CEF Microsoft Windows Add on for Splunk Documentation

Ryan Faircloth/Splunk Inc

Jan 08, 2019

Contents:

This add on implements the foundations for Microsoft Windows when processed by the ArcSight connector into CEF format. For events available and provided in samples/* CIM compliance appears to be valid. Using CEF as an intermediary requires acceptance of the risk incorrect mapping by the connector can not be detected after the fact using raw. What you see is what you get.

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
- CEF add on for Splunk 0.1.1 or newer
- Splunk TA Windows 5.0.1 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 from Microsoft Windows
- Verify for the sourcetype “cef” source “CEFEventlog:*” can be found

CHAPTER 4

Next Steps

Review event data and validate the adequacy of the data and CIM mapping to support your use case

CHAPTER 5

Indices and tables

- genindex
- modindex
- search