Carbon Black - ArcSight Logger | Syslog Connector

### **ArcSight Setup**

***NOTE***: If you already have a Syslog connector you can skip to Carbon Black Setup

* Create a UDP receiver
  + Log into the logger web console **https://Logger IP Address:443**
  + Click on the **Configuration tab**
  + On the left select **Event Input**
  + Click Add
  + Name the receiver and select **UDP Receiver | CEF UDP Receiver**
  + Hit next
  + Select all if you have more than one IP on the logger available or the specific IP you want to use for the receiver.
  + For the port use any other dynamic port other than 514(this is for preference, you can use 514 if it is available)
  + Under source type select **Syslog** or select **CEF**(this will depend if you are going to use the default CEF templates available in carbon black or generate your own syslog templates. Also note that Syslog will still parse the CEF events)
  + Hit Save
  + Enable the receiver

### **Carbon Black Setup**

* SSH into the carbon black server **“ssh root@carbonblackserver”**
* Modify the cb.conf file location with vi or other preferred editor **“vi /etc/cb/cb.conf”**
* Go to the bottom of the page and add the below lines to tell the watchlist searcher to use the default templates provided for CEF. NOTE: Do not put spaces between any part of a syntax line e.g. text = text(wrong), text=text(correct)

**WatchlistSyslogTemplateProcess=/usr/share/cb/syslog\_templates/process\_cef.txt**

**WatchlistSyslogTemplateBinary=/usr/share/cb/syslog\_templates/binary\_cef.txt**

* Save the file
* Restart the enterprise services **“service cb-enterprise restart”**
* Go to the carbon black rsyslog: **NOTE**: this is not the regular rsyslog service but rsyslog service for carbon black. **“ vi /etc/rsyslog.d/cb-coreservices.conf”**
* Locate the Line **“if $programname == ‘cb-notifications’ then /var/log/cb/notifications/cb-all-notifications.log;CbLogFormatWithPID”**
* Add the line **“& @ArcSight Logger IP:UDP Port; CbLogFormatWithPID”**
* Also do the same for the line **“if $programname == ‘cb-notifications-’ then ?DynaFile;CbLogFormatWithPID”**
* Add the line **“& @ArcSight Logger IP:UDP Port; CbLogFormatWithPID”**

***NOTE***:   I choose to add this line because different watchlists have separated logs based on the number assigned to the watchlist. this allows you to collect all watchlist hits. If you just need specific add the entire name of the watchlist log you want by confirming the number from the web UI and locating it in /var/log/cb/notifications folder. e.g. “if $programname == ‘cb-notifications-####.log-#######’ then ?DynaFile;CbLogFormartWithPID”

* When edited correctly this is how it will look:

**if $programname == ‘cb-notifications’ then /var/log/cb/notifications/cb-all-notifications.log;CbLogFormatWithPID**

**& @ArcSight Logger IP:UDP Port; CbLogFormatWithPID**

**& ~**

**if $programname == ‘cb-notifications-’ then ?DynaFile;CbLogFormatWithPID**

**& @ArcSight Logger IP:UDP Port; CbLogFormatWithPID**

**& ~**

* Restart the rsyslog service **“service rsyslog restart”**
* Generate some traffic to test the templates by using the cbsyslog utility

**/usr/share/cb/cbsyslog –f –e watchlist.hit.process**

**OR**

**/usr/share/cb/cbsyslog –f –e --event watchlist.hit.process**

* This generates a log entry that will be pushed to the ArcSight Logger on the next transfer interval.
* Or Create traffic that will get flagged by a watchlist

#### 

#### **Troubleshooting**

If you do not receive the logs in ArcSight Logger do one of the below:

* Verify that the traffic is indeed being sent to the Logger.
* If you do not receive any events on the Logger verify the port receiver on the logger is open on the Logger local Firewall
* Verify there is a route and open port rule if a Firewall is present between the Carbon Black server and ArcSight.