SNYPR 6.1

DATA SOURCE GUIDE

CYBERARK

Securonix Proprietary Statement

This material constitutes proprietary and trade secret information of Securonix, and shall not be disclosed to any third party, nor used by the recipient except under the terms and conditions prescribed by Securonix.

The trademarks, service marks, and logos of Securonix and others used herein are the property of Securonix or their respective owners.

Securonix Copyright Statement

Contact Information

Securonix, Inc.

14665 Midway Rd. Ste. 100, Addison, TX 75001

www.securonix.com

855.732.6649

Revision History

Date	Product Version	Description
2/23/2018	6.1	First Release
3/13/2018	6.1	Revision

Table of Contents

CyberArk

This data source guide provides information about how the CyberArk data source events are parsed, normalized and categorized to SNYPR fields. In particular, it provides the following:

- Device event field mapping
- Device event severity mapping
- Device event categorization

To download the CyberArk parser from the Securonix Threat Library, search Available Resources Types for Deployment by Vendor name or Functionality. Downloading the resource downloads the parser along with the applicable dashboards, reports, policies and threat models.

What is CyberArk

CyberArk provides solutions that protect privileged credentials by securing, rotating, monitoring their usage and providing a way for clients to respond to potential attacks involving these sensitive credentials.

Supported Collection Methods

The method of collection is syslog.

Taxonomy

Securonix Open Event Format (OEF) 1.0 is used. OEF is an event interoperability standard/schema. It provides a set of standardized attributes (fields) for consistent representation of logging output from disparate security and non-security devices and applications. For additional information, refer to the Data Dictionary section on the Securonix documentation portal.

Device Event Field Mapping

This section lists the mappings of SNYPR fields to the device fields.

SNYPR Field	CyberArk Field
Mapped Attribute	Attribute
deviceseverity	deviceSeverity
DATETIME	rt
sourcehostname	shost

SNYPR Field	CyberArk Field
sourcentdomain	sntdom
sourceport	spt
sourceuserid	suid
destinationhostname	dhost
destinationaddress	dst
destinationntdomain	dntdom
accountname	duser
destinationuserid	duid
devicecustomstring1	cs1
devicecustomstring2	cs2
deviceeventcategory	cat
deviceaction	act
applicationprotocol	app
deviceCustomIPv6Address1	c6a1
deviceCustomIPv6Address2	c6a2
deviceCustomIPv6Address3	c6a3
deviceCustomIPv6Address4	c6a4
deviceCustomFloatingPoint1	cfp1
deviceCustomFloatingPoint2	cfp2
deviceCustomFloatingPoint3	cfp3
deviceCustomFloatingPoint4	cfp4
baseeventcount	cnt
customnumber1	cn1
customnumber2	cn2
customnumber3	cn3
devicecustomstring3	cs3

SNYPR Field	CyberArk Field
devicecustomstring4	cs4
devicecustomstring5	cs5
devicecustomstring6	cs6
destinationprocessid	dpid
destinationmacaddress	dmac
destinationuserprivileges	dpriv
destinationprocessname	dproc
destinationport	dpt
deviceaddress	dvc
devicehostname	dvchost
deviceprocessid	dvcpid
filename	fname
filesize	fileSize
bytesin	in
eventoutcome	outcome
bytesout	out
transportprotocol	proto
requesturl	request
sourcemacaddress	smac
sourceprocessid	spid
sourceprocessname	sproc
sourceuserprivileges	spriv
destinationdnsdomain	destinationDnsDomain
destinationServiceName	destinationServiceName
destinationTranslatedAddress	destinationTranslatedAddress
destinationTranslatedPort	destinationTranslatedPort

SNYPR Field	CyberArk Field
deviceCustomDate1	deviceCustomDate1
deviceCustomDate2	deviceCustomDate2
deviceDirection	deviceDirection
deviceDnsDomain	deviceDnsDomain
deviceExternalId	deviceExternalId
deviceFacility	deviceFacility
deviceinboundinterface	deviceInboundInterface
deviceMacAddress	deviceMacAddress
deviceNtDomain	deviceNtDomain
deviceoutboundinterface	deviceOutboundInterface
deviceprocessname	deviceProcessName
devicetranslatedaddress	deviceTranslatedAddress
filecreatetime	fileCreateTime
fileHash	fileHash
filemodificationtime	fileModificationTime
filepath	filePath
filePermission	filePermission
filetype	fileType
oldFileCreateTime	oldFileCreateTime
oldFileHash	oldFileHash
oldFileId	oldFileId
oldFileModificationTime	oldFileModificationTime
oldfilepath	oldFilePath
oldFilePermission	oldFilePermission
oldfilesize	oldFileSize
oldfiletype	oldFileType

