Windows auditing baseline

Author: mdecrevoisier
Version: 2022.04.15
Status: stable

Disabled event log

Noisy subcategory

Network related

Classic event log
- System
- Security
- Application

SYSMON
- Microsoft-Windows-Sysmon/Operational — Event log

SMB
- Client — Event log
  - Microsoft-Windows-SMBClient/Audit
  - Microsoft-Windows-SMBClient/Security
  - Microsoft-Windows-SMBClient/Connectivity
  - Microsoft-Windows-SMBClient/Operational
- Server — Event log
  - Microsoft-Windows-SMBServer/Audit
  - Microsoft-Windows-SMBServer/Security
  - Microsoft-Windows-SMBServer/Connectivity
  - Microsoft-Windows-SMBServer/Operational
- File Share
  - Security — Event log
    - Network share object was accessed — ID 5140 (Limited information. Prefer ID 5145)
    - A network share object was added — ID 5142
    - A network share object was modified — ID 5143
    - A network share object was deleted — ID 5144
  - Audit File Share (S/F) — Audit policy
- File Share (advanced)
  - Network share object was checked — ID 5145 (Provides more info. than ID 5140) — Security — Event log
  - Audit Detailed File Share (S/F) — Audit policy

Firewall configuration
- Firewall rules (basic)
  - A rule was added — ID 4946
  - A rule was modified — ID 4947
  - A rule was deleted — ID 4948
  - Security — Event log (Limited information. Use instead the "Advanced Security Firewall" event log)
  - Audit MPSSVC Rule-Level Policy Change (S/F) — Audit policy
- Firewall rules (advanced)
  - A rule was added — ID 2004
  - A rule was modified — ID 2005
  - A rule was deleted — ID 2006
  - Microsoft-Windows-Windows Firewall With Advanced Security/Firewall — Event log
- Configuration changes
  - Security — Event log
  - Audit Filtering Platform Policy Change (S/F) — Audit policy (Mainly about IPsec VPN)
  - Audit MPSSVC Rule-Level Policy Change (S/F) — Audit policy

Network flow
- Flow events
  - Security — Event log
  - Audit Filtering Platform Packet Drop (S/F) — Audit policy
  - Audit Filtering Platform Connection (S/F) — Audit policy
- File (TXT)
  - %systemroot%\system32\LogFiles\Firewall\pfirewall.log — File (TXT) (Limited information)
- Process connection
  - Microsoft-Windows-Sysmon/Operational — Event log (Network connection — ID 3)
- RPC traffic
  - zeronetworks / rpcfirewall (3rd party) — Event log

RDP server activity
- Event log
  - Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
    - Client timezone is [I] hour from UTC — ID 104
    - The server accepted a new UDP/TCP connection from client [IP]:PORT — ID 131
    - The resolution requested by the client: Monitor I: [X x Y] — ID 168
    - The client operating system type is (1, 3) > Server [SERVER] — ID 169
  - Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
    - RDS: Session logon succeeded — ID 21
    - RDS: Session reconnection succeeded — ID 25
  - Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
    - RDS: User authentication succeeded — ID 1149

RDP client activity
- Event log
  - Microsoft-Windows-TerminalServices-RDPClient/Operational
    - RDP ClientActiveX is trying to connect to the server [SERVERX] — ID 1024
    - Base64(SHA1(UserName)) — ID 1029

DNS client queries
- Event log
  - Microsoft-Windows-DNS-Client/Operational — DNS event — ID 3008 (Limited information. Prefer to use SYSMON)
  - Microsoft-Windows-Sysmon/Operational — DNS event — ID 22

Bits
- Event log
  - Microsoft-Windows-Bits-Client/Operational
    - BITS created a task — ID 3
    - BITS transfer completed — ID 4
    - BITS transfer job started with URL [URL] — ID 59
    - BITS transfer job stopped with URL [URL] — ID 60

OpenSSH
- Event log
  - OpenSSH/Operational — sshd: [message] — ID 4
  - OpenSSH/Admin

WinRM
- Event log — Microsoft-Windows-WinRM/Operational

Proxy
- Event log — Microsoft-Windows-WinINet-Config/ProxyConfigChanged — ID 5600

DHCP client
- Event log
  - Microsoft-Windows-Dhcp-Client/Admin
  - Microsoft-Windows-Dhcpv6-Client/Admin

Network profiles
- Event log — Microsoft-Windows-NetworkProfile/Operational

WLAN activity
- Event log — Microsoft-Windows-WLAN-AutoConfig/Operational

WinSock
- Event log — Microsoft-Windows-Winsock-WS2HELP/Operational

VPN (dlient)
- Event log — Microsoft-Windows-VPN-Client/Operational

VPN (IPsec)
- Event log
  - Security
  - Audit Filtering Platform Policy Change (S/F) — Audit policy

WMI / DCOM
- Event log
  - Microsoft-Windows-WMI-Activity
  - System — Provider: Microsoft-Windows-DistributedCOM

