Usecase 6- Attempt to Use a Blocked Application

Objective: Detect and create an alert when Windows Firewall blocks an attempt to use Chrome to create a connection

Log Source: Windows Security Event Logs

Event ID: 5157- “Windows Filtering Platform has blocked a connection”

Example Target Log From Event Viewer:

The Windows Filtering Platform has blocked a connection.

Application Information:
- Process ID: 21136
- Application Name: \device\harddiskvolume3\program files\google\chrome\application\chrome.exe

Network Information:
- Direction: Outbound
- Source Address: <host address>
- Source Port: 49968
- Destination Address: <destination address>
- Destination Port: 53
- Protocol: 17
- Interface Index: 11

Filter Information:
- Filter Origin: {8C6BCEC2-28A9-4D9E-B437-D8F2969B6A9C}
- Filter Run-Time ID: 193153
- Layer Name: Connect
- Layer Run-Time ID: 48
- Remote User ID: NULL SID
- Remote Machine ID:NULL SID
- Original Profile: Public
- Current Profile: Public
- Is Loopback: False
- Has Remote Dynamic Keyword Address: False

Pre-configuration: enable 5157 rules via the powershell command auditpol /set /subcategory:"Filtering Platform Connection" /failure:enable> to create a firewall rule blocking connection originating from chrome go into the firewall, outbound rules, rule type program, enter the program path, select block the connection, select which options are appropriate for when the rule applies then name it.

Custom Wazuh Rule:

```
<group name="windows, windows_security,">
    <rule id="100117" level="5">
    <if_sid>60104</if_sid>
    <field name="win.system.eventID">^5157$</field>
    <field name="win.eventdata.application">^\\\\device\\\\harddiskvolume3\\\\program files\\\\google\\\\chrome\\\\application\\\\chrome\
.exe$</field>
    <description>Windows Firewall blocked Chrome.</description>
    </rule>
</group>
```

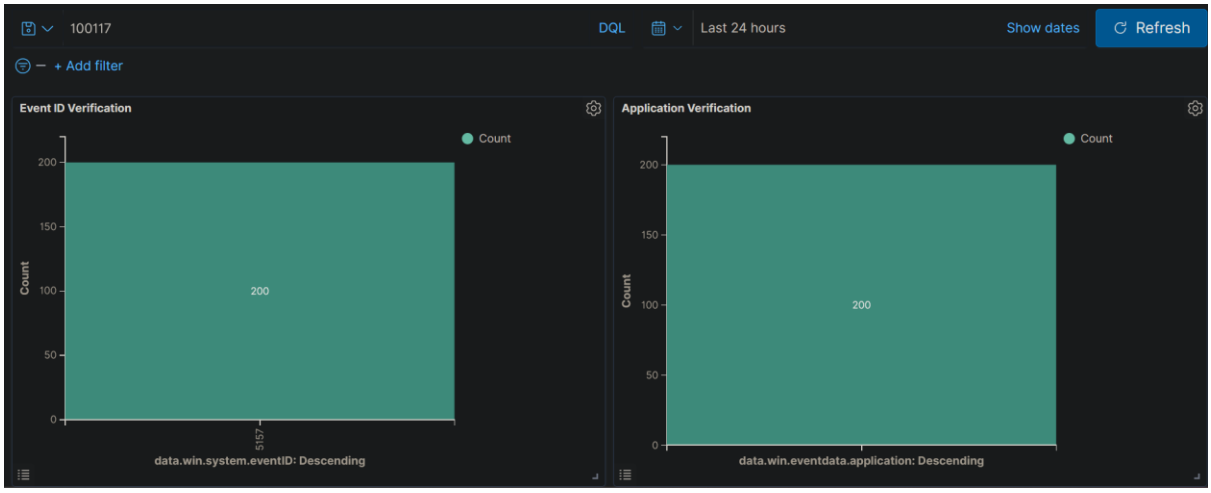
Sid 60104 is for any audit failure event

```
<rule id="60104" level="5">
  <if_sid>60001</if_sid>
  <field name="win.system.severityValue">^AUDIT_FAILURE$|^failure$</field>
  <description>Windows audit failure event</description>
  <group>pci_dss_10.6.1,gdpr_IV_35.7.d,hipaa_164.312.b,nist_800_53_AU.6,tsc_CC7.2,tsc_CC7.3,</group>
  <options>no_full_log</options>
</rule>
```

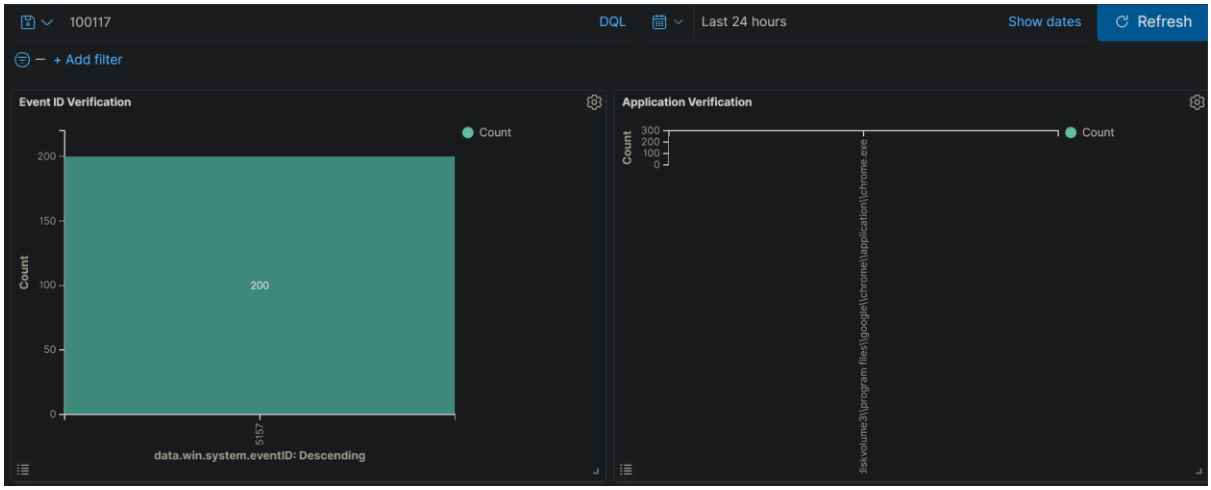
From these audit failure events, further filtering is done, including for system.eventID being 5157 and the eventdata.application being \device\harddiskvolume3\program files\google\chrome\application\chrome.exe

Example Alerts:

Verification of fields:



Label for application name is hidden because if it isn't the graph looks like this, however it works for verification because of there only being one term for the application


100117
DQL
Last 24 hours
Show dates
Refresh
+ Add filter
Event ID Verification
Count
200
150
100
50
0
Count
200
5157
data.win.system.eventID: Descending
Application Verification
300
200
100
0
Count
Count
#\skvolume3\\program files\\google\\chrome\\application\\chrome.exe