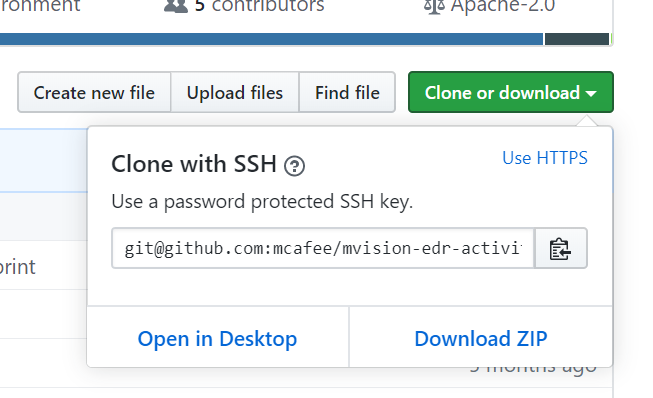
**[FORWARDER] Activity Feed install for ubuntu1804LTS, rsyslog & splunk (quick guide):**

1.Go to <https://github.com/mcafee/mvision-edr-activity-feed> and download it and unzip it (latest code from master branch):



2.[Pre requisite: Install python 2.7, 3.5, 3.6 or 3.7] (suggested 2.7).

3.[Pre requisite: Depending on the python version installed it might be needed to install setuptools package, this is> *sudo apt-get install python-setuptools* (suggested version) or *sudo apt-get install python3-setuptools*]

4. Go to the directory where AF was downloaded and unzipped and Run the following setup command inside mvision-edr-activity-feed directory (installation should succeed)> *sudo python setup.py install*

5.[Pre requisite: rsyslog should be installed by default under ubuntu> *rsyslogd -v*]. Edit rsyslog.conf located under /etc/rsyslog.conf running for instance> *sudo vim /etc/rsyslog.conf* and add the following line before Modules section \*.\* @SPNLUNK\_IP\_HERE:514 (as it will be installed under the same machine then it should be \*.\* @127.0.0.1:514); additionally, please enable reception of udp and tcp under Modules section (normally commented by default):

module(load="imudp")

input(type="imudp" port="514")

module(load="imtcp")

input(type="imtcp" port="514")

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |

Syslogs are being placed under /var/log/. Further details of how a rsyslog.conf file looks like can be observed here: <https://github.com/mcafee/mvision-edr-activity-feed/blob/master/rsyslog.conf>

7.Run the following command for restarting rsyslog and taking the changes> sudo service rsyslog restart

8.Go to the directory where AF was downloaded and unzipped and Run the following command inside mvision-edr-activity-feed directory> *sudo mvision-edr-activity-feed --url https://api.soc.mcafee.com/ --username 0812toe6@mvisionedr.technology --password MFEpoctnyGpGgsPf\!6 --module samples.splunk --loglevel=debug* (please notice it’s necessary to scape special chars set under password section, in this case “!” is being preceded with “\” in order to be interpreted by the system). At this point the system should be running and printing in console valid information (as mentioned before, rsyslog configuration will be completed in next section)

**[SPLUNK SERVER] Splunk8 install for ubuntu1804LTS (same machine: all in one method):**

9.Download splunk enterprise 8 for linux: <https://www.splunk.com/en_us/download/splunk-enterprise.html#tabs/linux> (select the file with extension “.deb”)

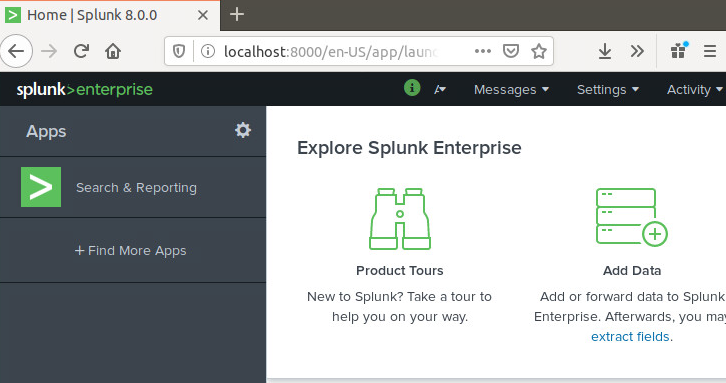
10.Run the following command on the temporal location where the “.deb” file was downloaded> *sudo dpkg -i splunk-8.[SETMINORVERSIONHERE]-linux-2.6-amd64.deb*

