Windows auditing baseline

Author: mdecrevoisier
Version: 2022.01.25
Status: stable

Classic event log

- System
- Security
- Application

SYSMON

- Microsoft-Windows-Sysmon/Operational — Event log

Network related

SMB

- Event log
  - Client
    - Microsoft-Windows-SMBClient/Operational
    - Microsoft-Windows-SMBClient/Security
  - Server
    - Microsoft-Windows-SMBServer/Security
    - Microsoft-Windows-SMBServer/Operational
    - Microsoft-Windows-SMBServer/Audit
    - Security
  - Audit policy
    - Audit Detailed File Share (S/F)
    - Audit File Share (S/F)

Firewall

- File (TXT)
  - Optional
  - %systemroot%\system32\LogFiles\Firewall\pfirewall.log
- Event log
  - Security
  - Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
  - Microsoft-Windows-Sysmon/Operational
- Audit policy
  - Noisy
  - Audit Filtering Platform Packet Drop (S/F)
  - Audit Filtering Platform Connection (S/F)
  - Audit Filtering Platform Policy Change (S/F)
  - Audit MPSSVC Rule-Level Policy Change
- 3rd party
  - zeronetworks / rpcfirewall

RDP (session activity)

- Event log
  - Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
  - Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
  - Microsoft-Windows-TerminalServices-RDPClient/Operational
  - Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
  - Microsoft-Windows-TerminalServices-RDPClient/Operational

DNS client

- Event log
  - Microsoft-Windows-DNS-Client/Operational
  - Microsoft-Windows-Sysmon/Operational

Bits

- Event log
  - Microsoft-Windows-Bits-Client/Operational

OpenSSH

- Event log
  - OpenSSH/Operational
  - OpenSSH/Admin

WinRM

- Event log
  - Microsoft-Windows-WinRM/Operational

Proxy

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

https://nasbench.medium.com/finding-forensic-goodness-in-obscure-windows-event-logs-60e978ea45a3

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

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
  - WEC server
    - Microsoft-Windows-EventCollector/Operational
  - WEF client
    - Microsoft-Windows-Forwarding/Operational
  - Event log status
    - Provider: Microsoft-Windows-Eventlog
    - System

Group Policy (GPO)

- Event log
  - System
    - Provider: Microsoft-Windows-GroupPolicy
  - Microsoft-Windows-GroupPolicy/Operational
  - Microsoft-Windows-Security-Audit-Configuration-Client/Operational

Time

- Event log
  - System
    - Provider: Microsoft-Windows-Time-Service
    - Provider: Microsoft-Windows-Kernel-General
  - Microsoft-Windows-DateTimeControlPanel/Operational
  - Microsoft-Windows-Time-Service/Operational

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)

Security related

Windows Defender

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

AppLocker

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

CVE

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

Crypto

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

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

BitLocker

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

Microsoft Office

- Event log
  - OAlerts

Security mitigations

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

Code integrity & Kernel drivers

- Event log
  - Microsoft-Windows-CodeIntegrity/Operational
    - ID 3001-3004, 3010, 3023
  - 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

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

- Log file (TXT)
  - C:\Windows\INF\SetupAPI.dev.log
- Eventlog
  - 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

Disabled event log