

Common Event Format Configuration Guide

CyberArk Software, Inc

Privileged Threat Analytics (PTA) v. 2.6.3

Date: Friday, October 02, 2015



CEF Connector Configuration Guide

This document is provided for informational purposes only, and the information herein is subject to change without notice. Please report any errors herein to HP. HP does not provide any warranties covering this information and specifically disclaims any liability in connection with this document.

Certified CEF:

The event format complies with the requirements of the HP ArcSight Common Event Format. The HP ArcSight CEF connector will be able to process the events correctly and the events will be available for use within HP's ArcSight product. In addition, the event content has been deemed to be in accordance with standard SmartConnector requirements. The events will be sufficiently categorized to be used in correlation rules, reports and dashboards as a proof-of-concept (POC) of the joint solution

CyberArk Privileged Threat Analytics (PTA)

August 31, 2015

Revision History

Date	Description
08/31/2015	First edition of this Configuration Guide.
10/02/2015	Version 2.6.3 Certified by HP Enterprise Security

CEF Connector Support Information when an issue is outside of the ArcSight team's ability

In some cases the ArcSight customer service team is unable to help with issues that lie within the configuration itself in which case, the certified vendor should be contacted for assistance:

CyberArk's Customer Support

CyberArk's Customer Support offerings are focused on helping our clients consistently achieve rapid and sustainable results when utilizing our privileged account security solutions. Our Support offerings are backed by a dedicated staff of support engineers and customer service managers who are committed to helping you realize the greatest value, performance and results with CyberArk.

Email support@cyberark.com

For support by phone:

Support Hotline – North America, South America, Latin America

Business hours (8AM-5PM Eastern Standard Time) 1-888-808-9005

Off hours (Maintenance Plus 24x7)

– US Toll Free: 1-844-537-7700

– Americas: +1-617-965-1544 ext. 2, press 2 at the prompt to submit a critical case

Support Hotline – EMEA, APAC

Tel: +972-3-9180011

Support Hotline – Middle East

Business hours (8AM-5PM Eastern Standard Time) 1-888-808-9005

Off hours (Maintenance Plus 24x7) 1-844-537-7700



CyberArk PTA Connector Configuration Guide

This guide provides information for configuring the CyberArk PTA Connector for syslog event collection. This Connector is supported on CyberArk's PTA (the virtual appliance runs on Linux CentOS 6.4) platforms. Device with PTA versions starting at 2.6.3 are supported.

Overview

Privileged Threat Analytics, part of the CyberArk Privileged Account Security Solution, is an expert system for privileged account security intelligence, providing targeted, immediately actionable threat alerts by identifying previously undetectable malicious privileged user and account activity. The solution applies patent pending analytic technology to a rich set of privileged user and account behavior collected from multiple sources across the network. CyberArk Privileged Threat Analytics then produces highly accurate and immediately actionable intelligence, allowing incident response teams to respond directly to the attack. By combining CyberArk Privileged Threat Analytics with ArcSight, organizations are able to analyze a rich set of data in order to detect, alert, and rapidly respond to cyber attacks.

Configuration

When PTA detects an incident, it sends a syslog record to your HP ArcSight solution in real time using CEF format. PTA sends a record when an incident is created, when an existing incident is updated with new security events that are correlated to the same incident, and when an incident is closed. You can identify PTA records by their device vendor name, "CyberArk", and their device product name, "PTA".

To Configure PTA to Send syslog Records to Your SIEM Solution

1. On the PTA machine, open the `systemparm.properties` configuration file using a text editor such as `vi`:
`vi /opt/tomcat/diamond-resources/local/systemparm.properties`
2. Uncomment the **syslog_outbound** property and edit the following parameters in the sample configuration:
 - **Host** – The Host/IP address of the server where your SIEM solution is installed.
 - **Port** – The port number through which the syslog records will be sent to the server where your SIEM solution is installed.
 - **Protocol** – The protocol used to transfer the syslog records to the server where your SIEM solution is installed. Currently, PTA supports only `udp`.
 - **Format** – The format used to transfer the syslog records to the server where your SIEM solution is installed. Currently, PTA supports only HP ArcSight.
3. Save the configuration file and close it.
4. Restart the PTA.