11.Go to /opt/splunk/bin/ (the location where splunk start scripts were was installed) and run> *sudo ./splunk enable boot-start* (license agreement will be requested pressing “y”).

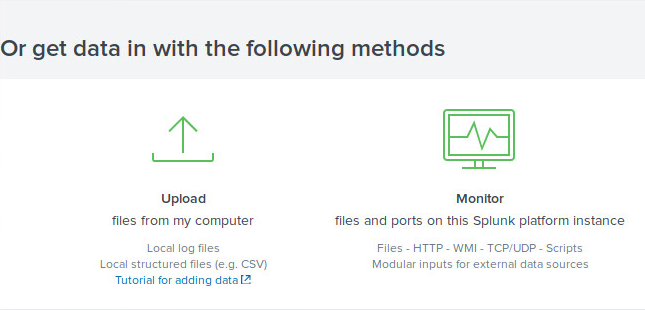
12.Run the following command for starting the main process> *sudo service splunk start* (the creation of the user and password for accessing the console is being requested here and it will be used in next step).

13.Open a browser and go to IP\_WHERE\_SPLUNK\_SEVER\_IS\_INSTALLED:8000 (If splunk was installed successfully then the console will be displayed and requesting the user and password created in previous step).

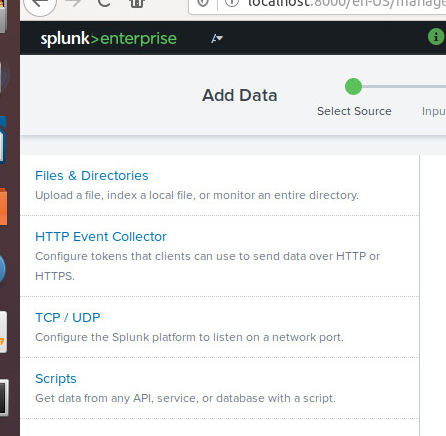
14.Once logged, click in Add Data section:



15.Once Add Data section is open click on Monitor section:



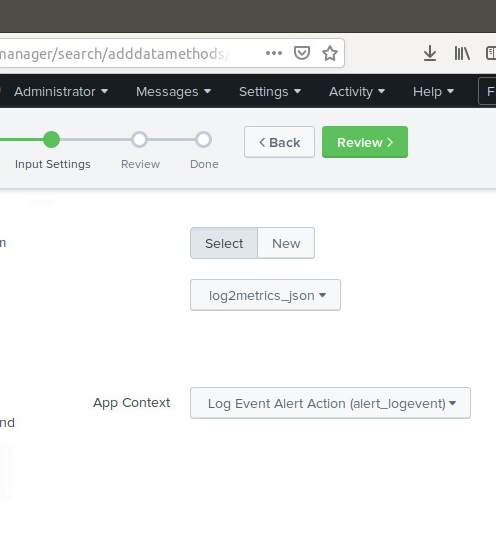
16.Then, once Monitor sections is open click on TCP/UDP section:



17.Then for this 1st interaction UDP protocol will be enabled but consider that TPS over TLS can also be enabled (514 port is suggested by default). The recommendation is to try the 1st approach to verify connectivity and then try with a more secured method if plain communication was OK.

18.Click on Next button to display Input Section.

19. Under the Input Section select: Structured -> json, then Ap Context=Log Event Alert Action, Method=Custom->Host Filed Value=IP and Index=default.



