Splunk® Supported Add-ons
Splunk Add-on for CyberArk released

Generated: 10/25/2022 8:10 am

Table of Contents

Overview

About the Splunk Add-on for CyberArk

Version	1.2.0
Vendor Products	Privileged Threat Analytics (PTA) 12.2, Enterprise Password Vault (EPV) 12.2

The Splunk Add-on for CyberArk allows a Splunk software administrator to pull system logs and traffic statistics from Privileged Threat Analytics (PTA) 12.2 and Enterprise Password Vault (EPV) 12.2 using syslog in Common Event Format (CEF). This add-on extracts CyberArk real-time privileged account activities (such as individual user activity when using shared accounts) into the Splunk platform and Splunk Enterprise Security, providing a single place to analyze unusual account activity.

This add-on provides the inputs and **CIM**-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security and the Splunk App for PCI Compliance.

Download the Splunk Add-on for CyberArk from Splunkbase at http://splunkbase.splunk.com/app/2891.

Installation overview for the Splunk Add-on for CyberArk

Complete the following steps to install and configure this add-on on your supported platform.

1. Download the add-on from Spunkbase here: https://splunkbase.splunk.com/app/2891.

2. Install the add-on.

3. Configure CyberArk to produce syslog output.

4. Configure an input on your data collection node.

Hardware and software requirements

You must have access to the CyberArk EPM Admin Console so that you can configure it and send data to the Splunk platform instance. Since this is modular input TA and Universal Forwarders do not come with a UI, Universal Forwarders are not supported for configuration in Splunk Web.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply to the Splunk software that you use to run this add-on.

- You must be running version 8.0 or later of Splunk Platform.
- For Splunk Enterprise system requirements: see "System Requirements" in the Splunk Enterprise *Installation Manual*.
- If you manage on-premises forwarders to get data into Splunk Cloud, see "System Requirements" in the Splunk Enterprise *Installation Manual*, which includes information about forwarders.

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

Installation and Configuration

Install the Splunk Add-on for CyberArk

Use the tables in this topic to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise. See the "installation walkthrough" section at the bottom of this page for links to installation instructions specific to a single-instance deployment, distributed deployment, or Splunk Cloud.

Distributed installation of this add-on

This table provides a quick reference for installing this add-on to a distributed deployment of Splunk Enterprise.

Splunk instance type	Supported	Required	Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where CyberArk knowledge management is required.
Indexers	Yes	No	Not required, because this add-on does not include any index-time operations.
Heavy Forwarders	Yes	No	All forwarder types are supported.
Universal Forwarders	Yes	No	All forwarder types are supported.

Distributed deployment compatibility

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features.

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality, but configure inputs only on a forwarder to avoid duplicate data collection. Before installing this add-on to a cluster, remove the `eventgen.conf` file and all files in the `Samples` folder.
Indexer Clusters	Yes	Before installing this add-on to a cluster, remove the `eventgen.conf` file and all files in the `Samples` folder.
Deployment Server	Yes	Supported for deploying configured add-on to your forwarder.

Installation walkthrough

See "Installing add-ons" in *Splunk Add-Ons* for detailed instructions describing how to install a Splunk add-on in the following deployment scenarios:

- single-instance Splunk Enterprise
- distributed Splunk Enterprise
- Splunk Cloud

Configure CyberArk to produce syslog for the Splunk Add-on for CyberArk

To enable the Splunk Add-on for CyberArk to collect data from your EPV and PTA instances, you need to configure your CyberArk devices to produce syslog output and push it to a data collection node of your Splunk platform installation.

Configure EPV to produce syslog

For EPV, apply the translator file provided in the forExport folder of the Splunk Add-on for CyberArk, then see "Integrating with SIEM Applications" in the Privileged Account Security Implementation Guide to configure syslog output.

