



Hewlett Packard Enterprise

Common Event Format Configuration Guide

CyberArk Privileged Account Security v9.7

Date: Tuesday, October 18, 2016



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 HPE. HPE 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 HPE ArcSight Common Event Format. The HPE ArcSight CEF connector will be able to process the events correctly and the events will be available for use within HPE'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 Account Security – Enterprise Password Vault 9.7

September 20, 2016

Revision History

Date	Description
06/25/2012	First edition of this Configuration Guide.
07/10/2012	v7.1 Certified by HP Enterprise Security
09/20/2016	Updates for Version 9.7
10/17/2016	Version 9.7 Certified by HPE 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:

<http://www.cyberark.com/services-support/support/>

Phone -1-888-808-9005

Email support@cyberark.com

CyberArk Enterprise Password Vault Configuration Guide

This guide provides information for configuring the CyberArk PAS solution for syslog event collection. This Connector is supported on Windows, Linux, and Solaris platforms. Device versions 6.0 and above are supported.

Overview

CyberArk® Software is a global information security company that specializes in protecting and managing privileged users, applications and sensitive information to improve compliance, productivity and protect organizations against insider threats and advanced external threats. With its award-winning Privileged Account Security (PAS), Sensitive Information Management and Privileged Session Management Suites, organizations can more effectively manage and govern data center access and activities, whether on-premise, off-premise or in the cloud, while demonstrating returns on security investments.

In regards to ArcSight Integration, CyberArk's PAS solution provides the capability to monitor and track the usage of every privileged account in an organization. It allows organizations the capability to answer the question of who is using privileged credentials, when and why. With the addition of the Privileged Session Manager, organizations can then extend this functionality to answer the question of what is occurring during the usages of these privileged credentials. This audit information plus much more regulatory data required for determining access controls, etc. can be forwarded to your HP ArcSight Implementation to provide one unified view for all privileged activity. For example, when a user checks out an Administrator id from our PAS solution, connects to that Windows Server, and performs some type of privileged activity including clearing the native windows audit log, an event will show in ESM that Administrator cleared the log. Here is where CyberArk comes in. We provide the accountability through correlation or just simple CEF forwarding that will allow you to see the exact person that used that credential within the same console. Furthermore, you could create correlation rules, possible active remediation rules, session management viewing, and/or dashboards from within ESM. This will ultimately provide an organization with one unified approach for alerting and notification for lighting fast forensics and change management capabilities.

Configuration

In regards to configuration within the CyberArk PAS, a simple configuration change needs to be made to the Digital Vault server. Included out of the box is an xsl parser for HPE/ArcSight CEF. On the Vault server, you will simply point to the IP Address(s) of your HPE ArcSight implementation and define the Port you are sending over (514 UDP is default but can be modified to TCP. Lastly you will configure the event ids that you want to send from the CyberArk solution to HP ArcSight. Included with this document are the available events that can be sent. Over 300 events can be configured. Below is a screenshot of the configuration in the CyberArk PAS solution. A restart of the Vault server is required once configured. You also have the option of sending to an ArcSight CEF Smart Connector which can then forward on to ESM.