20.Click Review buthon & if information displayed is OK then press Submit (otherwise click on back and for correcting settings).

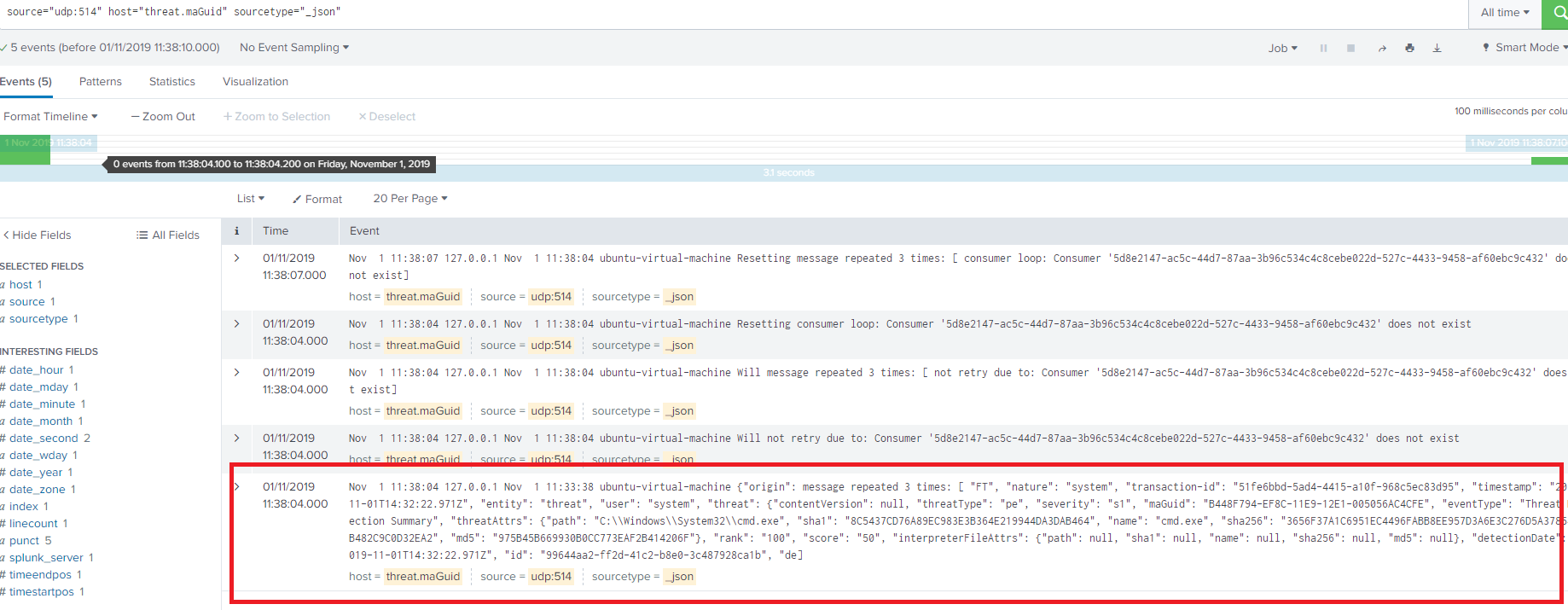
21.Go to to Start Searchng page and leave the page open and select the Job to gather Data created recently.

**[THREATS DISPLAY AS ALERTS]:**

22.[Pre requisite: execute a threat under one of the endopints monitored by ePO].

23.[Optional but it can be used for troubleshooting if threats aren’t displayed under Splunk]Go to MVEDR UI -> Monitoring section and verify threats detected (recently created threat w/high score will be displayed here).

24.Go to the page opened in step 21 (Splunk Searching -> Job recently created for gathering UDP data in json format). A success result will be displayed showing MVEDR Threats as its displayed here:



25.Doing a specific search is more appropiate for dislaying Threats if desired, for instance (this query can be used as input for making a narrowed alert):

source="udp:514" sourcetype="\_json" Threat Detection

