Annex

- Examples, on page 1

Examples

Herebelow, you will find some examples of syslog messages.

```
<158>2022-06-02T10:13:14.195894+00:00 Center cybervision[1]: type="Software" severity="Medium"
 category="Cisco Cyber Vision Administration" family="Cisco Cyber Vision" description="Admin
 Admin has changed Syslog configuration to local3.* tcp192.168.3.21:1238"
<158>2022-06-02T10:13:14.427693+00:00 Center cybervision[1]: CEF:0|Cisco|Cyber
Vision|1.0|syslog_update|Syslog configuration updated|1|cat=Cisco Cyber Vision Administration
 msg=Admin Admin has changed Syslog configuration to local3.* tcp192.168.3.21:1238
suser=admin@sentryo.net spriv=User
<158>2022-06-02T10:13:18.017445+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
<158>2022-06-02T10:13:18.020814+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=created SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
<158>2022-06-02T10:13:18.021489+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVImportDataDumpFilename=/foo/bar
SCVImportDataMigrationRequired=true SCVImportDataUpdateSuccess=true
<158>2022-06-02T10:13:18.021995+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=deleted SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
<158>2022-06-02T10:13:18.022578+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=changed email SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
SCVUserNewAdminValue=true SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe
SCVUserOldAdminValue=false SCVUserOldEmailValue=jane@doe.com SCVUserOldValue=Jane Doe
<158>2022-06-02T10:13:18.024364+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=changed password SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
SCVUserNewAdminValue=true SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe
SCVUserOldAdminValue=false SCVUserOldEmailValue=jane@doe.com SCVUserOldValue=Jane Doe
<158>2022-06-02T10:13:18.026156+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=renamed SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49 SCVUserNewAdminValue=true
 SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe SCVUserOldAdminValue=false
SCVUserOldEmailValue=jane@doe.com SCVUserOldValue=Jane Doe
<158>2022-06-02T10:13:18.028013+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=changed rights SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
SCVUserNewAdminValue=true SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe
SCVUserOldAdminValue=false SCVUserOldEmailValue=jane@doe.com SCVUserOldValue=Jane Doe
<158>2022-06-02T10:13:18.029973+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.030028+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
<158>2022-06-02T10:13:18.030076+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|system_reboot|System reboot|3|cat=Cisco Cyber Vision Operations msg=Sensor
e8631c25-e78c-41f9-b0ab-736be48bc2c0 has been rebooted from Cyber Vision by John Smith.
suser=john@smith.com spriv=User SCVEventtype=sensor_reboot
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.030116+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
<158>2022-06-02T10:13:18.030151+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|system_shutdown|System shutdown|3|cat=Cisco Cyber Vision Operations msg=Sensor
e8631c25-e78c-41f9-b0ab-736be48bc2c0 has been shut down from Cyber Vision by John Smith.
suser=john@smith.com spriv=User SCVEventtype=sensor_shutdown
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.030235+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
<158>2022-06-02T10:13:18.030269+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|decode_failure|Decode failure|1|cat=Security Events msg=<Dissector message for
decode failure> SCVEventtype=decode_failure SCVFlowId=00000000-0000-0000-0000-000000000000
 SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.030308+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|decode_failure|Decode failure|1|cat=Security Events msg=<Dissector message for
decode failure> SCVEventtype=decode_failure SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
 SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.030346+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|analyzer_tags_assign|Tag(s) assigned on flow or component|0|cat=Inventory Events
 msg=New tag(s) 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>2022-06-02T10:13:18.030384+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.030434+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.030469+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sensor_authorize|Sensor authorized|0|cat=Cisco Cyber Vision Administration
msg=Sensor EXP1-001 has been authorized. SCVEventtype=sensor
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSensorAction=enrolled
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.030513+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0 SCVSensorNewCaptureMode=industrial
SCVSensorOldCaptureMode=all SCVSensorOldCustomInput=oldcustominput
<158>2022-06-02T10:13:18.031488+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0 SCVSensorNewCaptureMode=industrial
SCVSensorOldCaptureMode=custom SCVSensorOldCustomInput=oldcustominput
<158>2022-06-02T10:13:18.033368+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSensorAction=created
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.033429+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sensor_delete|Sensor deleted|1|cat=Cisco Cyber Vision Administration msg=Sensor
 EXP1-001 has been removed. SCVEventtype=sensor
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSensorAction=erased
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.033468+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSensorAction=renamed
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0 SCVSensorNewName=newname
SCVSensorOldName=oldname
<158>2022-06-02T10:13:18.033514+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sensor_reset|Sensor reset|1|cat=Cisco Cyber Vision Administration msg=Sensor
EXP1-001 has been erased. SCVEventtype=sensor SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
 SCVSensorAction=revoked SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.033551+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=2022-06-02T10:13:18Z SCVSensorVersion=3.1.0
<158>2022-06-02T10:13:18.034437+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.034497+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.034538+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSbsUpdateUpdated=false
<158>2022-06-02T10:13:18.034577+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
```

```
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSbsUpdateUpdated=true
<158>2022-06-02T10:13:18.034622+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVTokenAction=add
SCVTokenEnable=true SCVTokenId=3c18bc6b-0dac-4401-89f0-ce659b7ad3bd SCVTokenName=<Name>