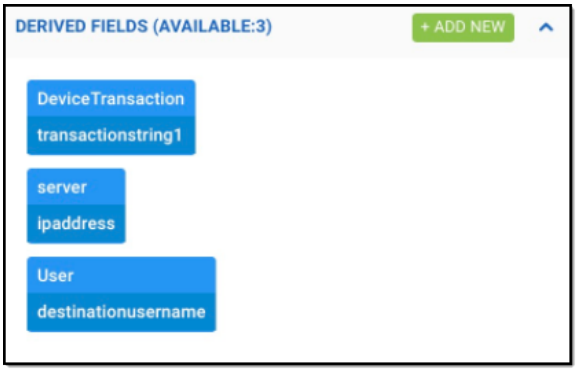
SNYPR Field	CyberArk Field
requestclientapplication	requestClientApplication
requestcontext	requestCookies
requestmethod	requestMethod
sourceDnsDomain	sourceDnsDomain
sourceServiceName	sourceServiceName
transalatedipaddress	sourceTranslatedAddress
translatedport	sourceTranslatedPort
SiemId	eventId
baseeventid	externalId
message	message
customstring1	signatureId
transactionstring1	DeviceTransaction
customstring2	msg
destinationusername	User
ipaddress	server

Device Event Categorization

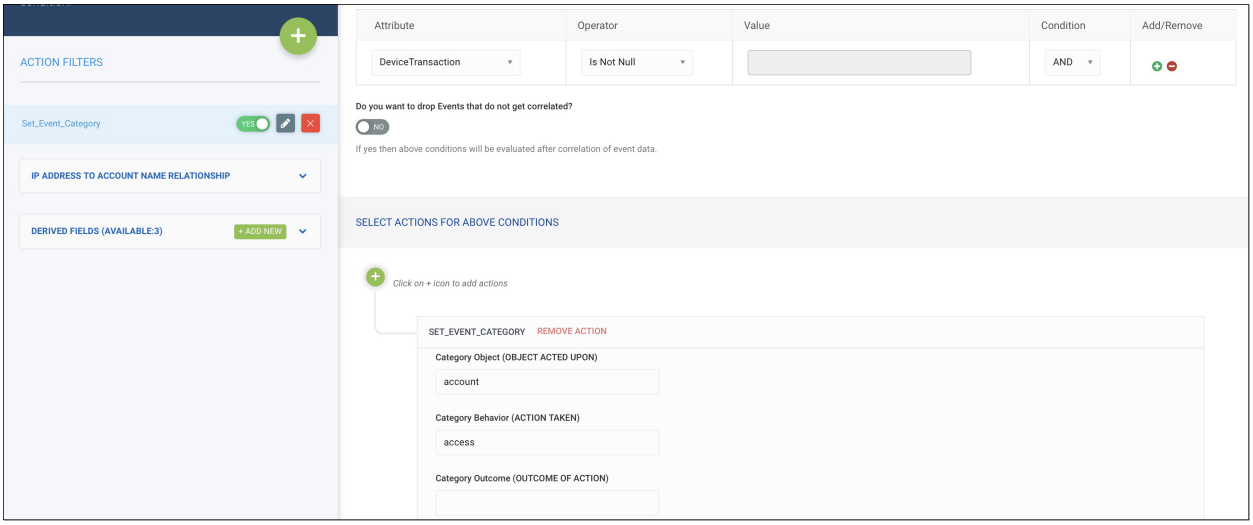
This section contains the rules used to categorize the device events.

