Syslog Cef User Guide

CB v4.2.4.150206.1225

February 06, 2015

Contents

Syslog Common Event Format

Background

The Common Event Format is a standard by ArcSight to align the output format of the various technology vendors into a common form.

Carbon Black Watchlist Syslog output supports fully templated formats, so modifying the template to match the CEF-defined format is simple.

Applying the default CEF templates

There are CEF syslog templates at `/usr/share/cb/syslog_templates`. To use them, add the following lines to cb.conf:

```
WatchlistSyslogTemplateProcess=/usr/share/cb/syslog_templates/process_cef.txt
WatchlistSyslogTemplateBinary=/usr/share/cb/syslog_templates/binary_cef.txt
```

The watchlist searcher process will automatically pick up the new template at the next watchlist hit.

An example Process Watchlist hit in CEF format:

```
CEF:0|Carbon Black|Carbon Black|4.1.0.131118.1540|reason=process_watchlist_-1|
SyslogTest|10|dproc=wmiprvse.exe fname=c:\\windows\\system32\\wbem\\wmiprvse.exe
start=2014-01-14T20:36:19.526Z dhost=J-8205A0C27A0C4 msg=group:Default Group
process_md5:0ffae66e6d5b1c87cbd22d1f3b6079fd last_update:2014-01-14T20:36:19.526Z
guid:-5850106436655859636 segment_id:1
```

An example Binary Watchlist hit in CEF format:

```
CEF:0|Carbon Black|Carbon Black|4.1.0.131118.1540|reason=binary_watchlist_-1|
SyslogTest|10|start=2014-01-13T14:49:55.189Z msg=md5:6D778E0F95447E6546553EEEA709D03C
desc:Windows Command Processor company_name:Microsoft Corporation
product_name:MicrosoftÂ:registered: WindowsÂ:registered: Operating System
product_version:5.1.2600.5512 file_version:5.1.2600.5512 (xpsp.080413-2111)
signed:Signed
```

Extension Dictionary

The CEF specification is heavily influenced by network device vendors and, to a lesser extent, host-based Antivirus products. Products like Carbon Black, with rich endpoint visibility, did not exist when the specification was developed and, as a result, the built-in key names supported by the Extension Dictionary do not map well to the data in Carbon Black.

In the default template, we have chosen to use the catch-all `msg` parameter for the fields that do not map well to the specified list of default keys. This both limits required configuration as well as avoids the limitations of custom extensions.

If you would like to use custom extension keys, you can configure your SIEM device to support the custom keys and modify the Carbon Black default CEF template as desired. Details are available in the CEF specification and the Carbon Black document Syslog Templating. Contact your support representative with any questions.