SECRET VISONS

Technology Add-on for HP ArcSight CEF data inputs

Release Notes

Version 2.2.0

Yan Wen

Digitally signed by Yan Wen
Date: 2018.06.06 00:06:20 +10'00'

Publish Date: 06/06/2018

Legal Notices

License

The Technology Add-on for HP ArcSight CEF data inputs is open source add-on developed by Secret Visons under GNU General Public License v3.0. The users may use this software for both private and commercial usages free of charge. The developers may modify the software and redistribute the modification version of the application, but the developers should NOT remove the information of the original authors, NOR should the developers change the license conditions for commercial activities.

Warranty

The current version of Technology Add-on for HP ArcSight CEF data inputs is certified by Splunk and does NOT contain any malicious code which may impact the Splunk environment, including the Splunk application, the backbone infrastructure and the stored data. However, based on the GNU General Public License v3.0 agreement, Secret Visons do not hold any public liability of this product, nor should provide any warranty.

Support Information

Currently, Secret Visons provide the community support for the Technology Add-on for HP ArcSight CEF data inputs, while the Splunk Cloud deployment is also under community support.

If you encountered any issue or have any question, please feel free to contact the support (support@secretvisons.com), or send the emails to the author (rockey@secretvisons.com), or you can raise the tickets via GitHub (https://github.com/SecretVisons/Splunk_ArcSight).

Revision History

Version	Date	Author	Summary
1.0	April 28, 2018	Yan (Rockey) Wen	Release notes for Splunk_SA_cefinput version 2.0.0.
1.1	May 06, 2018	Yan (Rockey) Wen	Release notes for Splunk_SA_cefinput version 2.0.1.
1.2	May 21, 2018	Yan (Rockey) Wen	Release notes for Splunk_SA_cefinput version 2.0.2.
1.3	May 21, 2018	Yan (Rockey) Wen	Release notes for Splunk_SA_cefinput version 2.1.0.
1.4	June 5, 2018	Yan (Rockey) Wen	Release notes for TA-ArcSightCEF_datainputs version 2.2.0.

Contents

Change History

Content Changes

The following table lists the changes have been made in the current release (version 2.2.0):

File path	File Name	Summary
Splunk_SA_cefinput/	README	Updated to reflect the changes in version 2.2.0.
	LICENSE	License statement of GNU General Public License version 3.0, introduced in version 2.2.0
	app.manifest	Manifest file generated by the Splunk Package Toolkit. Introduced in version 2.2.0
Splunk_SA_cefinput/default	app.conf	Updated to reflect the changes in version 2.2.0.
	props.conf	Updated the sections for field extractions and fixed the optional field alias in version 2.2.0.
	transforms.conf	Updated the sections for field extractions and fixed the optional field alias in version 2.2.0.
Splunk_SA_cefinput/docs	CHANGES.LOG	Updated in version 2.2.0. Brief summary of the change histories
	REFERENCES	Updated in version 2.2.0. Listed of the reference documents and URLs.
Splunk_SA_cefinput/metadata	default.meta	No change in current version.
Splunk_SA_cefinput/static	appIcon.png	No change in current version.
	appIcon_2x.png	No change in current version.
	appLogo.png	No change in current version.
	appLogo_2x.png	No change in current version.

Support Changes

The following table lists the support details between different versions of the Splunk support add-on (SA) for ArcSight Common Event Format (CEF) input:

App Version	Splunk Enterprise (on premise or public clouds)	Splunk Cloud
1.0.0	6.5.x, 6.6.x	-
2.0.0	6.5.x, 6.6.x, 7.0.x, 7.1.x	Experimental
2.0.1	6.5.x, 6.6.x, 7.0.x, 7.1.x	Yes
2.0.2	6.5.x, 6.6.x, 7.0.x, 7.1.x	Yes
2.1.0	7.0.x, 7.1.x	Yes
2.2.0	7.0.x, 7.1.x	Yes

New Features

New features in the current version

There no new feature introduced in the current version (version 2.2.0).

New features in the previous version

The following new features have been introduced in the previous versions:

