# Cisco Cyber Vision QRadar application Integration Guide

1.1.0, 4 May 2021

Cisco Systems, Inc.

Total pages: 30

# Cisco Cyber Vision QRadar application Integration Guide

1.1.0, 4 May 2021

**Owner:** Cisco IoT

**Author:** Juliette Maffet

Cisco Systems, Inc.



**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

# Contents

# 1 About this documentation

## 1.1 Document purpose

This document explains how to install the Cisco Cyber Vision QRadar application in IBM QRadar.

This manual is applicable to **system version 3.2.2**.

## 1.2 Warnings and notices

This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

The notices referring to your personal safety and to your property damage are highlighted in the manual by a safety alert symbol described below. These notices are graded according to the degree of danger.

**WARNING**

Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage if proper precautions are not taken.

**IMPORTANT**

Indicates risks that could involve property or Cisco equipment damage and minor personal injury if proper precautions are not taken.

**Note**

Indicates important information on the product described in the documentation to which attention should be paid.

# 2 Introduction

Cisco Cyber Vision is a two-tier monitoring platform made up of sensors and central data visualization and analytics software. It enables organizations to perform OT monitoring: asset tracking, control system integrity and cybersecurity. Cisco Cyber Vision provides full situational awareness, advanced anomaly detection and incident response core capabilities.

The Cisco Cyber Vision QRadar application enables SOC teams to include Operational Technology networks in their security monitoring posture, including detection of targeted attacks, vulnerabilities and industrial malware. By using Cisco Cyber Vision, security analysts can now leverage QRadar to manage security events across their organizational industrial environments and to detect threats or attacks based on both IT and OT environments.

The Cisco Cyber Vision QRadar application provides a dedicated dashboard and search analysis to identify anomalous behavior on the Operational Technology infrastructure. The analysis is based on Cisco Cyber Vision Center log messages, all fields are normalized, and custom analysis and correlation rules can easily be added. By default, the application provides search analysis based on anomalous activities, vulnerabilities, protocol violations, operational anomalies and industrial process modifications.

# 3 Product details and prerequisites

Version: 1.0.10

Release date: April 2021

QRadar minimum version: 2019.14.0.20191031163225

QRadar 7.3.3 / 7.4.1 and 7.3.3 CE

Supported browsers:

- Firefox (verified on xx.x),
- Chrome (verified on xx.x).

# 4 Cisco Cyber Vision installation in QRadar

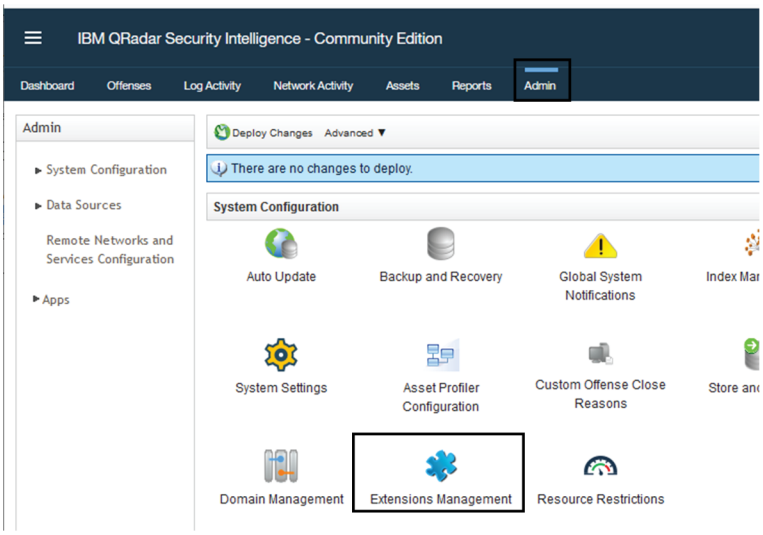
To install the Cisco Cyber Vision QRadar application in QRadar, you will:

1. Install the Cisco Cyber Vision extension.
2. Perform tests by playing sample logs from Cisco Cyber Vision.
3. If needed, configure the Cisco Cyber Vision source log type.
4. Synchronize the Pulse dashboard templates.

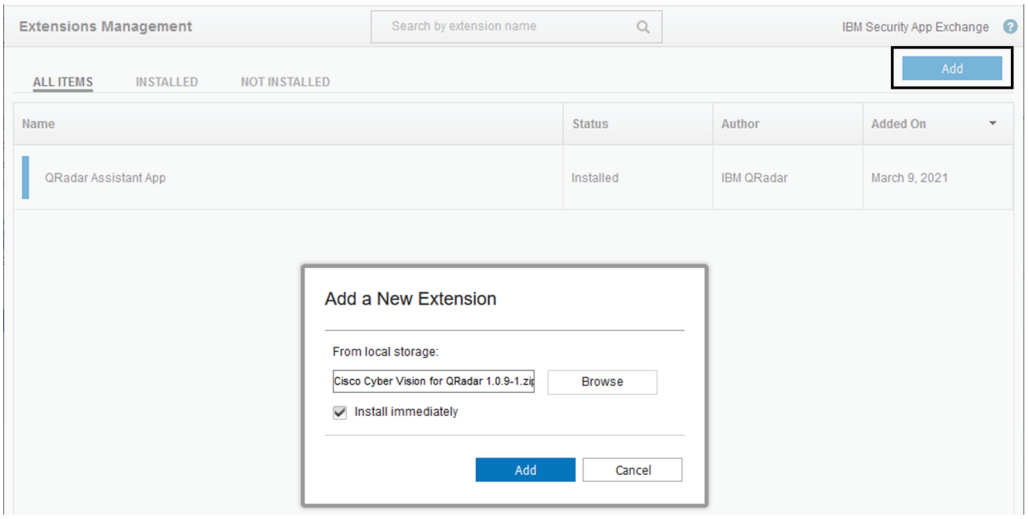
## 4.1 Install the Cisco Cyber Vision extension

To install the Cisco Cyber Vision extension, proceed with the following procedure.

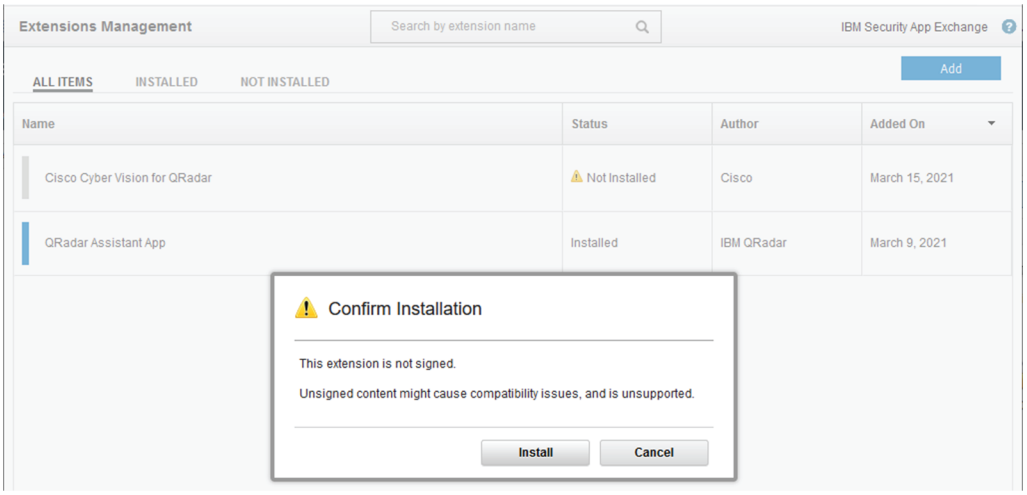
1. Log in to IBM QRadar Security Intelligence.
2. From the Admin menu, click Extensions Management.



