Kaspersky Add-on for Splunk Documentation

Release 0.1.3

Diogo Silva

Mar 23, 2023

Contents:

CHAPTER 1

Release Notes

1.1 v0.1.4 - April 2020

- App compatibility changed to starting from 7.1.0 due to app.manifest version and Splunk Cloud compatibility
- Improved CIM Change datamodel coverage
- Improved CIM Malware datamodel coverage
- Added missing extractions of signature field for several sourcetypes

1.2 v0.1.3 - October 2019

- Fix issue with the events timezone detection

LEEF format outputs a timestamp in UTC and splunk was detecing it as system default resulting in events in the future for systems in GMT- and in the past for systems in GMT+

1.3 v0.1.2 - September 2019

- Small fixes
- Improvements on some extractions

1.4 v0.1.0 - August 2019

- Public release to Splunkbase

CHAPTER 2

Requirements

- Kaspersky Security Center 10 or newer
- Splunk 7.0 or newer

CHAPTER 3

Installation

3.1 Install the Kaspersky Add-on for Splunk

- Get the Kaspersky Add-on for Splunk by downloading it from Splunkbase or browsing to it using the app browser within Splunk Web.
- Determine where and how to install this add-on in your deployment, using the tables on this page.
- Perform any prerequisite steps before installing, if required and specified in the tables below.
- Complete your installation.

3.1.1 Distributed deployments

Reference the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise or any deployment for which you are using forwarders to get your data in. Depending on your environment, your preferences, and the requirements of the add-on, you may need to install the add-on in multiple places.

Where to install this add-on

Unless otherwise noted, all supported add-ons can be safely installed to all tiers of a distributed Splunk platform deployment. See Where to install Splunk add-ons in Splunk Add-ons for more information.

This table provides a reference for installing this specific add-on to a distributed deployment of Splunk Enterprise.

Splunk platform component	Supported	Required	Comments
Search Heads	Yes	Yes	Install this add-on to all search heads.
Indexers	Yes	Optional	Required for the parsing operations (sourcetype renaming) if the data is not coming from a heavy forwarder.
Heavy Forwarders	Yes	Optional	Required for the parsing operations (sourcetype renaming).
Universal Forwarders	Yes	Optional	

Distributed deployment compatibility

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features.

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality.
Indexer Clusters	Yes	
Deployment Server	Yes	Supported for deploying via Deployment server.

3.1.2 Installation walkthroughs

The Splunk Add-Ons manual includes an Installing add-ons guide that helps you successfully install any add-on to your Splunk platform. For a walkthrough of the installation procedure, follow the link that matches your deployment scenario:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud

CHAPTER 4

Troubleshooting

4.1 The timestamp in the data is wrong

Kaspersky LEEF format outputs the timestamp in UTC. In the Add-on versions <=0.1.2 the time zone setting was not set explicitly in props, so splunk was assuming system default time. The result was events showing up in the future for systems in GMT- and in the past for systems in GMT+.

CHAPTER 5

Support

5.1 Bugs & Support Issues

You can file bug reports on our GitHub issue tracker, and they will be addressed as soon as possible. **Support is a volunteer effort**, and there is no guaranteed response time.

CHAPTER 6

Indices and tables

- genindex
- modindex
- search