1. The following new features have been introduced in the current version (version 2.1.0):
    - Dynamic field extractions of the additional fields [ad.someFieldName], [ad.Key[{number}], and [ad.fieldNameWithSpecialCharacters];
    - Allow the tow device custom fields (e.g., cs1 and cs1Label) merge into new fields based on the values of the original fields
2. Extended the field extractions of the following fields which are not the common fields across three main ArcSight ingestion platforms and were not included in version 2.0.0:
    - catdt
    - categorySignificance
    - categoryBehavior
    - categoryDeviceGroup
    - categoryTechnique
    - categoryOutcome
    - categoryObject
    - deviceSeverity
3. The rule-based field extraction functions have been implemented tested and verified. The configuration samples have been provided in the samples.
4. Extended the field extractions of the following fields which are not the common fields across three main ArcSight ingestion platforms and were not included in version 1.0.0:
    - eventAnnotationStageUpdateTime
    - eventAnnotationModificationTime
    - eventAnnotationAuditTrail
    - eventAnnotationVersion
    - eventAnnotationFlags
    - eventAnnotationEndTime
    - eventAnnotationManagerReceiptTime
    - cefVer
    - locality
5. Added the full names of the ArcSight CEF fields which only have the key names available in the version 1.0.0:
    - act (deviceAction)
    - app (applicationProtocol)
    - c6a1 (deviceCustomIPv6Address1)
    - c6a1Label (deviceCustomIPv6Address1Label)
    - c6a2 (deviceCustomIPv6Address2)
    - c6a2Label (deviceCustomIPv6Address2Label)
    - c6a3 (deviceCustomIPv6Address3)
    - c6a3Label (deviceCustomIPv6Address3Label)
    - c6a4 (deviceCustomIPv6Address4)
    - c6a4Label (deviceCustomIPv6Address4Label)

- cat (deviceEventCategory)
- cfp1 (deviceCustomFloatingPoint1)
- cfp1Label (deviceCustomFloatingPoint1Label)
- cfp2 (deviceCustomFloatingPoint2)
- cfp2Label (deviceCustomFloatingPoint2Label)
- cfp3 (deviceCustomFloatingPoint3)
- cfp3Label (deviceCustomFloatingPoint3Label)
- cfp4 (deviceCustomFloatingPoint4)
- cfp4Label (deviceCustomFloatingPoint4Label)
- cn1 (deviceCustomNumber1)
- cn1Label (deviceCustomNumber1Label)
- cn2 (deviceCustomNumber2)
- cn2Label (deviceCustomNumber2Label)
- cn3 (deviceCustomNumber3)
- cn3Label (deviceCustomNumber3Label)
- cnt (baseEventCount)
- cs1 (deviceCustomString1)
- cs1Label (deviceCustomString1Label)
- cs2 (deviceCustomString2)
- cs2Label (deviceCustomString2Label)
- cs3 (deviceCustomString3)
- cs3Label (deviceCustomString3Label)
- cs4 (deviceCustomString4)
- cs4Label (deviceCustomString4Label)
- cs5 (deviceCustomString5)
- cs5Label (deviceCustomString5Label)
- cs6 (deviceCustomString6)
- cs6Label (deviceCustomString6Label)
- dhost (destinationHostName)
- dmac (destinationMacAddress)
- dntdom (destinationNtDomain)
- dpid (destinationProcessId)
- dpriv (destinationUserPrivileges)
- dproc (destinationProcessName)
- dpt (destinationPort)
- dst (destinationAddress)
- dtz (deviceTimeZone)
- duid (destinationUserId)
- duser (destinationUserName)
- dvc (deviceAddress)
- dvchost (deviceHostName)
- dvcmac (deviceMacAddress)
- dvcpid (deviceProcessId)
- end (endTime)
- fname (filename)
- fileSize (fileSize)

- in (bytesIn)
- msg (message)
- out (bytesOut)
- outcome (eventOutcome)
- proto (transportProtocol)
- reason (Reason)
- request (requestUrl)
- rt (deviceReceiptTime)
- shost (sourceHostName)
- smac (sourceMacAddress)
- sntdom (sourceNtDomain)
- spid (sourceProcessId)
- spriv (sourceUserPrivileges)
- sproc (sourceProcessName)
- spt (sourcePort)
- src (sourceAddress)
- start (startTime)
- suid (sourceUserId)
- suser (sourceUserName)
- agt (agentAddress)
- ahost (agentHostName)
- aid (agentId)
- amac (agentMacAddress)
- art (agentReceiptTime)
- at (agentType)
- atz (agentTimeZone)
- av (agentVersion)
- dlat (destinationGeoLatitude)
- dlong (destinationGeoLongitude)
- slat (sourceGeoLatitude)
- slong (sourceGeoLongitude)

6. Merge the values from custom field label and the custom fields to form new fields, as well as keep the custom field labels and the custom fields separately at the same time.
7. Dynamically extract the additional ArcSight device fields (ad.someFieldName) similar below:

```
ad.Key[2]=krbtgt/AU ad.WindowsKeyMapFamily=Windows 2003 R2|2003|XP
ad.EventIndex=1551624412 ad.Key[5]=0 ad.Key[0]=acoe_wpaas_epo_rd
ad.WindowsParserFamily=Windows 2003 R2|2003|XP ad.Key[6]=::ffff:10.231.65.57
ad.Key[1]=S-1-5-21-1229272821-1123561945-839522115-670269 ad.Key[3]=0x40810010
ad.Key[4]=0x12 ad.Key[9]= ad.Key[8]= ad.Key[7]=61893 ad.Key[10]=
ad.WindowsVersion=Windows Server 2003 R2
```

