Windows Logging for SOC

Windows log: C:\Windows\System32\winevt\Logs\...
all of the logs are in binary

So we will use Event Viewer (eventvwr)

Event ID → 4624 (successful logon)
Purpose → Detect Remote Desktop protocol/network logins and identify the attack starting point

~~Logging~~

Event ID → 4625 (failed logon)

→ 4634 (Logoff)

→ 4688 (it tells what program started who started)

→ 4648 (Logon attempt using explicit credential)

→ 4720 (User account was created)
→ 4722 (User account was enabled)
→ 4738 (User account was changed)

→ 4725 (User account was disabled)
→ 4726 (account deleted)

→ 4723 (changed password)
→ 4724 (password reset)

4732 → (user added a security group)
4733 → (user removed from a security group)

Sysmon
1 → Sysmon Process creation
11 → File Creation :
13 → Registry Value Set
3 → Network Connection
22 → DNS Query