SentinelX Weekly Forensic Report

Generated: 22-06-2025 19:37:35

Time	Severity	Source	Message	IP Address

2025-06-22 19:34:22	Info	SecurityLog	Successful login: An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:SHA$ Account Domain:WORKGROUP Logon ID:0x3e7 Logon Information: Logon Type:5 Restricted Admin Mode:- Remote Credential Guard:- Virtual Account:%%1843 Elevated Token:%%1842 Impersonation Level:%%1833 New Logon: Security ID:S-1-5-18 Account Name:SYSTEM Account Domain:NT AUTHORITY Logon ID:0x3e7 Linked Logon ID:0x0 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x4a4 Process Name:C:\Windows\System32\services.exe Network Information: Workstation Name:- Source Network Address:-	

			Source Port:- Detailed Authentication Information: Logon Process:Advapi Authentication Package:Negotiate Transited Services:- Package Name (NTLM only):- Key Length:0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in	

			some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.	