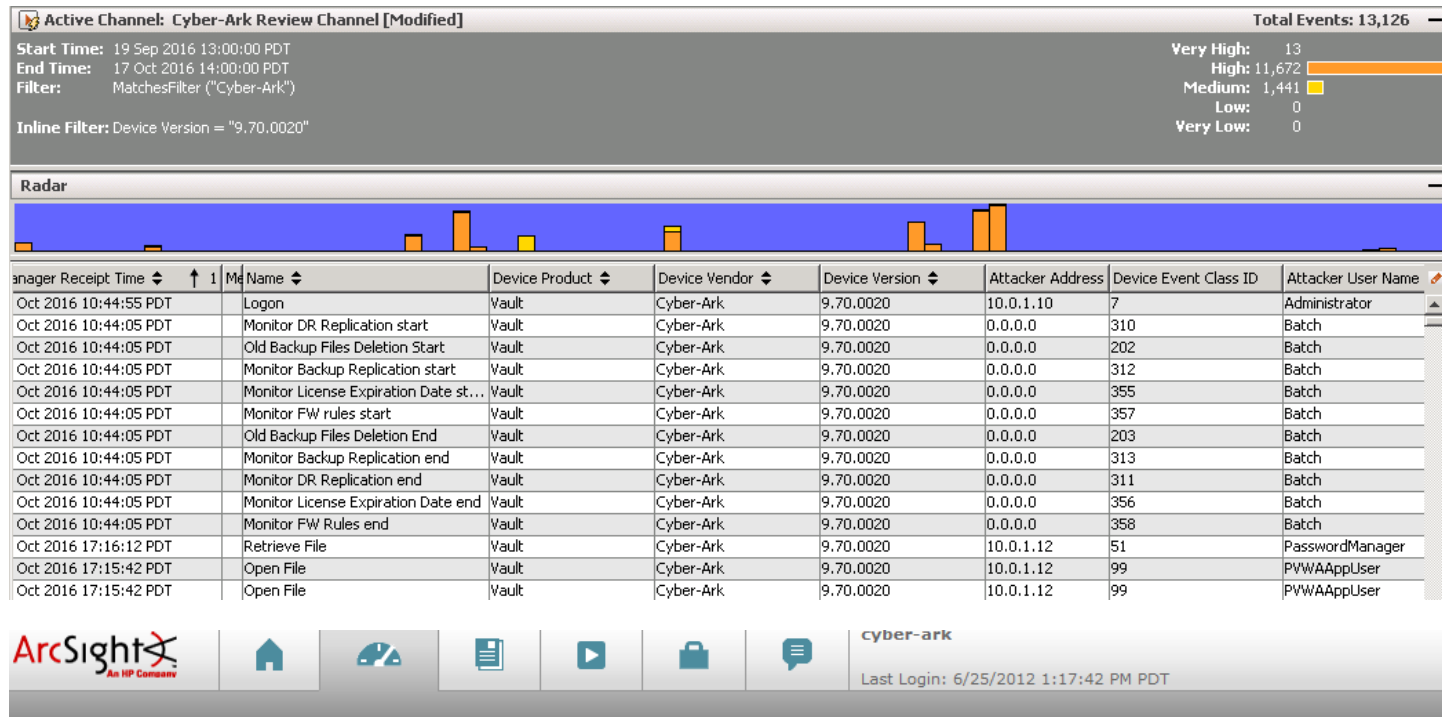
```
[SYSLOG]
syslogTranslatorFile=syslog\Arcsight.xsl
syslogServerPort=514
syslogServerIP=10.0.1.13
syslogMessageCodeFilter=0-5,7-8,18,22,24,28-31,36-38,57,63-66,68,80,82-83,109,114-117
syslogSendBOMPrefix=No
```

The following table lists the most useful events to monitor:

Code	Action
4	User Authentication
22	CPM Verify Password
24	CPM Change Password
31	CPM Reconcile Password
38	CPM Verify Password Failed
57	CPM Change Password Failed
60	CPM Reconcile Password Failed
130	CPM Disable Password
295	Retrieve Password succeeded
300	PSM Connect
302	PSM Disconnect
308	Use Password
319	Retrieve Password (from Provider)
344	Privileged Command Initiated
346	Privileged Command Completed
359	SSH Command
361	PSM Command
378	PSM Secure Connect Session Start
380	PSM Secure Connect Session End
411	PSM Window Title

