CEF Add on for Splunk Documentation

Ryan Faircloth/Splunk Inc.

Apr 23, 2019

Contents:

This add on implements the foundations for proper parsing of ArchSight's CEF format. Modular add ons or extensions can be created. The first one created using this framework is "CEF Microsoft Windows Add on for Splunk"

CHAPTER 1

Requirements

This add on has index time extractions and must be installed on the indexer or heavy forwarder

- Splunk Enterprise 7.1 or newer
- Splunk Common Information Model 4.11 or newer

CHAPTER 2

Installation

- Install the add on on each indexer and heavy forwarder
- Install the add on on each search head applicable
- Configure inputs - For “syslog” format event use sourcetype=cef:syslog - For “plain” format without a syslog header use sourcetype=cef:file

CHAPTER 3

Validation

- Search an expected to contain events
- Validate the sourcetype is “cef” NOT “cef:file” or “cef:syslog” if so this indicates the add on has not been properly deployed to the indexers or heavy forwarders
- Validate the following indexed field have values - cef_device_vendor - cef_device_product - cef_device_version

CHAPTER 4

Next Steps

This add on provides support for ArcSight as a Vendor product and can be extended for additional products. Review the bitbucket project for additional existing add ons or use one of the existing add ons as a model to develop your own.

Development of connector specific CEF add ons should be accomplished as bespoke add ons for Splunk. Utilizing a transform that will be processed after `TRANSFORMS-bheader` and before `TRANSFORMS-zzzstrip` (associated to `cef:file` and `cef:syslog` in `props.conf`. Set the `source::` meta data as required and define all additional knowledge objects using `source::<newsource>` in `props.conf`. All common CEF fields will be extracted and aliased based on the `[cef]` source type.

CHAPTER 5

Indices and tables

- genindex
- modindex
- search