Configuration Changes

Configuration changes in the current version

Configuration Changes in version 2.2.0

The following changes have been implemented in version 2.2.0:

- Renamed the app folder from Splunk_SA_cefinput to TA-ArcSightCEF_datainputs;
- Update the support id from Splunk_SA_cefinput to TA-ArcSightCEF_datainputs.
- Renamed the REGEX stanzas in transforms.conf with the prefix "c_" which stands for the community versions;
- Redesigned the field extractions for the standard CEF fields
- Added a few new non-standard CEF fields
- Added the non-standard CEF fields with multiple values

Configuration changes in the previous versions

Configuration Changes in version 2.1.0

The following changes have been implemented in version 2.1.0:

- Updated the REGEX in the default/transforms.conf and switch to use the basic regex modular rather than the actual regexes in each stanzas for better quality control.

Configuration Changes in version 2.0.2

The following changes have been implemented in version 2.0.2:

- Remove the field alias with the prefix "cef_";
- Enabled the full names of the CEF fields from the key names by default;
- Removed the sections for the index time source renaming and simplify the implementation procedures.
- Change the add-on from visible back to invisible.

Configuration Changes in version 2.0.1

Instead of the original source base field extractions shipped by default, in the current version, the sourcetype based field extractions and source based field extractions will be both shipped by default.

Configuration changes in version 2.0.0

There are some changes to the stanza [cef_header_fields] in the transforms.conf file. The original stanza was designed to cover the normal CEF header stings as well as the ones with the Microsoft SQL server action audit group events. (Sample event below)

```
2015/12/11 17:57:06 AEDT CEF:0|Microsoft|SQL Server||LX\|LGO|LOGIN\|LOGOUT|Low|
eventId=894 externalId=33205 ……
```

However, this might reduce the performance of the field extractions and transformations as the additional REGEX matches need to run. If the users can confirm that they won't have the SQL audit action group events in ArcSight CEF format, they can switch to the alternative REGEX, which can be

found in the Technical Reference guide, Deployment guide and the sample configuration files (full_transforms.conf.sample).

Fixed issues and bugs

Bugs and issues fixed in the current release

Bug #5: Fixed the field extraction issues when some fields do not show up unless performing the extract searches by appending the strings "… | search <fieldname>=* …".

Bugs and issues fixed in the previous release

The following bug exists in the version 1.0.0 of the Splunk SA for ArcSight CEF input has been fixed in the current release:

Bug #1: Incomplete field extraction of the custom strings and flex strings when the values of the custom strings or flex strings contain the base64 encoded identifiers.

Sample event:

```
CEF:0|ArcSight|ArcSight|6.0.2.6627.0|agent:015|Device connection down|Very-High|
eventId=37350412 msg=Host Unreachable mrt=1437695604815
categorySignificance=/Informational/Error categoryBehavior=/Access/Start
categoryDeviceGroup=/Application catdt=Security Mangement categoryOutcome=/Failure
categoryObject=/Host/Application art=1437695604816 cat=/Agent/Connection/Device?Failure
deviceSeverity=Warning rt=1437695604815 dhost=database1.sample.com dst=5.5.5.5
destinationZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-
10.255.255.255 fileType=Agent cs2=<Resource ID\="3KDZG6kkBABCAA7iSgTWqfw\=\="/>
c6a4=::1 cs2Label=Configuration Resource c6a4Label=Agent IPv6 Address ahost=::1%6 agt=4.4.4.4
agentZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-
10.255.255.255 av=6.0.2.6627.0 atz=Australia/NSW aid=3ngVO6kkBABCV3m12GeFa2w\=\=
at=windowsfg dvchost=auirsarc004 dvc=10.19.96.68 deviceZoneURI=/All Zones/ArcSight
System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 dtz=Australia/NSW
_cefVer=0.1
```

Original field extraction outcome:

Field Name	Field Value
cs2	<Resource ID\

Current field extraction outcome:

Field Name	Field Value
cs2	<Resource ID\="3KDZG6kkBABCAA7iSgTWqfw\=\="/>

The following bug exists in the version 2.0.0 has been fixed in version 2.0.1:

Bug #3: Fixed the inconsistent field alias for the CEF field full names and the corresponding names with the prefix "cef_";

The following bug exists in the version 2.0.1 has been fixed in version 2.0.2:

Bug #2: Fixed the REGEX issues when dynamically extract the fields (ad.someFieldNameHere and ad.Key[{num}))

Bug #4: Fixed the REGEX inconsistency issues for the CEF header and get the field extractions more efficient.

Known issues

This add-on is designed to replace the old edition of technology add-on for ArcSight CEF inputs (https://splunkbase.splunk.com/app/3694/) due to Splunk base naming convention compliance purposes. This add-on cannot either be installed or running on the same Splunk infrastructure while the old edition of the technology add-on for ArcSight CEF inputs also installed.