1. Copy the `SplunkCIM.xsl` file to the folder %ProgramFiles%\PrivateArk\Server\Syslog of the Vault Server.

2. Follow the instructions in "Integrating with SIEM Applications" in the Privileged Account Security Implementation Guide to configure the `DBParm.ini`.

3. For the SyslogTranslatorFile parameter, enter `SplunkCIM.xsl`.

4. For the SyslogServerIP and SyslogServerPort parameters, enter the address of your SC4S server (recommended) or syslog aggregator or specify a Splunk platform instance that you want to use to receive syslog directly.

5. Restart your CyberArk Vault server service.

Configure PTA to produce syslog

For PTA, see "Sending PTA syslog records to SIEM" in the Privileged Threat Analytics (PTA) Implementation Guide and follow the instructions to configure syslog output. For the Host and Port parameters, enter the address of your syslog aggregator, or specify the address of your SC4S server (recommended) or syslog aggregator that you want to use to receive syslog directly.

Configure inputs for Splunk Add-on for CyberArk

The Splunk Add-on for CyberArk handles inputs through syslog. There are three ways to capture this data.

1. Using Splunk Connect for Syslog, this is the recommended option.

2. Use a syslog aggregator with a Splunk forwarder installed on it. Configure a monitor input to monitor the file or files generated by the aggregator.

3. Create a set of TCP or UDP inputs to capture the data sent on the ports you have configured in CyberArk.

Splunk Connect for Syslog

Splunk recommends you use (Splunk Connect for Syslog) SC4S for data collection. Follow the steps in the doc link below to configure SC4S.

https://splunk.github.io/splunk-connect-for-syslog/main/sources/vendor/CyberArk/epv/

Monitor input

If you are using a syslog aggregator, install a forwarder on that machine and set up two monitor inputs to monitor the files that are generated. Set your source type to `cyberark:epv:cef` for the output from EPV and `cyberark:pta:cef` for the output from PTA. The CIM is dependent on these source types.

See Monitor files and directories in the *Getting Data In* manual for information about setting up a monitor input.

TCP/UDP input

In the Splunk platform node handling data collection, configure two inputs to match your protocol and port configurations in CyberArk. PTA only supports UDP, and EPV supports either TCP or UDP, if possible, use TCP, becuase UDP doesn't ensure delivery and logs may be lost in transit as a result. Match the protocol for EPV to the one you configured in the CyberArk Admin Console.

Set your source type to `cyberark:epv:cef` for the output from EPV and `cyberark:pta:cef` for the output from PTA. The CIM mapping is dependent on these source types.

For information on how to configure a Splunk forwarder or single-instance to receive a syslog input using the CLI for the configuration files, see Get data from TCP and UDP ports in the *Getting Data In* manual. You can also configure syslog inputs using the Splunk Web UI if you have access to Splunk Web on your collection node as described in Monitor network ports in the *Getting Data In* manual.

Validate data collection

Once you have configured the inputs, run this search to check that you are ingesting the data that you expect.

```
sourcetype=cyberark:*
```

Troubleshooting

Troubleshoot the Splunk Add-on for CyberArk

For helpful troubleshooting tips that you can apply to all add-ons, see "Troubleshoot add-ons" in *Splunk Add-ons*. For additional resources, see "Support and resource links for add-ons" in *Splunk Add-ons*.

Reference

Lookups for the Splunk Add-on for CyberArk

The Splunk Add-on for CyberArk has the following **lookups**. The lookup files map fields from CyberArk systems to CIM-compliant values in the Splunk platform. The lookup files are located in `$SPLUNK_HOME/etc/apps/Splunk_TA_cyberark/lookups`.

Filename	Description
`cyberark_epv_vault_audit_action_codes_lookup.csv`	Maps `code` to `description`, `alert`, `cim_data_model`, `action`, `change_type`, `extratag`, `vendor_object`, `object_category`, and `status`.
`cyberark_epv_all_changes_result.csv`	Maps `code` to `result`, `object_attrs`.
`cyberark_epv_vault_alert.csv`	Maps `code` to `type`, `dest_type`.
`cyberark_epv_all_changes_object.csv`	Maps `code` to `object`, `object_id`.