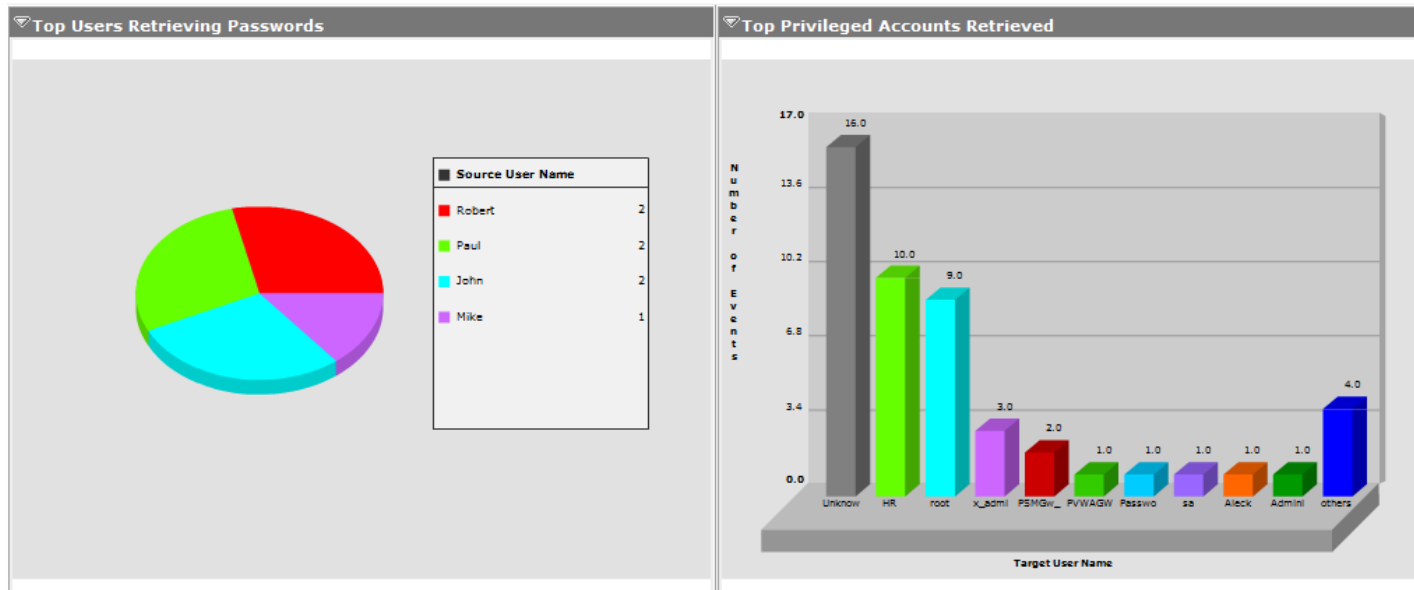
Screen Shots

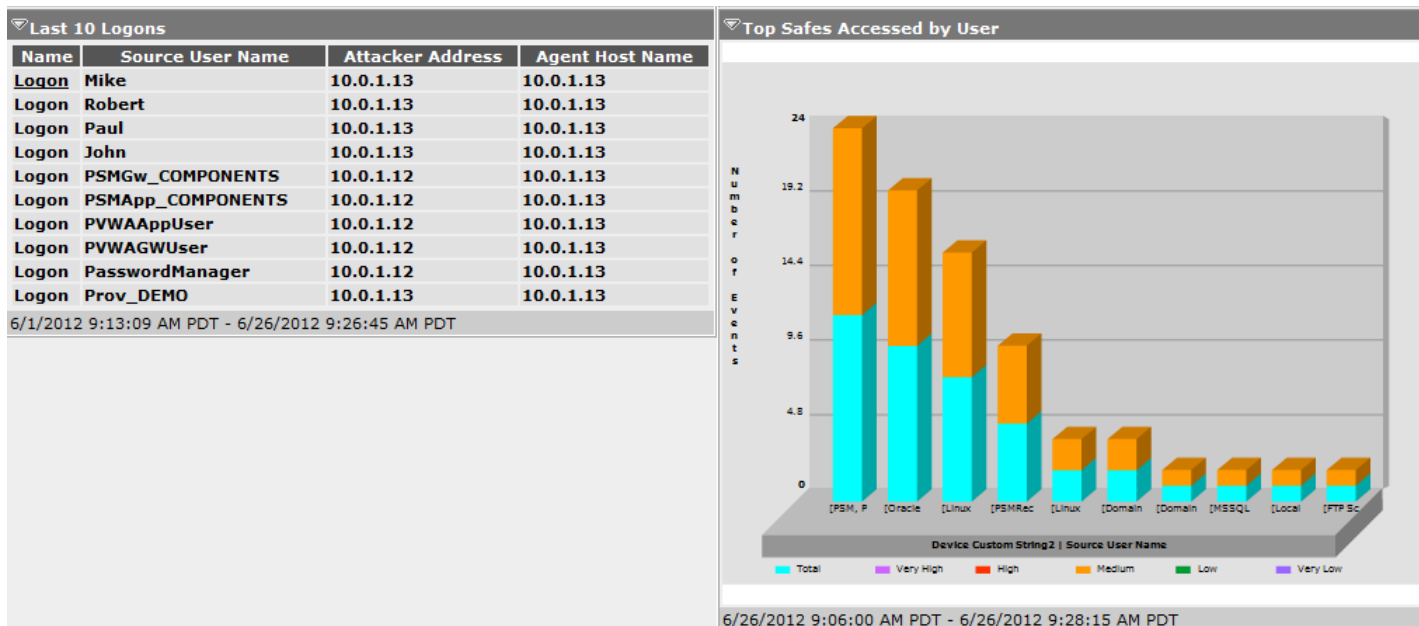
Included below are screenshots illustrating various connections into the CyberArk PAS solution including retrieval of credentials for Windows, Unix and Databases. Dashboard examples are also illustrated below.



Dashboard: Cyber-Ark Overview

Next refresh in 55 seconds





Events

For a complete list of events and action codes available in the User and Safe Activities (LogList) report that can be exported to a SIEM solution using Syslog protocol, refer to the *Vault Audit Action Codes* section of the *Privileged Account Security Reference Guide* v9.7, page 281.

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 Connector Field Mappings

ArcSight Event Data Field	CyberArk Field Definition	Field Description
act	Action	A description of the audit record (Login, PSM Connect/Disconnect, Password Retrieval, etc)
suser	Issuer	The name of the Vault user who performed the operation
fname	File	The name of the target file, ie: Object path (Folder+ObjectName)
dvc	GatewayStation	The IP of the web application machine (PVWA).
shost	SrcHost	If it's PSM Connect and Disconnect event we will show SrcHost value otherwise we will show station value.
dhost	DstHost	If it's PSM Connect and Disconnect event we will show DstHost value.
duser	User	If it's PSM Connect and Disconnect event we will show User value.
externalid	SessionID	PSM Session ID
app	Protocol	
reason	Command ExtraDetails	Specific extra details of the audit records.
cs1Label	Affected User Name	
cs2Label	Safe Name	
cs3Label	Device Type	
cs4Label	Database	
cs5Label	Other Info	
cn1Label	Request ID	
cn2Label	Ticket ID	