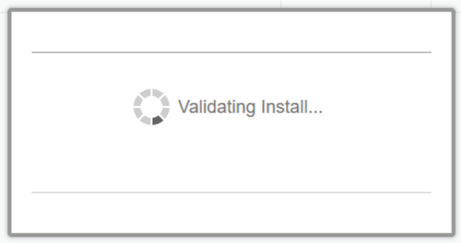

3. Click Add.
   The window Add a New Extension pops up.



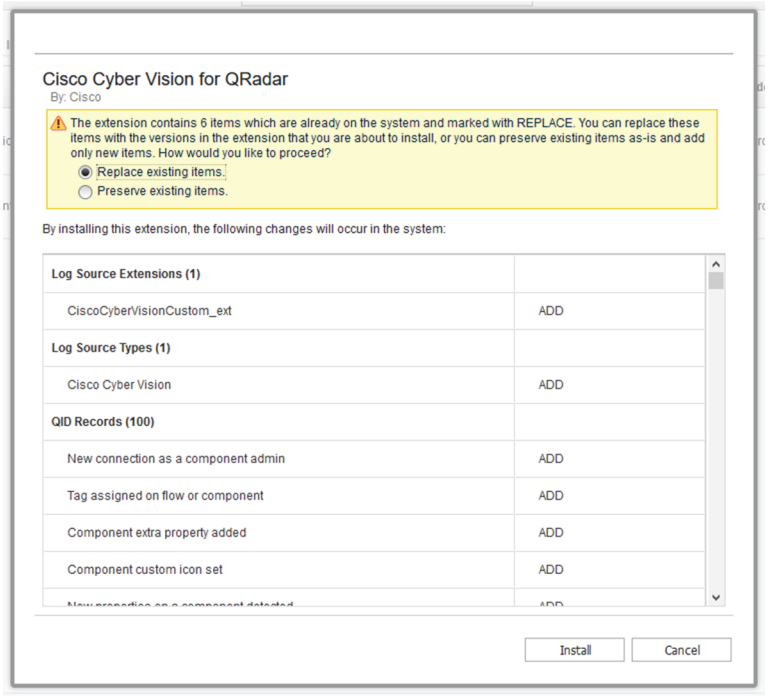

4. Select the package "Cisco Cybervision for QRadar 1.0.10.zip" on your disk.
5. Tick Install immediately and click Add.
6. Click Install to confirm the installation.



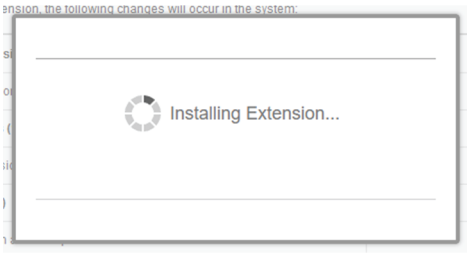

The validation takes a few moments.



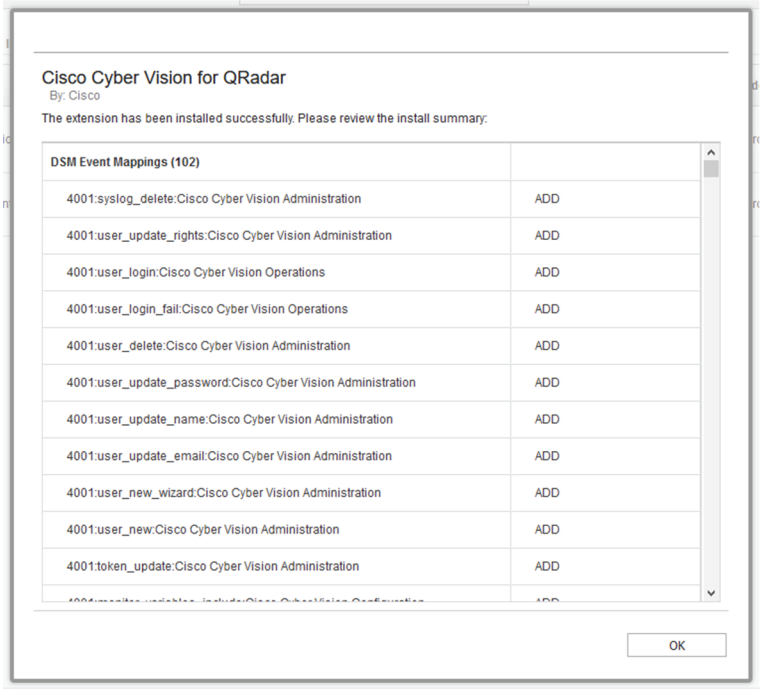

7. If needed, overwrite any existing custom properties by selecting "Replace existing items".



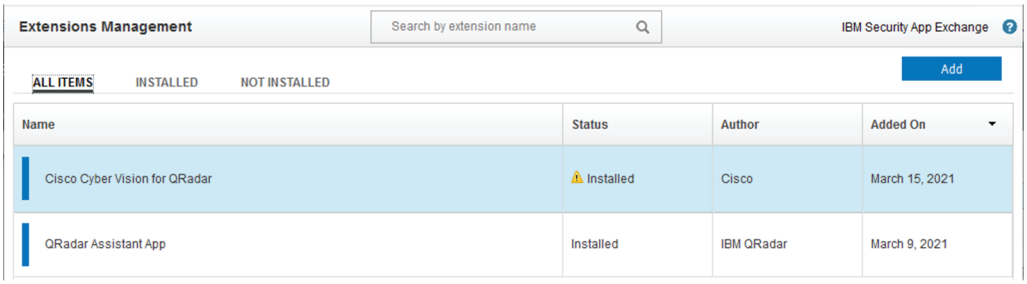

The installation takes a few minutes.




8. Review the install summary and click OK.




The Cisco Cyber Vision extension should appear as installed in Extensions Management.




## 4.2 Play sample logs from Cisco Cyber Vision

To test the installation and see data in the dashboard, play the sample logs as described below.

1. Copy the contents of the Appendix A (page 14) to a text file.
2. Upload the file with scp/ssh on the QRadar development/test machine. To do so, use the following command:

```
scp syslog-CEF.log root@10.0.1.60:
```

```
root@10.0.1.60's password:
```

```
syslog-CEF.log 100% 60KB 15.0MB/s 00:00
```

3. Send logs using the following command:

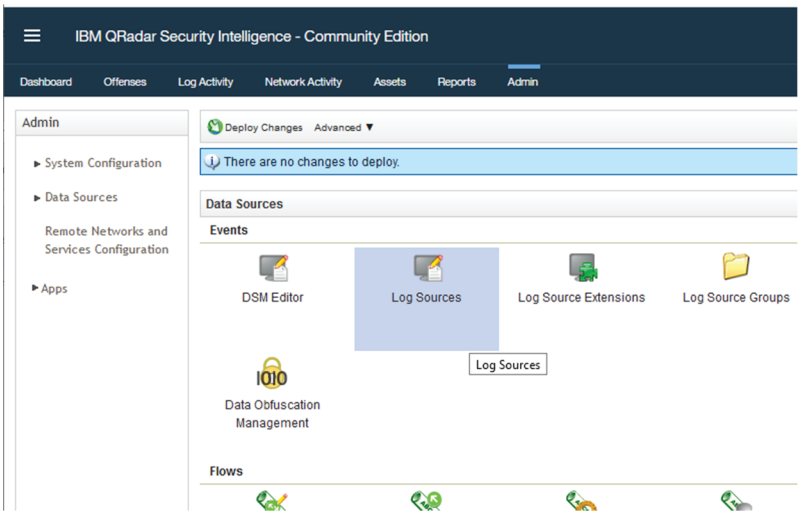
```
/opt/qradar/bin/logrun.pl -f ./syslog-CEF.log -v 10 -l -n ciscolab1
```

The log source for Cisco Cyber Vision is automatically created. You can check in IBM QRadar Log Source Management.