Source types for the Splunk Add-on for CyberArk

The Splunk Add-on for CyberArk provides index-time and search-time knowledge for CyberArk alerts, events, and traffic in the following formats.

Source type	Description	Eventtype	CIM compatibility
`cyberark:epv:cef`	Data from Enterprise Password Vault	cyberark_epv_authentication	Authentication
		cyberark_epv_authentication_success	Authentication
		cyberark_epv_authentication_failure	Authentication
		cyberark_epv_change_analysis	Change
		cyberark_epv_change_analysis_cpm	Change
		cyberark_epv_change_analysis_cpm_tasks	Change
		cyberark_epv_change_analysis_cpm_auto_detection	Change
		cyberark_epv_change_analysis_account	Change
		cyberark_epv_change_analysis_psm	Change
		cyberark_epv_change_analysis_safe_acl	Change
		cyberark_epv_change_analysis_audit	Change
		cyberark_epv_network_sessions	Network Sessions
		cyberark_epv_network_sessions_start	Network Sessions
		cyberark_epv_network_sessions_end	Network Sessions
cyberark_epv_endpoint_filesystem	Endpoint		
cyberark_epv_endpoint_process	Endpoint		
cyberark_epv_alert	Alerts		

Source type	Description	Eventtype	CIM compatibility
`cyberark:pta:cef`	Data from Privileged Threat Analytics.	cyberark_pta_alerts	Alerts

Release notes

Release notes for the Splunk Add-on for CyberArk

Version 1.2.0 of the Splunk Add-on for CyberArk was released on December 2, 2021.

About this release

Version 1.2.0 of the Splunk Add-on for CyberArk is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	8.0, 8.1, 8.2
CIM	4.20.2
Platforms	Platform independent
Vendor Products	Privileged Threat Analytics (PTA) 12.2, Enterprise Password Vault (EPV) 12.2

New features

Version 1.2.0 of the Splunk Add-on for CyberArk has the following new features.

- Added the support for the latest CyberArk Enterprise Password Vault 12.2 and CyberArk Privileged Threat Analytics 12.2.
- Added support for the latest Splunk Common Information Model version 4.20.2.

See the following tables for information on field changes between 1.1.0 and 1.2.0:

Source-type	sourcetype	Fields added	Fields removed
`['cyberark:epv:cef']`	cyberark:epv:cef	EventID, user_name, src_user_name, id, result_id, SourceAddress, object_id, description, signature_id	

Source-type	sourcetype	Fields added	Fields removed
`['cyberark:pta:cef']`	cyberark:pta:cef	user_name, dvc, description	

See the following table for a list of fields modified between 1.1.0 and 1.2.0:

Sourcetype	CIM Field	cef_name	Vendor Field in 1.1.1	Vendor Field in 1.2.0
cyberark:epv:cef	object	Add Location, Delete Location, Rename/Move Location, Update Location	suser, Example: user404	Static: location
Delete Group	suser, Example: user404	Static: group		
Move Network Area, Rename Network Area, Update Network Area	suser, Example: user404	Static: network area		

