**Usecase 5- Successful Remote Logon Attempt**

Objective: Create an alert when a remote logon attempt succeeds

Log Source: Windows Security Event Logs

Event ID: 4624- “Account was successfully logged on”

Example Target Log From Event Viewer:

An account was successfully logged on.

Subject:

Security ID: SYSTEM

Account Name: <system name>$

Account Domain: WORKGROUP

Logon ID: 0x3E7

Logon Information:

Logon Type: 3

Restricted Admin Mode: -

Remote Credential Guard: -

Virtual Account: No

Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:

Security ID: <system name>\<account name>

Account Name: <account name>

Account Domain: W11AGENT

Logon ID: 0xC3C1B8

Linked Logon ID: 0x0

Network Account Name: -

Network Account Domain: -

Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

Process ID: 0x2638

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

Network Information:

Workstation Name: -

Source Network Address: -

Source Port: -

Detailed Authentication Information:

Logon Process: sshd

Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0

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:

Sid 60122 is for unsuccessful logon attempts

A screen shot of a computer code

AI-generated content may be incorrect.  
Sid 60106 is for successful logon attempts

A black background with white text

AI-generated content may be incorrect.

Of these successful logon logs, win.system.eventID is event ID 4624 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.