## 4.3 Configure Cisco Cyber Vision source logs

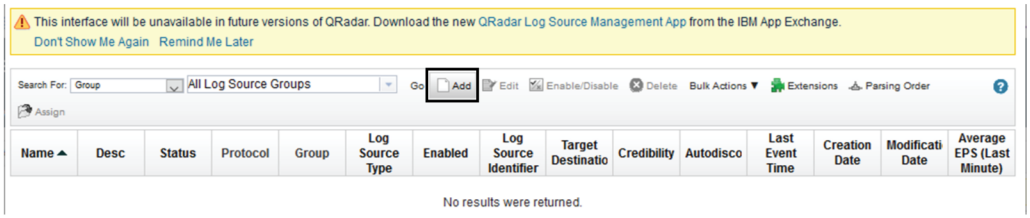
If needed, define the Cisco Cyber Vision Log Source Type:

1. From the Admin menu, click Log Sources.

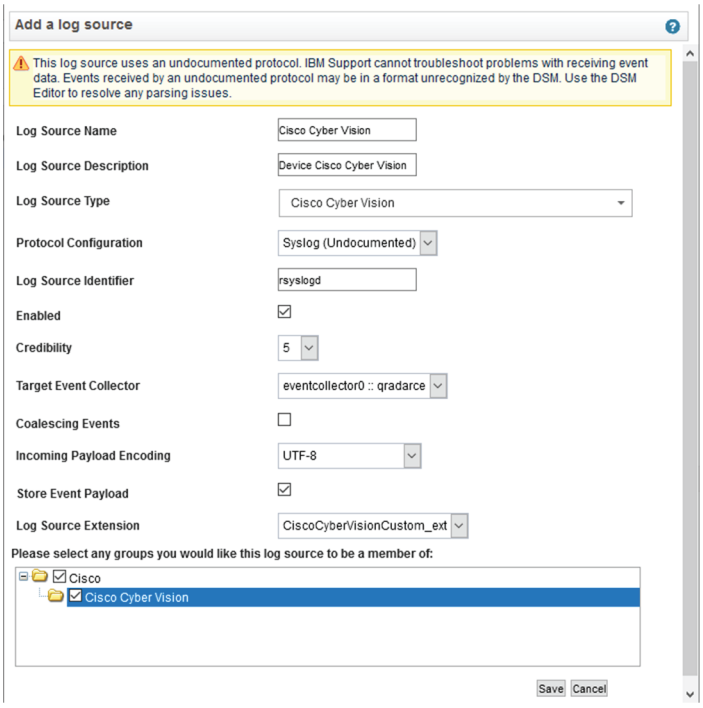



A new window appears.

2. Click Add.

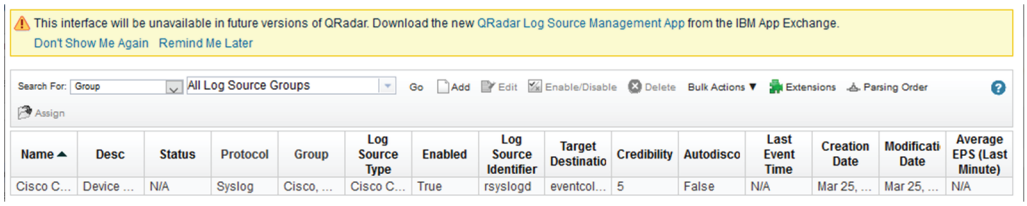



The Add a log source form is displayed.




3. Fill in the following fields:
    - Set Log Source Name to Cisco Cyber Vision and add a description if needed.
    - Set Log Source Type to Cisco Cyber Vision.
    - Set the protocol to Syslog and Log Source Identifier to rsyslogd (depending on the host name you defined).
    - Uncheck Coalescing Events.
    - Select CiscoCyberVisionCustom_ext in the Log Source Extension dropdown.
    - Tick Cisco and Cisco Cyber Vision groups.
4. Click Save.

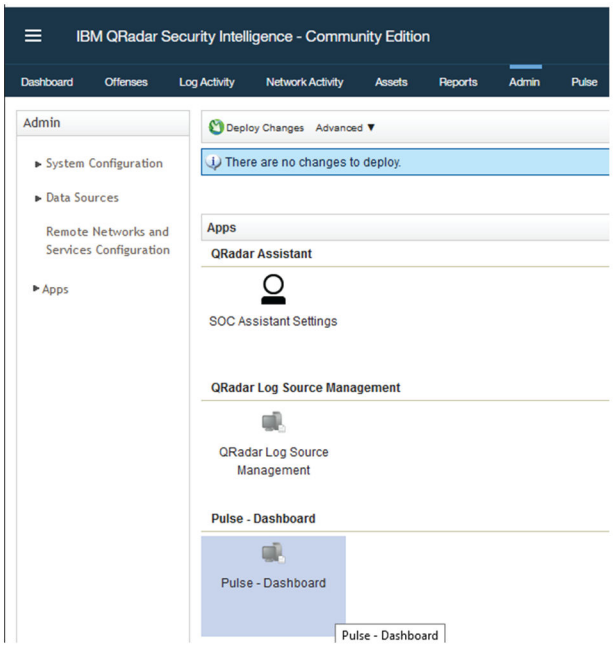
   The log source is displayed in the list.



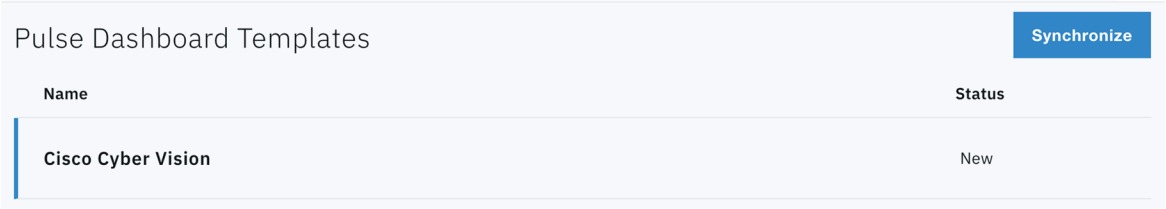
## 4.4 Synchronize the Pulse dashboard template

To complete the installation and see data, follow the instructions below to synchronize with the latest templates found in the pulse_imports reference table. You will be presented with a list of new, existing, or updated dashboards. Select Synchronize to update the Pulse dashboard templates, including the Cisco Cyber Vision one.