Screen Shot

ArcSight        **cyber-ark**
Last Failed Login: 9/3/2015 1:00:07 PM EST
Failed Attempts: 2

PTA Channel    

PTA Channel (100%)  

Start Time: 8/27/2015 7:00:00 PM EST
End Time: 9/3/2015 9:00:00 PM EST
Evaluation: Continuous
Filter: Device_Product = "PTA"
Inline Filter: <No Filter>

Very High: 0
High: 4
Medium: 7
Low: 3
Very Low: 0
Total Events: 14

 Updated

Displaying: All

   Field Set: PTA

	Manager Receipt Time	Event ID	Device Vendor	Device Product	Device Version	Start Time	Detection Date	Priority	Device Event Class ID	Message	Link
☐	9/3/2015 11:01:32 AM EST	879639244	CyberArk	PTA	2.6.3	8/31/2015 4:56:31 AM EST	3 Sep 2015 01:53:28 PDT	3	20	Incident updated. Now contains 2 anomalies	https://10.0.1.210/incidents/55e42c
☐	9/3/2015 10:50:02 AM EST	879629585	CyberArk	PTA	2.6.3	8/31/2015 4:44:59 AM EST	3 Sep 2015 01:41:56 PDT	3	20	Incident created	https://10.0.1.210/incidents/55e42c
☐	9/1/2015 2:00:42 PM EST	877767945	CyberArk	PTA	2.6.3	8/31/2015 3:34:08 AM EST	1 Sep 2015 13:52:24 PDT	5	20	Incident created	https://10.0.1.210/incidents/55e41c
☐	9/1/2015 1:57:22 PM EST	877761880	CyberArk	PTA	2.6.3	8/31/2015 3:30:53 AM EST	1 Sep 2015 11:49:12 PDT	5	20	Incident created	https://10.0.1.210/incidents/55e41c
☐	9/1/2015 1:38:37 PM EST	877739700	CyberArk	PTA	2.6.3	8/31/2015 3:11:57 AM EST	1 Sep 2015 13:30:06 PDT	5	20	Incident created	https://10.0.1.210/incidents/55e40c
☐	9/1/2015 1:35:52 PM EST	877733558	CyberArk	PTA	2.6.3	8/31/2015 3:09:13 AM EST	1 Sep 2015 11:27:14 PDT	7	20	Incident updated. Now contains 2 anomalies	https://10.0.1.210/incidents/55e40c
☐	9/1/2015 1:33:42 PM EST	877731485	CyberArk	PTA	2.6.3	8/31/2015 3:07:08 AM EST	31 Aug 2015 22:34:53 PDT	5	20	Incident created	https://10.0.1.210/incidents/55e40c
☐	8/30/2015 10:51:25 PM EST	875687991	CyberArk	PTA	2.6.3	8/30/2015 10:43:19 PM EST	30 Aug 2015 20:43:01 PDT	5	20	Incident created	https://10.0.1.210/incidents/55e3cc
☐	8/30/2015 10:28:45 PM EST	875678118	CyberArk	PTA	2.6.3	8/30/2015 10:20:34 PM EST	30 Aug 2015 22:20:05 PDT	5	20	Incident created	https://10.0.1.210/incidents/55e3cc

Events

CyberArk PTA Connector sends an Event Type 20, for both new Incident Created or Incident Updated events.

Device Event Mapping to ArcSight Data Fields

Information contained within vendor-specific event definitions is sent to the ArcSight SmartConnector, then mapped to an ArcSight data field.

The following table lists the mappings from ArcSight data fields to the supported vendor-specific event definitions.

CyberArk PTA Connector Field Mappings

Vendor-Specific Event Definition	ArcSight Event Data Field
PREFIX FIELDS	
The CEF header and version. The version number identifies the version of the CEF format.	CEF:0
Information about the device sending the message. For PTA, the Device Vendor is CyberArk , and the Device Product is PTA .	Device Vendor, Device Product, Device Version
A unique ID that identifies the event that is reported. Currently, this value is 20.	Signature Id
A description of the reported event.	Event Name
A number that reflects the importance of the event. On a scale of 0 to 10, 10 indicates the most important event.	Severity
Extension Fields	
The ID of the PTA incident.(IncidentID)	ExternalId
The system time when the latest event in the incident occurred.(StartTime)	rt
The system time when PTA identified the latest event in the incident. (detectionDate)	deviceCustomDate1 & deviceCustomDate1Label

Vendor-Specific Event Definition	ArcSight Event Data Field
This field describes whether the incident was created, updated, or closed. The relevant text is displayed: • Incident created – An incident with one event. • Incident updated. Now contains <number> anomalies – An incident with more than one event, including the number of identified events. • Incident closed – A closed incident.	message
An HTTPS link to the Incident Details page in the PTA. (link)	cs2 & cs2Label
Number of anomalies. (updatedEvents)	cn1 & cn1Label