Palo Alto Networks (Firewall) data connector

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Known Issue:

Palo Alto Networks (Firewall) Data Connector curreltly does not support variable length CEF headers.

Starting with PAN-OS 10.0, Palo Alto started using variable Length CEF headers on some templates and that is not supported by the Palo Alto Networks (Firewall) data connector.

The data connector expects 7 CEF headers and will drop messages missing headers.

Workaround:

A workaround is to add an additional header to the Palo Alto CEF template, see example below where we duplicate the $subtype header on the GlobalProtect template:

- CEF:0|Palo Alto Networks|PAN-OS|$sender_sw_version|$type|$subtype| **$subtype|** rt=$receive_time PanOSDeviceSN...

A feature request to support variable length CEF headers was created and expected to be release by the end of the year.

BACKLOG Item: https://msazure.visualstudio.com/One/_workitems/edit/13869362