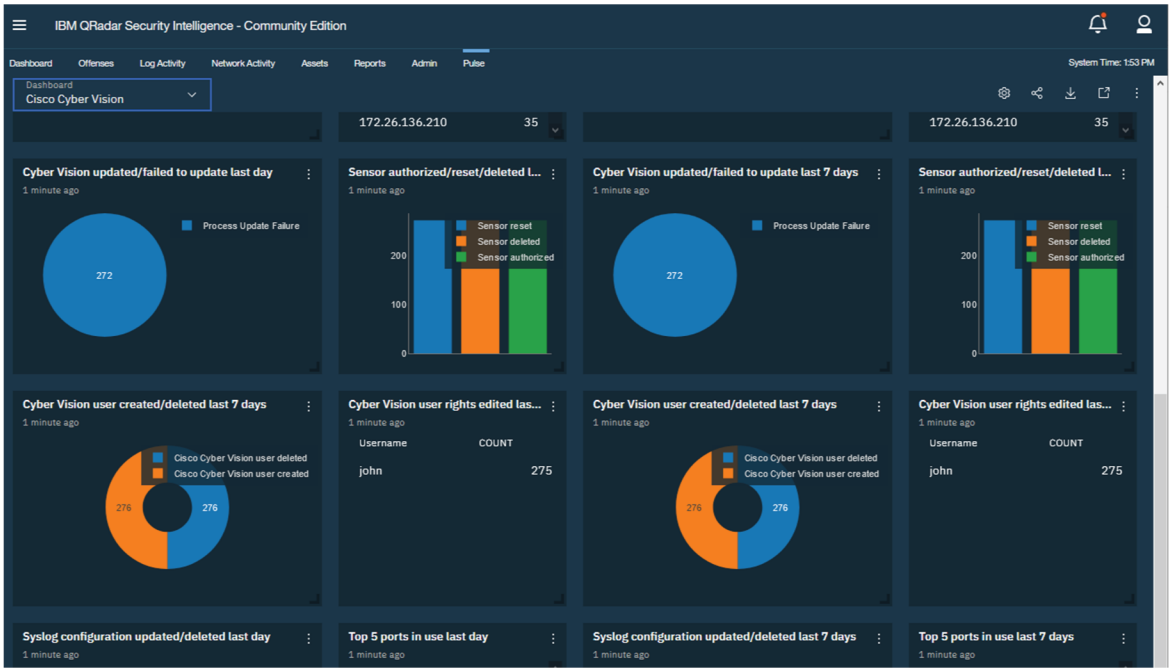
1. From the Admin menu, click Pulse - Dashboard.




The window Pulse Dashboard Templates opens.




2. Click the Synchronize button.
3. The Cisco Cyber Vision template status switched from New to Synchronized.
4. Wait a few moments. Once the import is done, check if the Cisco Cyber Vision dashboard is displayed.




> **Note**
>
> Non admin users must go to the Pulse tab and Switch to Dashboard > New Dashboard > Templates, to add/update these templates into their local dashboard work space.

