ACTI Add-ON For Splunk  
Accenture Cyber Threat Intelligence

Accenture Security

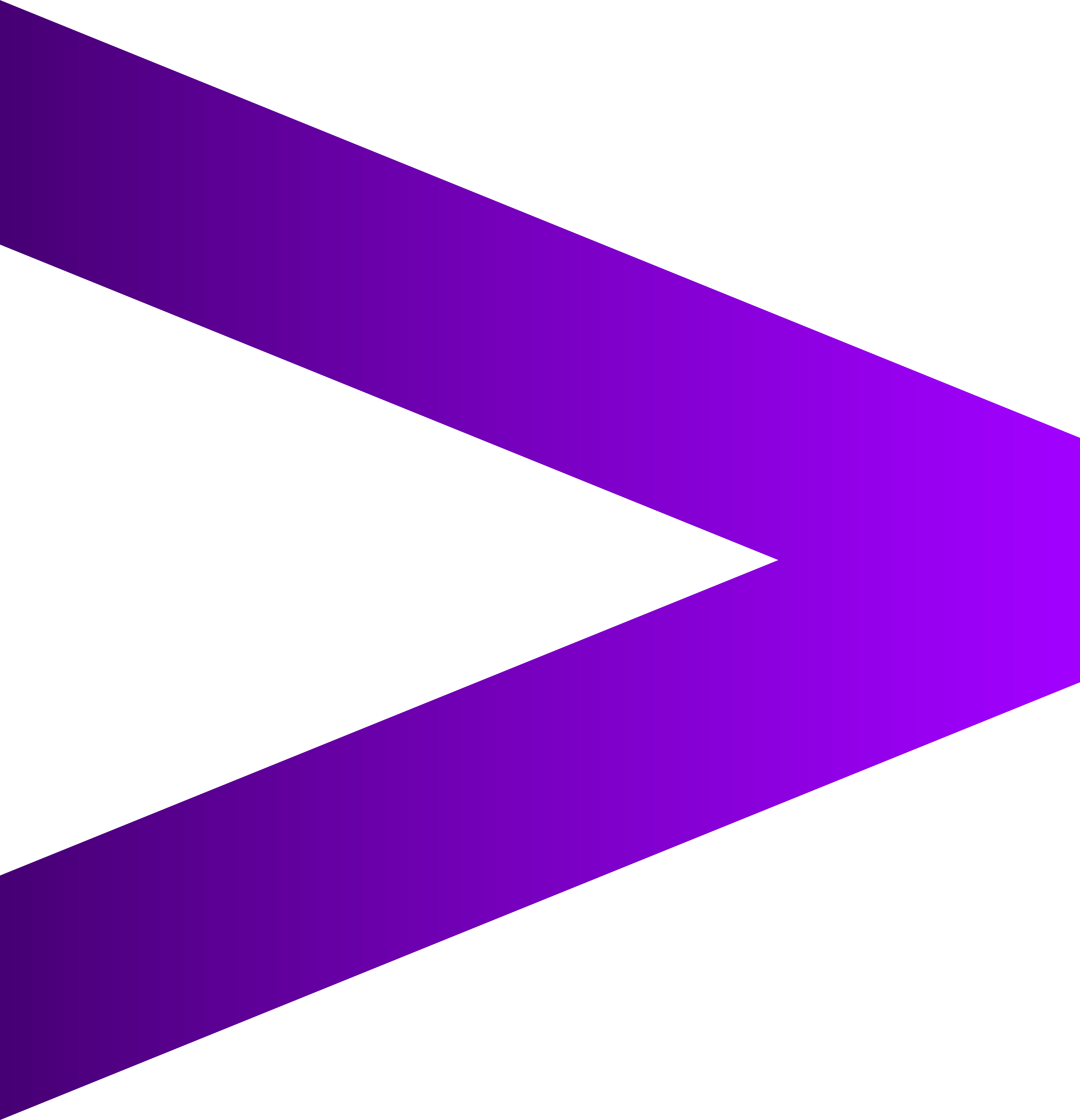


Table of Contents

[About 3](#_Toc103078073)

[Requirements 3](#_Toc103078074)

[Installation and Configuration 3](#_Toc103078075)