Rule Name	Condition	Category Object	Category Behavior
"Set_Event_Category"	DeviceTransaction is NOT NULL	account	access

Sample Derived Fields for Event Categorization

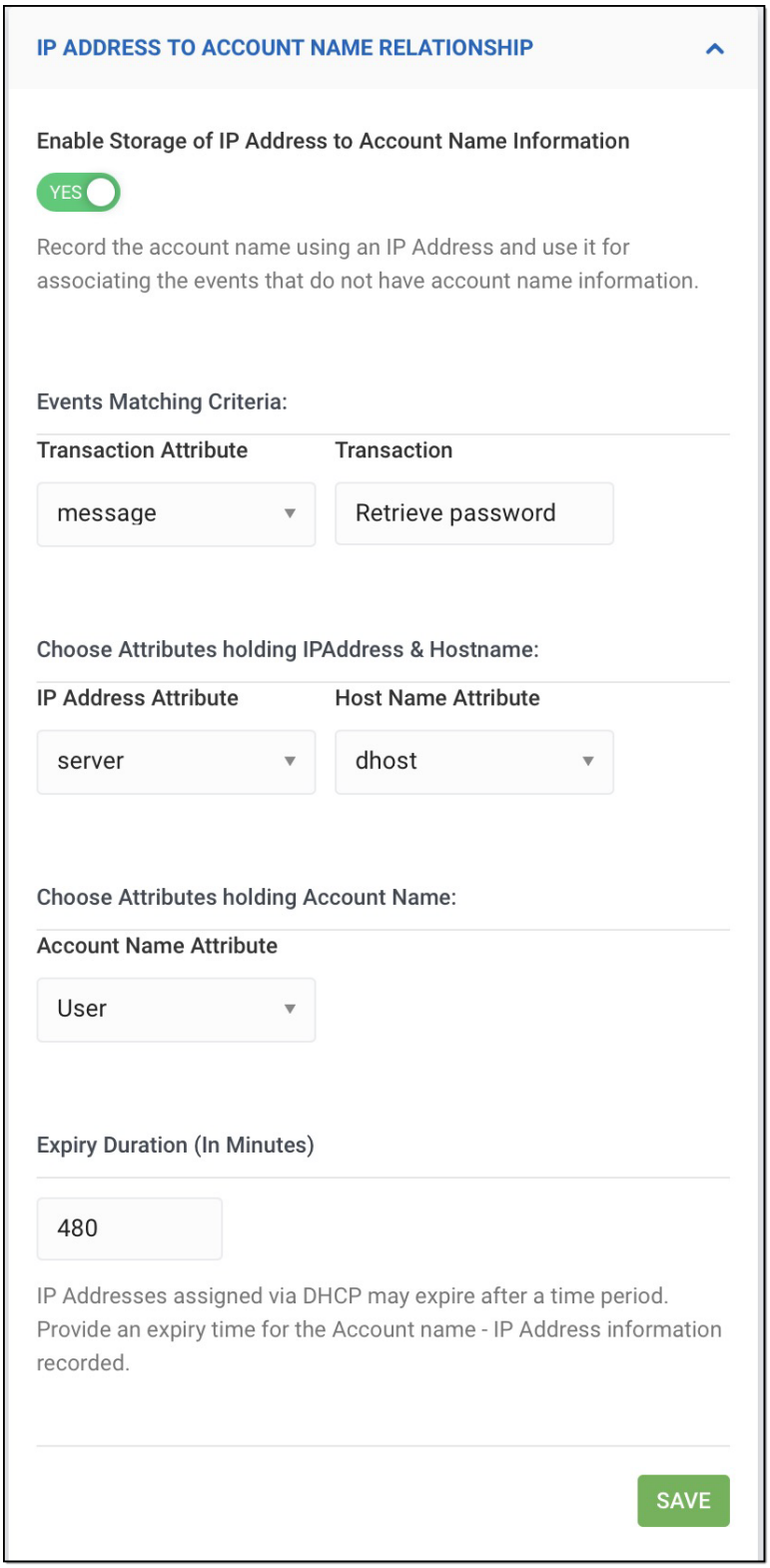


Sample of setting the event categorization in the Web Console.



Sample Mapping

IP Attribution



Policies

The policies available for CyberArk:

- Abnormal number of password retrieval compared to past behavior
- Possible Backdoor Account Creation
- Privilege misuse - Password checkout by CyberArk admin
- Checked Out Password with Reason
- CyberArk Account Modification
- Terminated User Performing Activity
- High number of Failed attempts across multiple hosts
- Privileged account being used by user for the first time
- Rare safe-name accessed by user

Sample Dashboards