## 4.6 Appendix A - syslog CEF example

```
<158>2020-11-18T15:45:15.373149+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|token_auth_fail|Cisco Cyber Vision
API token authentification failed|1|cat=Cisco Cyber Vision
Administration msg=Token auth failed: FAIL REASON
```

```
<158>2020-11-18T15:45:15.373989+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|baseline_difference_ignore|
Differences acknowledged but not included in the Baseline|1|
cat=Cisco Cyber Vision Configuration msg=Difference ignored in
baseline 'label' by 'John Smith' with message 'comment'. The
problematic component was 'Component A'. suser=john@smith.com
spriv=User
```

```
<158>2020-11-18T15:45:15.374483+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|set_custom_name|Component custom
name set|1|cat=Inventory Modifications msg=The custom-name
'name' on component 1.2.3.4 has been set from API.
```

```
<158>2020-11-18T15:45:15.374984+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sensor_capture_mode_change|Sensor
capture mode changed|1|cat=Cisco Cyber Vision Administration
msg=User 'John Smith' has changed the capture mode for sensor
EXP1-001 from all to industrial. suser=john@smith.com spriv=User
SCVEventType=sensor_capture_mode
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVSensorId=75c749d2-3612-43d9-9ed7-770dec773089
SCVSensorNewCaptureMode=industrial SCVSensorOldCaptureMode=all
SCVSensorOldCustomInput=oldcustominput
```

```
<158>2020-11-18T15:45:15.375437+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|user_update_name|Cisco Cyber
Vision user name edited|0|cat=Cisco Cyber Vision Administration
msg=Renamed from 'Jane Doe' to 'Dane Joe'. Changes done by John
Smith. The updated user now has administrator rights.
suser=john@smith.com spriv=User SCVEventType=user_manage
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVUserAction=renamed SCVUserId=1caf20a9-c1f0-4e3a-
b6ba-9bf82cb59b3d SCVUserNewAdminValue=true
SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe
SCVUserOldAdminValue=false SCVUserOldEmailValue=jane@doe.com
SCVUserOldValue=Jane Doe
```

```
<158>2020-11-18T15:45:15.376781+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|vuln_unack|Component vulnerability
unacknowledged in Cisco Cyber Vision|2|cat=Security Events
msg=Vulnerability Big Vuln on component Component A is no longer
ignored (John Smith) SCVEventType=user_vulnerabilities
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVVulnAction=unack SCVVulnId=Big vuln
```

```
<158>2020-11-18T15:45:15.377298+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sensor_rename|Sensor renamed|0|
cat=Cisco Cyber Vision Administration msg=Sensor EXP1-001 has
been renamed from 'oldname' to 'newname'. SCVEventType=sensor
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVSensorAction=renamed
SCVSensorId=75c749d2-3612-43d9-9ed7-770dec773089
SCVSensorNewName=newname SCVSensorOldName=oldname
```

```
<158>2020-11-18T15:45:15.377790+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|annotation_update|Component extra
property updated|1|cat=Inventory Modifications msg=An extra
property (myProperty: false) has been updated on component
1.2.3.4 from API.
```

```
<158>2020-11-18T15:45:15.378232+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|delete_custom_name|Component
custom name deleted|1|cat=Inventory Modifications msg=The
custom-name of the component 1.2.3.4 has been deleted from API.
```

```
<158>2020-11-18T15:45:15.378691+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|baseline_differences|Differences
detected on a Baseline|2|cat=Anomaly Detection msg=Baseline
'label' got 1 difference
```

```
<158>2020-11-18T15:45:15.379173+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sensor_reset|Sensor reset|1|
cat=Cisco Cyber Vision Administration msg=Sensor EXP1-001 has
been erased. SCVEventType=sensor
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVSensorAction=revoked
SCVSensorId=75c749d2-3612-43d9-9ed7-770dec773089
```

```
<158>2020-11-18T15:45:15.380130+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|baseline_new|Cisco Cyber Vision
Baseline created|0|cat=Cisco Cyber Vision Configuration
msg=Baseline 'label' has been created by 'John Smith'
suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.381096+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|flow_login_failure|Authentication
failure on component|2|cat=Security Events msg=3 unsuccessful
authentication attempts detected from 1.2.3.4:1234 on
4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-
mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-
port=1234 cmp-b-port=4321 SCVEventType=flow_login_failure
SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVFlowLoginFailureAttempt0=wrongpassword1
SCVFlowLoginFailureAttempt1=wrongpassword2
SCVFlowLoginFailureAttempt2=wrongpassword3
SCVFlowLoginFailureNumberOfAttempts=3
SCVFlowLoginFailureProtocol=
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.383035+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|initial_name|Component initial
name detected|1|cat=Inventory Events msg=Found an initial name
'new' for new component at SCVEventType=initial_name
SCVComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVComponentNewName=new SCVComponentPropertiesNumber=0
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
```

```
<158>2020-11-18T15:45:15.383717+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|system_reboot|System reboot|3|
cat=Cisco Cyber Vision Operations msg=Sensor
75c749d2-3612-43d9-9ed7-770dec773089 has been rebooted from
Cyber Vision by John Smith. suser=john@smith.com spriv=User
SCVEventType=sensor_reboot SCVAuthorId=e2b1e161-5e3a-4bcd-940d-
d540ac8f00b2 SCVSensorId=75c749d2-3612-43d9-9ed7-770dec773089
```

```
<158>2020-11-18T15:45:15.384789+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|baseline_difference_ack|
Differences acknowledged and included to a Baseline|1|cat=Cisco
Cyber Vision Configuration msg=Difference included in baseline
'label' by 'John Smith' with message 'comment'. The problematic
component was 'Component A'. suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.385474+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sensor_high_ressources|Sensor high
ressources usage|1|cat=Cisco Cyber Vision Administration
msg=Sensor [Name: blah, IP: 127.0.0.1] high usage of ressources:
```

```
CPU [81% >\= 80%], Memory [81% >\= 80%], Disk [81% >\= 80%]
SCVEventType=sensor SCVSensorAction=high ressources usage
SCVSensorCpu=81 SCVSensorDisk=81
SCVSensorId=00000000-0000-0000-0000-000000000000
SCVSensorIp=127.0.0.1 SCVSensorMemory=81 SCVSensorName=blah
SCVSensorTime=2020-11-18T15:44:46Z SCVSensorVersion=3.1.0
```

```
<158>2020-11-18T15:45:15.387187+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|analyzer_tag_assign|Tag assigned
on flow or component|0|cat=Inventory Events msg=New tag NETBIOS
automatically assigned for the component. cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
```

```
<158>2020-11-18T15:45:15.387982+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|system_shutdown|System shutdown|3|
cat=Cisco Cyber Vision Operations msg=Center has been shut down
from Cyber Vision by John Smith. suser=john@smith.com spriv=User
SCVEventType=center_shutdown
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
```

```
<158>2020-11-18T15:45:15.388343+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|syslog_update|Syslog configuration
updated|1|cat=Cisco Cyber Vision Administration msg=John Smith
has changed Syslog configuration to local3.*
UDP123.23.23.32:1234 (with tls) suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.388703+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|user_login|Login success to Cisco
Cyber Vision|0|cat=Cisco Cyber Vision Operations msg=User 'John
Smith' has logged into Cyber Vision. suser=john@smith.com
spriv=User SCVEventType=user_login
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
```

```
<158>2020-11-18T15:45:15.389090+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|baseline_delete|Cisco Cyber Vision
Baseline deleted|0|cat=Cisco Cyber Vision Configuration
msg=Baseline 'label' has been deleted by 'John Smith'
suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.389433+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|annotation_update|Component extra
property updated|1|cat=Inventory Modifications msg=User 'John
Smith' has updated an extra property (myProperty: false) on
component 1.2.3.4. suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.389830+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|exception|Protocol exception
detected|2|cat=Security Events msg=Exception 'illegal-function'
has been detected between 1.2.3.4 and 4.3.2.1 cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=flow_exception SCVExceptionLabel=illegal-function
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.390639+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|annotation_delete|Component extra
property deleted|1|cat=Inventory Modifications msg=User 'John
Smith' has deleted an extra property (myProperty: false) of
component 1.2.3.4. suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.390958+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|set_custom_icon|Component custom
icon set|0|cat=Inventory Modifications msg=The custom-icon
'name' on component 1.2.3.4 has been set from API.
```

```
<158>2020-11-18T15:45:15.391321+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sensor_delete|Sensor deleted|1|
cat=Cisco Cyber Vision Administration msg=Sensor EXP1-001 has
been removed. SCVEventType=sensor
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVSensorAction=erased
SCVSensorId=75c749d2-3612-43d9-9ed7-770dec773089
```

```
<158>2020-11-18T15:45:15.391777+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|program_download|New program
downloaded|2|cat=Control Systems Events msg=New program download
requested from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=flow_program_download_started
SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.392613+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|user_login_fail|Login fail to
Cisco Cyber Vision|2|cat=Cisco Cyber Vision Operations
msg=Failed attempt to log in with the user 'ali@baba.fr' (ip:
192.168.69.42). suser=ali@baba.fr src=192.168.69.42
```

```
<158>2020-11-18T15:45:15.392854+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|user_new|Cisco Cyber Vision user
created|0|cat=Cisco Cyber Vision Administration msg=User 'John
Smith' has created the user 'Jane Doe'. suser=john@smith.com
spriv=User SCVEventType=user_manage
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVUserAction=created SCVUserId=1caf20a9-c1f0-4e3a-
b6ba-9bf82cb59b3d
```

```
<158>2020-11-18T15:45:15.393164+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|set_custom_name|Component custom
name set|1|cat=Inventory Modifications msg=User 'John Smith' has
set the custom name 'name' on component 1.2.3.4.
suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.393426+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|stop_cpu|New stop cpu command|3|
cat=Control Systems Events msg=Stop CPU command has been
detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=flow_stop_cpu SCVEventDetailsOrientation=
```

```
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.394018+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|admin_connection|New connection as
a component admin|2|cat=Control Systems Events msg=New admin
connection has been detected from 1.2.3.4:1234 to 4.3.2.1:4321
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-
a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=admin_connection SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.394506+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|decode_failure|Decode failure|2|
cat=Security Events msg=<Dissector message for decode failure>
SCVEventType=decode_failure
SCVSensorId=f8ad95b3-76b5-481e-95d8-2de744108465
SCVSensorLogFlowId=00000000-0000-0000-0000-000000000000
SCVSensorLogSensorId=f8ad95b3-76b5-481e-95d8-2de744108465
```

```
<158>2020-11-18T15:45:15.394752+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|vuln_detect|Component
vulnerability detected|2|cat=Security Events msg=The component
'1.2.3.4' has been detected vulnerable to : Big Vuln
SCVEventType=vulns_assigned
SCVComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVVulns0VulnId=Big vuln SCVVulnsNumber=1
```

```
<158>2020-11-18T15:45:15.394987+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|vuln_ack|Component vulnerability
acknowledged in Cisco Cyber Vision|1|cat=Security Events
msg=Vulnerability Big Vuln on component Component A has been
ignored by John Smith (<Comment>)
```

```
<158>2020-11-18T15:45:15.395212+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|reset_process|Reset process
command|2|cat=Control Systems Events msg=Reset Process command
has been detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=flow_reset_process SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.395697+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|syslog_delete|Syslog configuration
deleted|1|cat=Cisco Cyber Vision Administration msg=John Smith
has deleted Syslog configuration. suser=john@smith.com
spriv=User
```

```
<158>2020-11-18T15:45:15.395936+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|user_delete|Cisco Cyber Vision
user deleted|0|cat=Cisco Cyber Vision Administration msg=User
```

```
'John Smith' deleted the user 'Jane Doe'. suser=john@smith.com
spriv=User SCVEventType=user_manage
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVUserAction=deleted SCVUserId=1caf20a9-c1f0-4e3a-
b6ba-9bf82cb59b3d
```

```
<158>2020-11-18T15:45:15.396165+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|user_update_email|Cisco Cyber
Vision user email edited|0|cat=Cisco Cyber Vision Administration
msg=Changed the email from 'jane@doe.com' to 'dane@joe.com'.
Changes done by John Smith. The updated user now has
administrator rights. suser=john@smith.com spriv=User
SCVEventType=user_manage SCVAuthorId=e2b1e161-5e3a-4bcd-940d-
d540ac8f00b2 SCVUserAction=changed email SCVUserId=1caf20a9-
c1f0-4e3a-b6ba-9bf82cb59b3d SCVUserNewAdminValue=true
SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe
SCVUserOldAdminValue=false SCVUserOldEmailValue=jane@doe.com
SCVUserOldValue=Jane Doe
```

```
<158>2020-11-18T15:45:15.396670+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|port_scan|Port scan detection|3|
cat=Security Events msg=Port scan detected by 1.2.3.4 on 4.3.2.1
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-
a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=port_scan SCVPortScanDetailsProtocol=TCP
SCVPortScanTargetComponentId=bcae40b8-3a98-4bb2-8528-
d870e143dbaf
SCVPortScannerComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.396941+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|offline_data_upload|Offline data
file uploaded to Cisco Cyber Vision|0|cat=Cisco Cyber Vision
Operations msg=An offline data file named 'foo' was uploaded to
Cyber Vision (status: OK).
```

```
<158>2020-11-18T15:45:15.397229+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|delete_custom_name|Component
custom name deleted|1|cat=Inventory Modifications msg=User 'John
Smith' has deleted the custom name of the component 1.2.3.4.
suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.397535+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|component_no_more_vuln|Component
no more vulnerable|1|cat=Security Events msg=The component
'1.2.3.4' seems no more vulnerable to : Big Vuln
SCVEventType=vulns_unassigned
SCVComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVVulns0VulnId=Big vuln SCVVulnsNumber=1
```

```
<158>2020-11-18T15:45:15.397812+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|component_properties_change|
Changed properties on a component detected|1|cat=Inventory
Events msg=Found changed <Protocol> properties:
Property1\="Value1", Property2\="Value2", Property3\="Value3"
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-
a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=changed_properties
SCVComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
```

```
SCVComponentProperties0Name=Property1
SCVComponentProperties0Value=Value1
SCVComponentProperties1Name=Property2
SCVComponentProperties1Value=Value2
SCVComponentProperties2Name=Property3
SCVComponentProperties2Value=Value3
SCVComponentPropertiesNumber=3 SCVComponentProtocol=<protocol>
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.398234+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|system_shutdown|System shutdown|3|
cat=Cisco Cyber Vision Operations msg=Sensor
75c749d2-3612-43d9-9ed7-770dec773089 has been shut down from
Cyber Vision by John Smith. suser=john@smith.com spriv=User
SCVEventType=sensor_shutdown
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVSensorId=75c749d2-3612-43d9-9ed7-770dec773089
```

```
<158>2020-11-18T15:45:15.398411+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|user_update_rights|Cisco Cyber
Vision user rights edited|0|cat=Cisco Cyber Vision
Administration msg=Rights have been changed for 'Dane Joe'.
Changes done by John Smith. The updated user now has
administrator rights. suser=john@smith.com spriv=User
SCVEventType=user_manage SCVAuthorId=e2b1e161-5e3a-4bcd-940d-
d540ac8f00b2 SCVUserAction=changed rights SCVUserId=1caf20a9-
c1f0-4e3a-b6ba-9bf82cb59b3d SCVUserNewAdminValue=true
SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe
SCVUserOldAdminValue=false SCVUserOldEmailValue=jane@doe.com
SCVUserOldValue=Jane Doe
```

```
<158>2020-11-18T15:45:15.398866+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|system_reboot|System reboot|3|
cat=Cisco Cyber Vision Operations msg=Center has been rebooted
from Cyber Vision by John Smith. suser=john@smith.com spriv=User
SCVEventType=center_reboot SCVAuthorId=e2b1e161-5e3a-4bcd-940d-
d540ac8f00b2
```

```
<158>2020-11-18T15:45:15.399049+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sensor_capture_mode_change|Sensor
capture mode changed|1|cat=Cisco Cyber Vision Administration
msg=User 'John Smith' has changed the capture mode for sensor
EXP1-001 from custom "oldcustominput" to industrial.
suser=john@smith.com spriv=User SCVEventType=sensor_capture_mode
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVSensorId=75c749d2-3612-43d9-9ed7-770dec773089
SCVSensorNewCaptureMode=industrial
SCVSensorOldCaptureMode=custom
SCVSensorOldCustomInput=oldcustominput
```

```
<158>2020-11-18T15:45:15.399455+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|event_metadata_update|Cisco Cyber
Vision events settings updated|2|cat=Cisco Cyber Vision
Administration msg=User 'John Smith' updated settings of the
event '' retroactively. suser=john@smith.com spriv=User
SCVEventType=event_metadata_update
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVEventMetadataIsRetroactive=true
SCVEventMetadataNewSeverity=Low
```

```
SCVEventMetadataNewSyslogExport=false
SCVEventMetadataOldSeverity=Low
SCVEventMetadataOldSyslogExport=false
```

```
<158>2020-11-18T15:45:15.399628+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sensor_new_usb|Sensor created by
USB provisioning|0|cat=Cisco Cyber Vision Administration
msg=Sensor EXP1-001 has been manually created.
SCVEventType=sensor SCVAuthorId=e2b1e161-5e3a-4bcd-940d-
d540ac8f00b2 SCVSensorAction=created
SCVSensorId=75c749d2-3612-43d9-9ed7-770dec773089
```

```
<158>2020-11-18T15:45:15.399839+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|start_cpu|New start cpu command|3|
cat=Control Systems Events msg=Start CPU command has been
detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=flow_start_cpu SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.400283+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|decode_failure|Decode failure|2|
cat=Security Events msg=<Dissector message for decode failure>
SCVEventType=decode_failure SCVFlowCmpAComponentId=