System
- System boot — Event log — System
  - Provider: User32
  - Provider: Microsoft-Windows-Kernel-General
  - Provider: Microsoft-Windows-Kernel-Boot
  - Provider: Microsoft-Windows-Kernel-Power
- Windows Event log / WEF-WEC — Event log
  - Microsoft-Windows-EventCollector/Operational — WEC server
  - Microsoft-Windows-Forwarding/Operational — WEF client
  - System — Event log status (Provider: Microsoft-Windows-Eventlog)
- Group Policy (GPO) — Event log
  - Provider: Microsoft-Windows-GroupPolicy — System
  - Microsoft-Windows-GroupPolicy/Operational
  - Microsoft-Windows-Security-Audit-Configuration-Client/Operational
- Time — Event log
  - Provider: Microsoft-Windows-Time-Service — System
  - Provider: Microsoft-Windows-Kernel-General — System
  - Microsoft-Windows-DateTimeControlPanel/Operational
  - Microsoft-Windows-Time-Service/Operational

Security related

Software & Updates
- Software — Event log
  - Application — Provider: Msiinstaller
  - Microsoft-Windows-Application-Experience/Program-Inventory
  - Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant — ID 17 — Program Compatibility Assistant execution
- Windows Update — Event log
  - Microsoft-Windows-WindowsUpdateClient/Operational
  - System — Provider: Microsoft-Windows-WindowsUpdateClient
  - Setup — Provider: Microsoft-Windows-Servicing
- Application crash — Event log — System
  - Provider: Application Error
  - Provider: Application Hang
  - Provider: Windows Error Reporting

Task & Service
- Task Scheduler
  - Event log
    - Security
      - ID 4698 — Schedule task created
      - ID 4699 — Schedule task deleted
      - ID 4700 — Schedule task disabled
      - ID 4701 — Schedule task enabled
      - ID 4702 — Schedule task modified
    - Microsoft-Windows-TaskScheduler/Operational
  - Audit policy — Audit Other Object Access Events (S/F)
- Services
  - Event log
    - Security
    - System — Provider: Service Control Manager
  - Audit policy — Audit Security System Extension (S/F)

(Limited information. Prefer ID 5145)

Security mitigations
- Event log
  - Microsoft-Windows-Security-Mitigations/KernelMode
  - Microsoft-Windows-Security-Mitigations/UserMode

Code integrity & Kernel drivers
- Event log
  - Microsoft-Windows-CodeIntegrity/Operational
    - System — Provider: Kernel-PnP — ID 219 — Failed kernel driver loading
    - Security
      - ID 5038 — Invalid image hash of a file
      - ID 6281 — Invalid page hash of an image file
      - ID 6410 — File does not meet requirements to load into a process.

DLL load
- Event log
  - System — Provider: Wininit — ID 11 — Custom DLL loaded for every application
  - Sysmon — ID 7 — Image loaded

BitLocker
- Event log
  - Microsoft-Windows-BitLocker/BitLocker Operational
  - Microsoft-Windows-BitLocker/BitLocker Management

Microsoft Office
- Event log — OAlerts

LSA
- Event log
  - Microsoft-Windows-CodeIntegrity/Operational
    - ID 3033, 3063 — Block mode for failed LSA plug-ins and drivers (Requires registry changes for auditing)
    - ID 3065, 3066 — Audit mode for failed LSA plug-ins and drivers (Requires registry changes for auditing)
  - Microsoft-Windows-LSA/Operational — ID 300 — Group assigned to new session
  - Security
  - System — Provider: Wininit — ID 12 — LSA started as a protected process

CVE
- Event log — System — Provider : Microsoft-Windows-Audit-CVE

Crypto
- Event log
  - Microsoft-Windows-Crypto-DPAPI/Operational
  - Microsoft-Windows-CAPI2/Operational

AppLocker
- Event log
  - Microsoft-Windows-AppLocker/MSI and Script
  - Microsoft-Windows-AppLocker/EXE and DLL
  - Application — Provider: Microsoft-WindowsSoftwareRestrictionPolices

Windows Defender
- Event log
  - Microsoft-Windows-Windows Defender/Operational
  - Microsoft-Windows-DeviceGuard/Operational

PowerShell
- Transcript logs (TXT)
- Event log
  - Microsoft-Windows-PowerShell/Operational
  - Windows PowerShell
  - Microsoft-Windows-PowerShell-DesiredStateConfiguration-FileDownloadManager/Operational
- Auditing settings
  - Module logging
  - Script block logging
  - Transcript

External device related
- Drivers
  - Eventlog
    - Log file (TXT) — C:\Windows\INF\SetupAPI.dev.log
    - Security
    - Microsoft-Windows-Kernel-PnP/Configuration
      - ID 400 — New mass storage installation
      - ID 410 — New mass storage configuration
    - Microsoft-Windows-DriverFrameworks-UserMode/Operational
    - Microsoft-Windows-Partition/Diagnostic
  - Audit policy — Removable storage (S/F)
- Printer — Event log
  - Microsoft-Windows-PrintService/Admin
  - Microsoft-Windows-PrintService/Operational
- RDP (device activity) — Event log
  - Microsoft-Windows-TerminalServices-ClientUSBDevices/Operational
  - Microsoft-Windows-TerminalServices-PnPDevices/Operational
  - Microsoft-Windows-TerminalServices-ServerUSBDevices/Operational