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

```
<group name="windows, windows_security,">
    <rule id="100116" level="13">
    <if_sid>60106</if_sid>
    <field name="win.system.eventID">^4624$</field>
    <field name="win.eventdata.logonType">^3$|^8$|^10$</field>
    <description>Successful Remote Login Detected</description>
    </rule>
</group>
```

Sid 60106 is for successful logon attempts

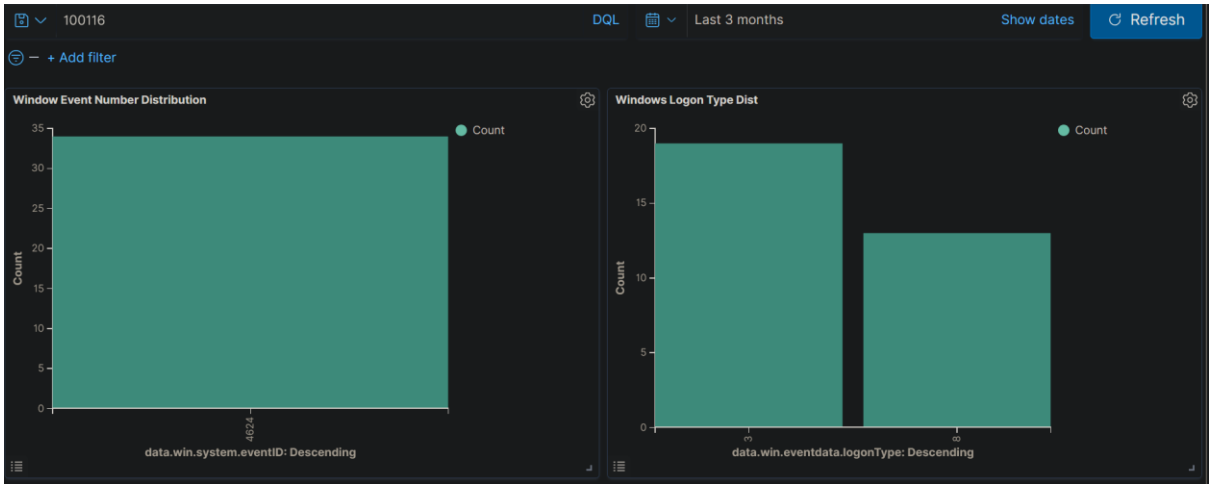
```
<rule id="60106" level="3">
  <if_sid>60103</if_sid>
  <field name="win.system.eventID">^528$|^540$|^673$|^4624$|^4769$</field>
  <description>Windows Logon Success</description>
  <options>no_full_log</options>
  <group>authentication_success,pci_dss_10.2.5,gpg13_7.1,gpg13_7.2,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7
      ,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
  <mitre>
    <id>T1078</id>
  </mitre>
</rule>
```

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:

	timestamp	agent.name	rule.description	data.win.system.eventID	data.win.eventdata.logonType
	Jul 3, 2025 @ 14:49:31.839	W11-VM_agent	Successful Remote Login Detected	4624	8
	Jul 3, 2025 @ 14:49:27.426	W11-VM_agent	Successful Remote Login Detected	4624	3
	Jul 2, 2025 @ 21:35:00.654	W11-VM_agent	Successful Remote Login Detected	4624	8
	Jul 2, 2025 @ 21:34:51.346	W11-VM_agent	Successful Remote Login Detected	4624	3
	Jul 2, 2025 @ 21:28:40.578	W11-VM_agent	Successful Remote Login Detected	4624	3

Verification of fields:


100116
DQL
Last 3 months
Show dates
Refresh
+ Add filter
Window Event Number Distribution
Count
35
30
25
20
15
10
5
0
4624
data.win.system.eventID: Descending
Windows Logon Type Dist
Count
20
15
10
5
0
3
8
data.win.eventdata.logonType: Descending