SCVFlowCmpBComponentId= SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-
a5c699bc5acf SCVSensorId=f8ad95b3-76b5-481e-95d8-2de744108465
SCVSensorLogFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorLogSensorId=f8ad95b3-76b5-481e-95d8-2de744108465
```

```
<158>2020-11-18T15:45:15.400462+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|token_update|Cisco Cyber Vision
API token updated|1|cat=Cisco Cyber Vision Administration
msg=Token <Name> has been updated by John Smith from [name
\=<Name>,expiration\=none, enable\=true] to [name
\=<Name>,expiration\=none, enable\=false] suser=john@smith.com
spriv=User SCVEventType=token
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVTokenAction=updated SCVTokenEnable=false
SCVTokenId=feafe9dd-297d-4605-9940-ada25038184c
SCVTokenName=<Name> SCVTokenTokenEnable=true
SCVTokenTokenName=<Name>
```

```
<158>2020-11-18T15:45:15.400891+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|delete_custom_icon|Component
custom icon deleted|0|cat=Inventory Modifications msg=The
custom-icon of the component 1.2.3.4 has been deleted from API.
```

```
<158>2020-11-18T15:45:15.401063+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|smb|SMB protocol event|2|
cat=Protocol Events msg=SMB event from 1.2.3.4:1234 to
4.3.2.1:4321 SMB event cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-
mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-
port=1234 cmp-b-port=4321 SCVEventType=flow_smb
SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
```

```
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVFlowProtocolEventDetected=SMB event
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.401480+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|program_download|New program
downloaded|2|cat=Control Systems Events msg=New program has been
downloaded, flow from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=flow_program_downloaded SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.401912+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|flow_forced_variable|Forced
variable|3|cat=Control Systems Events msg=New variable forced
(<VarName>: <NewVal>) has been detected from 1.2.3.4:1234 to
4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-
mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-
port=1234 cmp-b-port=4321 SCVEventType=flow_forced_variable
SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVFlowForcedVariableValue=<NewVal>
SCVFlowForcedVariableVarName=<VarName>
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.402324+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|baseline_update_meta|Cisco Cyber
Vision Baseline updated|0|cat=Cisco Cyber Vision Configuration
msg=Baseline 'label' has been edited by 'John Smith', new label
is 'label', new description is 'description'
suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.402498+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|component_new|New component
detected|2|cat=Inventory Events msg=New component detected on
the network: IP 1.2.3.4, MAC aa:bb:cc:dd:ee:ff
SCVEventType=new_component
SCVComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
```

```
<158>2020-11-18T15:45:15.402699+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|init|New init command|3|
cat=Control Systems Events msg=Init has been detected from
1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-
mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-
port=1234 cmp-b-port=4321 SCVEventType=flow_init
SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.403061+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|token_revoke|Cisco Cyber Vision
API token revoked|1|cat=Cisco Cyber Vision Administration
msg=Token <Name> (<Hash>) has been revoked by John Smith
suser=john@smith.com spriv=User SCVEventType=token
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVTokenAction=revoked SCVTokenEnable=true
SCVTokenId=5d60df8c-2b0a-41c2-9afe-38a8febd8821
SCVTokenName=<Name>
```

```
<158>2020-11-18T15:45:15.403216+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|program_upload|New program
uploaded|2|cat=Control Systems Events msg=New program has been
uploaded, flow from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=flow_program_uploaded SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.403573+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|annotation_new|Component extra
property added|0|cat=Inventory Modifications msg=An extra
property (myProperty: true) has been added to component 1.2.3.4
from API.
```

```
<158>2020-11-18T15:45:15.403717+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|baseline_difference_nack|Anomalies
reported on a Baseline|3|cat=Cisco Cyber Vision Configuration
msg=Incident declared in baseline 'label' by 'John Smith' with
message 'comment'. The problematic component was 'Component A'.
suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.403893+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sbs_update_failure|Cisco Cyber
Vision failed to update|3|cat=Cisco Cyber Vision Administration
msg=System has not been updated from a previously imported file
by John Smith. suser=john@smith.com spriv=User
SCVEventType=sbs_update SCVAuthorId=e2b1e161-5e3a-4bcd-940d-
d540ac8f00b2 SCVSbsUpdateUpdated=false
```

```
<158>2020-11-18T15:45:15.404086+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|user_new_wizard|Cisco Cyber Vision
user created through the Wizard|0|cat=Cisco Cyber Vision
Administration msg=User 'Welcome Wizard' has created the user
'Jane Doe'. SCVEventType=user_manage_wizard
SCVUserAction=created SCVUserId=1caf20a9-c1f0-4e3a-
b6ba-9bf82cb59b3d
```

```
<158>2020-11-18T15:45:15.404253+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sbs_update|Cisco Cyber Vision
updated|3|cat=Cisco Cyber Vision Administration msg=System has
been updated from a previously imported file by John Smith.
suser=john@smith.com spriv=User SCVEventType=sbs_update
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVSbsUpdateUpdated=true
```

```
<158>2020-11-18T15:45:15.404437+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sensor_authorize|Sensor
authorized|0|cat=Cisco Cyber Vision Administration msg=Sensor
EXP1-001 has been authorized. SCVEventType=sensor
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVSensorAction=enrolled
SCVSensorId=75c749d2-3612-43d9-9ed7-770dec773089
```

```
<158>2020-11-18T15:45:15.404651+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|component_properties_change|
Changed properties on a component detected|1|cat=Inventory
Events msg=Found new <Protocol> properties: Property1\="Value1",
Property10\="Value10", Property11\="Value11",
Property12\="Value12", Property13\="Value13",
Property14\="Value14", Property15\="Value15",
Property16\="Value16", Property17\="Value17",
Property18\="Value18", Property19\="Value19",
Property2\="Value2", Property20\="Value20",
Property21\="Value21", Property22\="Value22",
Property23\="Value23", Property24\="Value24",
Property25\="Value25", Property26\="Value26",
Property27\="Value27", Property28\="Value28",
Property29\="Value29", Property3\="Value3",
Property30\="Value30", Property31\="Value31",
Property32\="Value32", Property33\="Value33",
Property34\="Value34", Property35\="Value35",
Property4\="Value4", Property5\="Value5", Property6\="Value6",
Property7\="Value7", Property8\="Value8", Property9\="Value9"
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-
a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=changed_properties
SCVComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVComponentProperties0Name=Property1
SCVComponentProperties0Value=Value1
SCVComponentProperties1Name=Property10
SCVComponentProperties1Value=Value10
SCVComponentProperties10Name=Property19
SCVComponentProperties10Value=Value19
SCVComponentProperties11Name=Property2
SCVComponentProperties11Value=Value2
SCVComponentProperties12Name=Property20
SCVComponentProperties12Value=Value20
SCVComponentProperties13Name=Property21
SCVComponentProperties13Value=Value21
SCVComponentProperties14Name=Property22
SCVComponentProperties14Value=Value22
SCVComponentProperties15Name=Property23
SCVComponentProperties15Value=Value23
SCVComponentProperties16Name=Property24
SCVComponentProperties16Value=Value24
SCVComponentProperties17Name=Property25
SCVComponentProperties17Value=Value25
SCVComponentProperties18Name=Property26
SCVComponentProperties18Value=Value26
SCVComponentProperties19Name=Property27
SCVComponentProperties19Value=Value27
SCVComponentProperties2Name=Property11
SCVComponentProperties2Value=Value11
```

```
SCVComponentProperties20Name=Property28
SCVComponentProperties20Value=Value28
SCVComponentProperties21Name=Property29
SCVComponentProperties21Value=Value29
SCVComponentProperties22Name=Property3
SCVComponentProperties22Value=Value3
SCVComponentProperties23Name=Property30
SCVComponentProperties23Value=Value30
SCVComponentProperties24Name=Property31
SCVComponentProperties24Value=Value31
SCVComponentProperties25Name=Property32
SCVComponentProperties25Value=Value32
SCVComponentProperties26Name=Property33
SCVComponentProperties26Value=Value33
SCVComponentProperties27Name=Property34
SCVComponentProperties27Value=Value34
SCVComponentProperties28Name=Property35
SCVComponentProperties28Value=Value35
SCVComponentProperties29Name=Property4
SCVComponentProperties29Value=Value4
SCVComponentProperties3Name=Property12
SCVComponentProperties3Value=Value12
SCVComponentProperties30Name=Property5
SCVComponentProperties30Value=Value5
SCVComponentProperties31Name=Property6
SCVComponentProperties31Value=Value6
SCVComponentProperties32Name=Property7
SCVComponentProperties32Value=Value7
SCVComponentProperties33Name=Property8
SCVComponentProperties33Value=Value8
SCVComponentProperties34Name=Property9
SCVComponentProperties34Value=Value9
SCVComponentProperties4Name=Property13
SCVComponentProperties4Value=Value13
SCVComponentProperties5Name=Property14
SCVComponentProperties5Value=Value14
SCVComponentProperties6Name=Property15