<158>2022-06-02T10:13:18.034663+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVTokenAction=updated SCVTokenEnable=false
 SCVTokenId=d419579a-8f5f-49bd-a726-f29b2d9fbd74 SCVTokenName=<Name> SCVTokenTokenEnable=true
 SCVTokenTokenName=<Name>
<158>2022-06-02T10:13:18.036567+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.036628+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVTokenAction=revoked SCVTokenEnable=true SCVTokenId=3c18bc6b-0dac-4401-89f0-ce659b7ad3bd
 SCVTokenName=<Name>
<158>2022-06-02T10:13:18.036669+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVEventMetadataIsRetroactive=true
SCVEventMetadataNewSeverity=Low SCVEventMetadataNewSyslogExport=false
SCVEventMetadataOldSeverity=Low SCVEventMetadataOldSyslogExport=false
<158>2022-06-02T10:13:18.037663+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.037726+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
SCVVulns0VulnId=08cec8a3-5b9d-4b98-87c7-9d909488b1c8 SCVVulnsNumber=1
<158>2022-06-02T10:13:18.037774+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
SCVVulns0VulnId=08cec8a3-5b9d-4b98-87c7-9d909488b1c8 SCVVulnsNumber=1
<158>2022-06-02T10:13:18.037821+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3 SCVVulnAction=unack
SCVVulnId=08cec8a3-5b9d-4b98-87c7-9d909488b1c8
<158>2022-06-02T10:13:18.037861+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|port_scan||1|cat= 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
SCVEventtype=port_scan SCVPortScanDetailsProtocol=TCP
SCVPortScanTargetComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVPortScannerComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
<158>2022-06-02T10:13:18.037902+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.037946+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.037985+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.038030+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.038100+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|baseline_differences|Differences detected on a Baseline|2|cat=Anomaly Detection
 msg=Baseline 'label' got 1 difference on 1 item
<158>2022-06-02T10:13:18.040030+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.041577+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.042941+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.043347+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.043523+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|data_expired|Data expiration|2|cat=Cisco Cyber Vision Operations msg=10 old flows
 have been purged SCVEventtype=data_expired SCVObjectsName=flow SCVObjectsNb=10
<158>2022-06-02T10:13:18.043703+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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>2022-06-02T10:13:18.043846+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|extension_alert|Extension-related alert|3|cat=Extension-based alert msg=test
alert message from extension
<158>2022-06-02T10:13:18.044003+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|extension_info|Extension-related info|0|cat=Extension-based alert msg=test info
 message from extension
<158>2022-06-02T10:13:18.047080+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.049266+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3 SCVFlowCommunicationType=FTP
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.051306+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.051380+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowControlActionProcessName=<Process
Name> SCVFlowControlActionValue=<New Value> SCVFlowControlActionVarName=<Variable Name>
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.053586+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=00000000-0000-0000-0000-000000000000
<158>2022-06-02T10:13:18.055526+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowLoginFailureAttempt0=wrongpassword1
SCVFlowLoginFailureAttempt1=wrongpassword2 SCVFlowLoginFailureAttempt2=wrongpassword3
SCVFlowLoginFailureNumberOfAttempts=3 SCVFlowLoginFailureProtocol=
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.057547+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowForcedVariableValue=<NewVal>
SCVFlowForcedVariableVarName=<VarName> SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.059649+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.061499+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
```

```
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.063244+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.064925+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.067033+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=failover
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.068617+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=Active
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.070185+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.071706+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=SMB event
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.073187+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|weak_encryption|Weak encryption event|1|cat=Protocol Events msg=Weak encryption
 from 1.2.3.4:1234 to 4.3.2.1:4321 weak encryption description 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_weak_encryption SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=weak encryption
 description SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.074756+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
```

```
Vision|1.0|online|Online event|3|cat=Control Systems Events msg=Online 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_online SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.076239+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|offline|Offline event|3|cat=Control Systems Events msg=Offline 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_offline SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.077706+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|force_mode|Force mode change event|3|cat=Control Systems Events msg=Force mode
Enabled 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_force_mode SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=Enabled
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.079242+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|force_mode|Force mode change event|3|cat=Control Systems Events msg=Force mode
Disabled 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_force_mode SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=Disabled
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.080730+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.082348+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.083902+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.085398+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|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=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
```