Sourcetype	CIM Field	cef_name	Vendor Field in 1.1.1	Vendor Field in 1.2.0
object_category Failure:CPM Reconcile Password Failed	Add Note Static: User	Static: unknown Sttaic: user	Static: note	
Clear User History	Static: file	Static: user		
Failure: Open/Close Safe, Safe Access through Gateway	Static: object	Static: safe		
Update Address	Static: unknown	Static: user		
change_type	Add Owner, Update Owner	Static: vault	Static: Vault	
Delete Group	Static: Group	Static: AAA		
Set Password	Static: Password	Static: AAA		
action	Failure:CPM Reconcile Password Failed	created	modified	
Failure: User Has Expired, Failure: User Is Disabled	read	failure		
result	Delete Folder	N/A	Static: folder deleted	
Lock As Draft	N/A	Static: draft locked		
Move File	N/A	Static: file moved		
Rename File	N/A	Static: file renamed		
reason	Window Title	reason, Example: explorer.exe	Static: success	
cyberar:pta:cef	signature_id	All	EventId, Example: a2f3c7eb-0a56-41c9-8b55-99ceaab6cc97	cef_signature, Example: 24
severity		Static: unknown	Static: low	
dest_type		Static: storage	Static: instance	

CIM model changes

See the following CIM model changes between 1.1.0 and 1.2.0:

Sourcetype	cef_name	Previous CIM model	New CIM model
cyberark:epv:cef	Set Password, Delete Group	Change:All_Changes	Change:Account_Management
User Has Expired, User Is Disabled	Change:Auditing_Changes	Authentication:Authentication	
Update Safe, Delete Safe	Change:Account_Management	Change:All_Changes	

Sourcetype	cef_name	Previous CIM model	New CIM model
Monitor DR Replication start, Monitor DR Replication end, Monitor Backup Replication start, Monitor Backup Replication end	N/A	Change:All_Changes	
Privileged Threat Analytics Event	N/A	Alerts:Alerts	
Update existing Add Account Bulk Operation succeeded	N/A	Change:Account_Management	
`cyberark:pta:cef`	Privileged access to the Vault from irregular	N/A	Alerts:Alerts

Fixed issues

Version 1.2.0 of the Splunk Add-on for CyberArk contains the following fixed issues. If this section is blank, there are no fixed issues.

Known issues

Version 1.2.0 of the Splunk Add-on for CyberArk contains the following known issues. If this section is blank, there are no known issues.

Third-party software attributions

Version 1.2.0 of the Splunk Add-on for CyberArk does not incorporate any third-party software.

Release notes history

The latest version of the Splunk Add-on for CyberArk is version 1.2.0. See Release notes for the Splunk Add-on for CyberArk for the release notes of this latest version.

Version 1.1.1

Version 1.1.1 of the Splunk Add-on for CyberArk is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	7.3, 8.0, 8.1
CIM	4.18
Platforms	Platform independent
Vendor Products	Privileged Threat Analytics (PTA) 12.0, Enterprise Password Vault (EPV) 12.0

New features

Version 1.1.1 of the Splunk Add-on for CyberArk has the following new features.

- Added the support for the latest CyberArk Enterprise Password Vault 11.7 and 12.0 and CyberArk Privileged Threat Analytics 12.0.
- Added support for two new event types: endpoint filesystem and endpoint process.

- Added support for the latest Splunk Common Information Model version 4.18.0.

Fixed issues

Version 1.1.1 of the Splunk Add-on for CyberArk contains the following fixed issues. If this section is blank, there are no fixed issues.

Known issues

Version 1.1.1 of the Splunk Add-on for CyberArk contains the following known issues. If this section is blank, there are no known issues.

Third-party software attributions

Version 1.1.1 of the Splunk Add-on for CyberArk does not incorporate any third-party software.

Version 1.0.0

Version 1.0.0 of the Splunk Add-on for CyberArk is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.2.2 or later
CIM	4.2 or later
Platforms	Platform independent
Vendor Products	Privileged Threat Analytics (PTA) 2.6.3, Enterprise Password Vault (EPV) 9.x

New features

Version 1.0.0 of the Splunk Add-on for CyberArk has the following new features.

Date	Issue number	Description
2015-10-01	ADDON-4979	New Splunk-supported add-on.

Known issues

Version 1.0.0 of the Splunk Add-on for CyberArk has no reported known issues.

Third-party software attributions

Version 1.0.0 of the Splunk Add-on for CyberArk does not incorporate any third-party software.