Log format

In this section, we will describe the structure of a syslog message.

Here is an example of a log:

```
Timestamp Center cybervision[xyz]: CEF:Version|Device Vendor|Device Product|Device
Version|Device Event Class ID|Name|Severity|[Extension]
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
```

Common header

1. All syslog messages start with a timestamp and the string "`Center cybervision[xyz]:`".

   For example:

   ```
   2021-01-12T09:57:50.986718+00:00 Center cybervision[5485]:
   ```

   Here the timestamp is in RFC3164 Unix format.

2. CEF syslog messages have the same format, which consists of a list of fields separated by a “|”, such as:

   ```
   CEF:Version|Device Vendor|Device Product|Device Version| Device Event Class
   ID|Name|Severity|
   ```

   For example:

   ```
   CEF:0|Cisco|Cyber Vision|1.0|component_new|New component detected|2|
   ```

   The following fields have a fixed value:

   - “`CEF:Version`”: will always be “`CEF:0`”
   - “`Device Vendor`”: “`Cisco`”
   - “`Device Product`”: “`Cyber Vision`”

- “`Device Version`”: “`1.0`”

Then, the fields below vary depending on the message type:

- `Device Event Class ID`: ID of the event type.
- `Name`: name of the event type.
- `Severity`: severity of the event type.

Refer to the annex appended at the end of this document to see examples of syslog messages contaning these fields.

Finally, there are 4 types of severities:

- “0”: Low
- “1”: Medium
- “2”: High
- “3”: Critical

Extension

The extension part is made of two fixed fields and several optional fields.

Fixed extension fields

The extension starts with two fixed fileds which are:

- “cat”: Category of the event
- “msg”: Message

For example:

```
cat=Inventory Events msg=New component detected on the network: IP 192.168.69.205, MAC
d0:ec:35:ca:96:2a, vendor Cisco
```

The value of the category key is a string which can be one of the following values:

- Security Events
- Control Systems Events
- Inventory Events
- Cisco Cyber Vision Administration
- Cisco Cyber Vision Operations
- Cisco Cyber Vision Configuration
- Anomaly detection
- Signature Based Detection

- Extension-based alert
- Protocol Events

Messages' structure will be linked to the event type and will contain variable values like IP and MAC addresses.

For example:

- User 'John Smith' has logged into Cisco Cyber Vision
- Failed attempt to log in with the user 'admin@sentryo.net' (ip: 192.168.72.101)
- Baseline 'label' got 1 difference on 1 item
- New component detected on the network: IP 1.2.3.4, MAC aa:bb:cc:dd:ee:ff

Optional extension fields

After the ‘msg’ fields, several other fields can be found with relevant information for the event type.

For example:

- user_login_fail

  ```
  suser=admin@sentryo.net src=192.168.72.101
  ```

- user_login

  ```
  suser=admin@sentryo.net spriv=Administrator SCVEventType=user_login
  SCVAuthorId=3b56a1a9-e438-4037-a2ef-31509cc0367a
  ```

- component_new

  ```
  src=192.168.72.19 smac=00:0c:29:6f:e6:de SCVEventType=new_component
  SCVComponentId=19543bc9-f0c6-51c3-8bdf-2b2aa5d3d161
  SCVSensorId=0ab5830d-fe1a-46c3-842d-310662508ae6
  ```

- communication_new

  ```
  cmp-a-mac=00:0c:29:6f:e6:e8 cmp-b-mac=d0:ec:35:ca:96:2a cmp-a=192.168.69.1
  cmp-b=192.168.69.205 cmp-a-port=50630 cmp-b-port=22 SCVEventType=flow_new
  SCVFlowCmpAComponentId=e19e4522-5e28-5f2d-a96e-60a7997b322f
  SCVFlowCmpBComponentId=700f809f-fb3a-544d-a364-526f7b70f01b
  SCVFlowCommunicationType=REMOTE_ADMIN SCVFlowId=a0a23d42-e30b-57b5-903c-04669a1755ad
  SCVSensorId=0ab5830d-fe1a-46c3-842d-310662508ae6
  ```

All event types are listed at the end of this document. For some event types, some details are given below.

Component metadata

If the event is associated with a component, an additional component-id key is present. The value is the SCVComponentId (as a string) of the component in the Cisco Cyber Vision database. Component data can be queried via the Cisco Cyber Vision API using this SCVComponentId.

Flow metadata

If the event is associated with a flow, the following additional keys are present:

- **SCVFlowId:**

  ID of the flow

- **SCmp-a:**

  IPv4 or IPv6 IP address of component A

- **SCmp-a-mac:**

  MAC address of component A

- **SCmp-a-port:**

  Port number of component A

- **SCmp-b:**

  IPv4 or IPv6 IP address of component B

- **SCmp-b-mac:**

  MAC address of component B

- **SCmp-b-port:**

  Port number of component B

- **Sflow-properties:**

  a string containing a comma-separated list of additional properties for the flow. The properties are protocol-dependent and cannot be exhaustively enumerated in this document.

Important fields

SCVSensorId:

The value of sensor ID corresponds to the one from where the event was captured. It is the sensor ID that can be shown in ‘sbs-sensor’ command output.

We can see that property only on data captured from sensors, it’s hidden for login events for example.