**Usecase 6- Blocked Attempt to use Chrome**

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:

A black background with text

AI-generated content may be incorrect.

Sid 60104 is for any audit failure event

A computer code on a black background

AI-generated content may be incorrect.

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:

A screenshot of a computer

AI-generated content may be incorrect.

Verification of fields:

A screenshot of a computer

AI-generated content may be incorrect.

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

A screenshot of a computer

AI-generated content may be incorrect.