**Usecase 4- Failed Remote Logon Attempt**

Objective: Create an alert when a remote logon attempt fails

Log Source: Windows Security Event Logs

Event ID: 4625- “Account failed to logon”

Example Target Log From Event Viewer:

An account failed to log on.

Subject:

Security ID: SYSTEM

Account Name: <system name>$

Account Domain: WORKGROUP

Logon ID: 0x3E7

Logon Type: 8

Account For Which Logon Failed:

Security ID: NULL SID

Account Name: <account name>

Account Domain: <system name>

Failure Information:

Failure Reason: Unknown user name or bad password.

Status: 0xC000006D

Sub Status: 0xC000006A

Process Information:

Caller Process ID: 0x2638

Caller Process Name: C:\Windows\System32\OpenSSH\sshd.exe

Network Information:

Workstation Name: <system name>

Source Network Address: -

Source Port: -

Detailed Authentication Information:

Logon Process: Advapi

Authentication Package: Negotiate

Transited Services: -

Package Name (NTLM only): -

Key Length: 0

Pre-configuration: configuration of OpenSSH: run on powershell with admin privileges “Add-WindowsCapability -Online -Name OpenSSH.Server”> enable SSH connection through firewall with this “New-NetFirewallRule -Name sshd -DisplayName "OpenSSH Server (sshd)" -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22”> start the SSH server with Start-Service sshd> run the command Start-Service sshd <host username>@<host ip address> <host password> on the machine you want to establish the connecion with

Custom Wazuh Rule:

A screen shot of a computer code

AI-generated content may be incorrect.

Sid 60122 is for unsuccessful logon attempts

A computer screen shot of a code

AI-generated content may be incorrect.

Of these unsuccessful logon logs, win.system.eventID is event ID 4625 along with win.eventdata.logonType is 3 (network logon), 8 (network cleartext, meaning network logon without authentication) or 10 (RDP/terminal services) filters for the logs with the relevant logon types related to remote logons.

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.