**Log Dropping Playbook**

Please follow the defined methods to stop the logging of following Events

**Type:** Windows Filtering Platform

**Events:**

* **5154**: The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
* **5158**: The Windows Filtering Platform has permitted a bind to a local port.

**Step 1**

Locate the ***ossec.conf*** file in ***C:\Program Files (x86)\ossec-agent\ossec.conf***

**Step 2**

Locate these tags in the configuration file as highlighted in the image below

*<location>Security</location>*

*<log\_format>eventchannel</log\_format>*



**Step 3**

Add ***EventID != 5154 and EventID!= 5158*** to the list of suppressed event IDs already present there.

<localfile>

<location>Security</location>

<log\_format>eventchannel</log\_format>

<query>Event/System[EventID != 5154 and EventID!= 5158]</query>

</localfile>

**Step 4**

Restart the ossec agent service