SCVComponentProperties6Value=Value15
SCVComponentProperties7Name=Property16
SCVComponentProperties7Value=Value16
SCVComponentProperties8Name=Property17
SCVComponentProperties8Value=Value17
SCVComponentProperties9Name=Property18
SCVComponentProperties9Value=Value18
SCVComponentPropertiesNumber=35 SCVComponentProtocol=<protocol>
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.405171+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|restore_db_backup|Cisco Cyber
Vision database restored|2|cat=Cisco Cyber Vision Administration
msg=The database has been restored from a previously exported
dump. suser=john@smith.com spriv=User SCVEventType=dump_import
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVImportDataDumpFilename=/foo/bar
SCVImportDataMigrationRequired=true
SCVImportDataUpdateSuccess=true
```

```
<158>2020-11-18T15:45:15.405319+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|ids|Anomaly detected by signature|
3|cat=Signature based Detection msg=Snort alert id XXX with
signature "blablabla" 127.0.0.1:443 -> 192.168.1.1:8080 proto
blob SCVEventType=snort_event SCVSnortEventDstAddr=192.168.1.1
SCVSnortEventDstPort=8080 SCVSnortEventMsg=blablabla
SCVSnortEventService=blob SCVSnortEventSid=XXX
SCVSnortEventSrcAddr=127.0.0.1 SCVSnortEventSrcPort=443
```

```
<158>2020-11-18T15:45:15.405460+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|component_properties_new|New
properties on a component detected|1|cat=Inventory Events
msg=Found new <Protocol> properties: Property1\="Value1",
Property2\="Value2", Property3\="Value3" cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=new_properties
SCVComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVComponentProperties0Name=Property1
SCVComponentProperties0Value=Value1
SCVComponentProperties1Name=Property2
SCVComponentProperties1Value=Value2
SCVComponentProperties2Name=Property3
SCVComponentProperties2Value=Value3
SCVComponentPropertiesNumber=3 SCVComponentProtocol=<protocol>
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.405852+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|annotation_delete|Component extra
property deleted|1|cat=Inventory Modifications msg=An extra
property (myProperty: false) has been deleted of component
1.2.3.4 from API.
```

```
<158>2020-11-18T15:45:15.406000+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|flow_properties_new|New properties
on a flow detected|1|cat=Inventory Events msg=Found new
<Protocol> properties: Property1\="Value1", Property2\="Value2"
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-
a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=flow_properties
SCVComponentProperties0Name=Property1
SCVComponentProperties0Value=Value1
SCVComponentProperties1Name=Property2
SCVComponentProperties1Value=Value2
SCVComponentPropertiesNumber=2 SCVComponentProtocol=<protocol>
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.406361+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|new_name|Component new name
detected|1|cat=Inventory Events msg=Component 'new' at '' is now
known as 'newer'. SCVEventType=new_name
SCVComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVComponentNewName=newer SCVComponentOldName=new
SCVComponentPropertiesNumber=0
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
```

```
<158>2020-11-18T15:45:15.406501+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|flow_control_action|Action on
control parameters|3|cat=Control Systems Events msg=New <Process
Name> control action (<Variable Name>: <New Value>) has been
detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=flow_control_action SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVFlowControlActionProcessName=<Process Name>
SCVFlowControlActionValue=<New Value>
SCVFlowControlActionVarName=<Variable Name>
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.406905+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|baseline_update|Configuration of
Cisco Cyber Vision Baseline updated|1|cat=Cisco Cyber Vision
Configuration msg=Baseline 'label' has been edited by 'John
Smith', new scan period is '15' seconds suser=john@smith.com
spriv=User
```

```
<158>2020-11-18T15:45:15.407052+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|baseline_delete_element|Component,
Activity or Variable removed from a Baseline|0|cat=Cisco Cyber
Vision Configuration msg=Component 'Component A' was removed
from the baseline 'label' by 'John Smith' with message
'comment'. suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.407193+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sdb_import|Processing KnowledgeDB
import to Cisco Cyber Vision|1|cat=Cisco Cyber Vision
Administration msg=The user John Smith starts importing a
knowledge DB file: SDB.dat suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.407371+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|user_update_password|Cisco Cyber
Vision user password edited|0|cat=Cisco Cyber Vision
Administration msg=Changed the password of 'Dane Joe'. Changes
done by John Smith. The updated user now has administrator
rights. suser=john@smith.com spriv=User SCVEventType=user_manage
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVUserAction=changed password SCVUserId=1caf20a9-c1f0-4e3a-
b6ba-9bf82cb59b3d SCVUserNewAdminValue=true
SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe
SCVUserOldAdminValue=false SCVUserOldEmailValue=jane@doe.com
SCVUserOldValue=Jane Doe
```

```
<158>2020-11-18T15:45:15.407715+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|flow_properties_change|Changed
properties on a flow detected|1|cat=Inventory Events msg=Found
new <Protocol> properties: Property1\="Value1",
Property2\="Value2" cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-
mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-
port=1234 cmp-b-port=4321 SCVEventType=flow_changed_properties
SCVComponentProperties0Name=Property1
SCVComponentProperties0Value=Value1
SCVComponentProperties1Name=Property2
```

```
SCVComponentProperties1Value=Value2
SCVComponentPropertiesNumber=2 SCVComponentProtocol=<protocol>
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.407997+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|token_new|Cisco Cyber Vision API
token added|1|cat=Cisco Cyber Vision Administration msg=Token
<Name> has been added by John Smith suser=john@smith.com
spriv=User SCVEventType=token
SCVAuthorId=e2b1e161-5e3a-4bcd-940d-d540ac8f00b2
SCVTokenAction=add SCVTokenEnable=true
SCVTokenId=5d60df8c-2b0a-41c2-9afe-38a8febd8821
SCVTokenName=<Name>
```

```
<158>2020-11-18T15:45:15.408113+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|restart_cpu|New restart cpu
command|3|cat=Control Systems Events msg=Restart CPU command has
been detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=flow_restart_cpu SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.408363+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|sdb_imported|KnowledgeDB imported
to Cisco Cyber Vision|1|cat=Cisco Cyber Vision Administration
msg=The user John Smith has imported a Sentryo DB file:
'SDB.dat'. It is the version 42 of the Sentryo DB.
suser=john@smith.com spriv=User
```

```
<158>2020-11-18T15:45:15.408476+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|new_name|Component new name
detected|0|cat=Inventory Events msg=A new name has been found
for a component cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-
mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-
port=1234 cmp-b-port=4321
```

```
<158>2020-11-18T15:45:15.408586+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|network_event|Network event
redundancy|1|cat=Protocol Events msg=New network redundancy
event 'failover' has been detected between aa:bb:cc:dd:ee:ff and
ff:ee:dd:cc:bb:aa cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-
mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-
port=1234 cmp-b-port=4321 SCVEventType=flow_network_redundancy
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVFlowProtocolEventDetected=failover
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.408887+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|router_event|Router event
highavailability|1|cat=Protocol Events msg=New router ha event
```

```
'Active' has been detected between aa:bb:cc:dd:ee:ff and
ff:ee:dd:cc:bb:aa cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-
mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-
port=1234 cmp-b-port=4321 SCVEventType=flow_router_ha
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVFlowProtocolEventDetected=Active
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.409143+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|communication_new|New
communication|2|cat=Security Events msg=New FTP communication
has been detected between 1.2.3.4:1234 and 4.3.2.1:4321 cmp-a-
mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=flow_new
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowCommunicationType=FTP SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-
a5c699bc5acf SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.409393+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|firmware_activation|Controler
Firmware activation|3|cat=Control Systems Events msg=Firmware
Activation has been detected from 1.2.3.4:1234 to 4.3.2.1:4321
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-
a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventType=firmware_activation SCVEventDetailsOrientation=
SCVFlowCmpAComponentId=c19ea28b-893d-47b3-9165-37ec11f42cf0
SCVFlowCmpBComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVFlowId=63b1d3ad-8c4e-42c4-a5fe-a5c699bc5acf
SCVSensorId=00000000-0000-0000-0000-000000000000
```

```
<158>2020-11-18T15:45:15.409641+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|annotation_new|Component extra
property added|0|cat=Inventory Modifications msg=User 'John
Smith' has added an extra property (myProperty: true) to
component 1.2.3.4. suser=john@smith.com spriv=User
```