of Compromise	https://mysight.isightpartners.com/report/full/15-00014320	isight_indicators	Cyber Crime	null	Compromised	FINTEL
2015-12-15 15:14:00	15-00014320	LATENTBOT Malware: Introduction and Indicators of Compromise	https://mysight.isightpartners.com/report/full/15-00014320	isight_indicators	Cyber Crime	null	null	FINTEL
2015-12-15 15:14:00	15-00014320	LATENTBOT Malware: Introduction and Indicators of Compromise	https://mysight.isightpartners.com/report/full/15-00014320	isight_indicators	Cyber Crime	null	Compromised	FINTEL
2015-12-15 15:14:00	15-00014320	LATENTBOT Malware: Introduction and Indicators of Compromise	https://mysight.isightpartners.com/report/full/15-00014320	isight_indicators	Cyber Crime	null	Compromised	FINTEL
2015-12-15 15:14:00	15-00014320	LATENTBOT Malware: Introduction and Indicators of Compromise	https://mysight.isightpartners.com/report/full/15-00014320	isight_indicators	Cyber Crime	83.175.125.150	Compromised	FINTEL
2015-12-15 15:14:00	15-	LATENTBOT Malware: Introduction and Indicators of Compromise	https://mysight.isightpartners.com/report/full/15-	isight_indicators	Cyber Crime	null	Compromised	FINTEL