[Installation 3](#_Toc103078076)

[Manually Load Historical Threat Intelligence 6](#_Toc103078077)

[Change Intelligence Download Frequency 6](#_Toc103078078)

[Adding Accenture CTI Notable Review Fields to Splunk ES 7](#_Toc103078079)

[Configure Threat Intelligence Retention 8](#_Toc103078080)

[Contents 9](#_Toc103078081)

[Threat Intelligence KV Store 9](#_Toc103078082)

[Macros for Data Enrichment 10](#_Toc103078083)

[Adaptive Response Action: Accenture CTI Indicator Query 11](#_Toc103078084)

[Accenture CTI Integration Health Check Dashboard 13](#_Toc103078085)

[Correlation Search/Alert: iDefense Threat Match 14](#_Toc103078086)

[Troubleshooting 15](#_Toc103078087)

[Where to find the Logs for this Add-On 15](#_Toc103078088)

[Changing Log Level 16](#_Toc103078089)

[Health Check Dashboard 17](#_Toc103078090)

[Splunk Mission Control 17](#_Toc103078091)

[Getting the add-on ready for Splunk Mission Control 17](#_Toc103078092)

Copyright © 2018 Accenture

All rights reserved.

## About

The iDefense Technology Add-on provides an easy way to interact with iDefense IntelGraph API by loading threat indicators and vulnerabilities into dedicated KV Stores and 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 |
| 3.3.0 | 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 for the TA to load Threat Indicators.
* The customer must have a subscription to the Vulnerability API for the TA to load Vulnerabilites.
* The customer should 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](https://intelgraph.idefense.com/#/user/view/). The token must have at least the "iGraph Read API Threat Indicator" role.
* Install the add-on from [Splunkbase](https://splunkbase.splunk.com/app/4508/) into the Splunk Search Head containing Splunk ES.
* Once installed, click on the "Apps" drop-down menu, then on the iDefense Intelgraph Add-On.

Graphical user interface, application

Description automatically generated

* Then click on Continue to App Setup Page.

Graphical user interface, text, application

Description automatically generated

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

Graphical user interface, text, application, website

Description automatically generated

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

Graphical user interface, text, application

Description automatically generated

* 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.

A picture containing text, screenshot, monitor, screen

Description automatically generated

### 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)
5. ACTI-get\_vulnerability(ALL)

Graphical user interface, website

Description automatically generated

### 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.

Graphical user interface, application, Teams

Description automatically generated

* 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.

Graphical user interface, application, Teams

Description automatically generated

* 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.

Table

Description automatically generated

### 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
* acti\_vulnerability

|  |  |  |
| --- | --- | --- |
| Field | Type | Description |
| type | string | Denotes indicator type (IP, Domain or URL). |
| uuid | strting | The UUID for the indicator in IntelGraph. |
| 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 | number | 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](https://dev.splunk.com/enterprise/docs/devtools/enterprisesecurity/threatintelligenceframework/) 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:

Graphical user interface, application

Description automatically generated

### Adaptive Response Action: Accenture CTI Indicator Query

The add-on also includes a custom adaptive response action called **Accenture CTI Indicator Query** that allows one to ad-hoc query for indicators. The adaptive response action is integrated with Splunk Enterprise Security and can be used while working with notables.

Example:

Following is a notable in Splunk ES:

Graphical user interface, application

Description automatically generated

* One can click on the “Accenuture CTI Indicator Query” response action.
* Then Query for desired indicators in the notable event:

Graphical user interface, application

Description automatically generated

* The result can be viewed by clicking on the Adaptive Response Invocation history section.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, Teams

Description automatically generated

### 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:

A picture containing text, screenshot, monitor, screen

Description automatically generated

### 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:

Graphical user interface, text, application, email

Description automatically generated

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:

Graphical user interface, text, application

Description automatically generated

## 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.

Graphical user interface, text, application

Description automatically generated

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

Graphical user interface, text, application, email

Description automatically generated

### 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](https://alm.accenture.com/wiki/display/CTI/Splunk+Technical+Add-On+for+iDefense#SplunkTechnicalAddOnforiDefense-AccentureCTIIntegrationHealthCheckDashboard) 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.