Vendor - Microsoft

Product - Cloud App Security (MCAS)

Ref	Link
Splunk Add-on CCF	https://bit.ly/SPLServices/ta-cef-common-load/
Splunk Add-on Source Security	none
Product Manual	https://docs.microsoft.com/en-us/cloud-app-security/siem

Sourcetypes

sourcetype	notes	
cef	Common	sourcetype

Source

source	notes	
microsoft:cas	Common	sourcetype

Index Configuration

key	source	index	notes
MCAS_SIEM_agent	microsoft:cas	main	none

Filter type

MSG Parse: This filter parses message content

Options

Note listed for reference processing utilizes the Microsoft Cloud App Security Add-on Arcsight log path as this format is a subtype of CEF

Variable	default	description
SC4S_LISTEN_SIMPLE_CEF_TCP_PORT	empty string	Enable a TCP port for this specific vendor product using the number defined
SC4S_LISTEN_SIMPLE_CEF_UDP_PORT	empty string	Enable a UDP port for this specific vendor product using the number defined
SC4S_ARCHIVE_CEF	no	Enable archive to disk for this specific source
SC4S_DEST_CEF_HEC	no	When Splunk HEC is disabled globally yet enabled for this specific source

> NOTE: Set index any and CEF variables for the entire SC4S deployment. Regardless of how many parses are in use by this CEF source (or any other source) Select the 1:CEF common Event Format source destination