Sysmon

- Microsoft의 Sysinternal suite에 포함된 시스템 모니터링 툴
- 기본 윈도우 이벤트 로그로는 한계가 있는 프로세스 생성, 네트워크 연결, 파일 생성 시간 변경 등의 정보를 추출한 후 윈도우 이벤트 저장소에 저장

* 이벤트 기반 정보가 아닌 '**행동 기반 정보'를 수집에서 이벤트 저장소에 저장**

Sysmon 기능

- 실행 프로세스와 부모 프로세스의 전체 명령 줄을 로그로 저장
- MD5, SHA1, SHA256 알고리즘으로 실행 프로그램의 해시 값을 기록
- 여러 종류의 해시 값을 동시에 기록
- 네트워크 연결에서 IP주소, 포트번호, 호스트명, 포트명 등을 기록
- 레지스트리에서 환경 설정이 변경된 경우 자동으로 다시 읽어 들임

Sysmon Installation

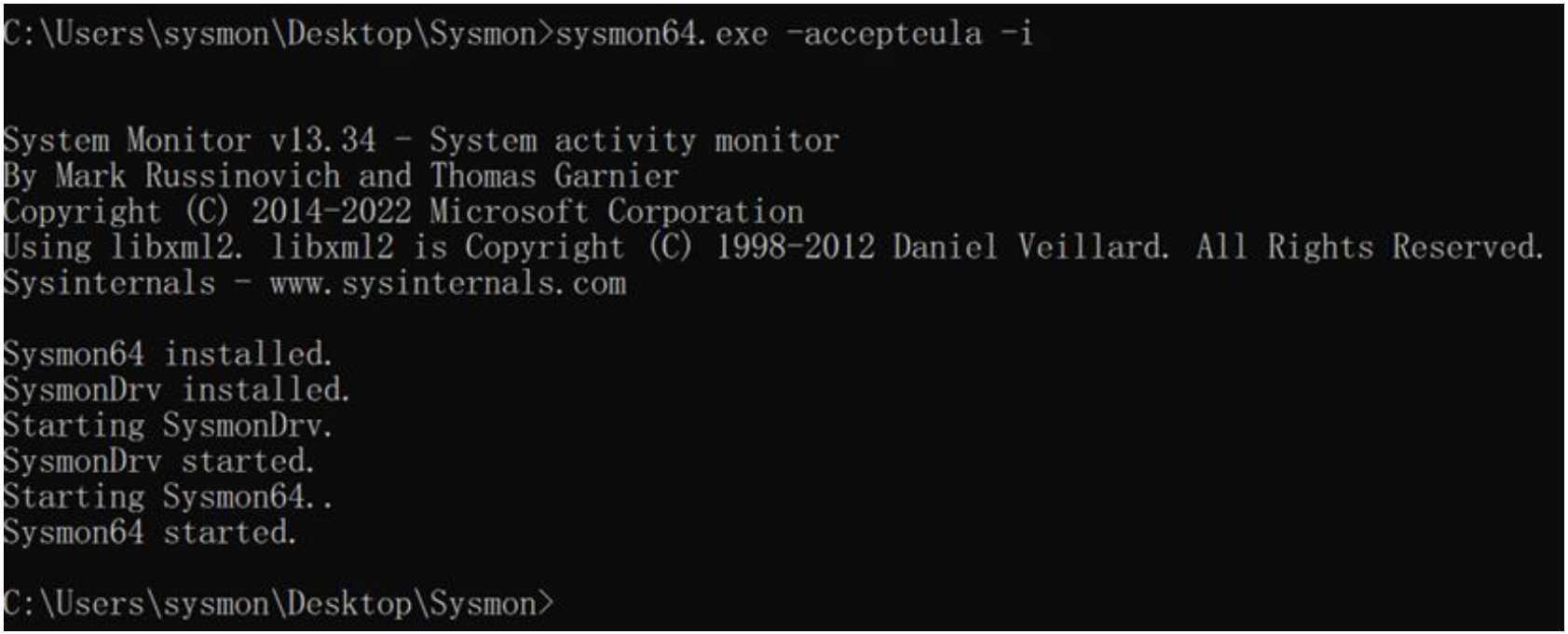
❶ 파일 다운로드 후 설치

https://download.sysinternals.com/files/Sysmon.zip

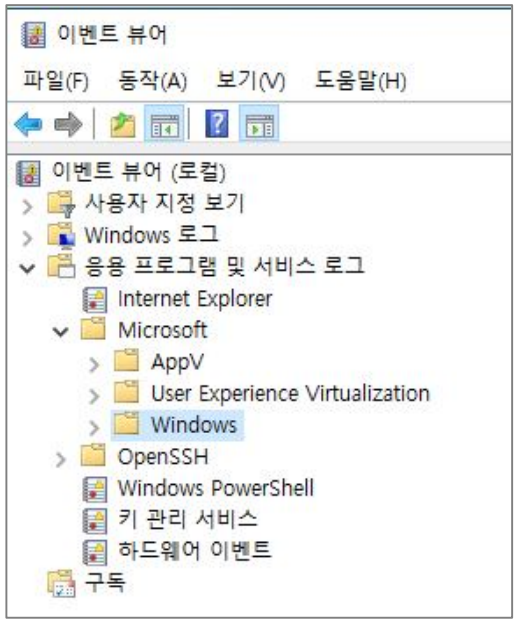
❷ sysmon 활성화

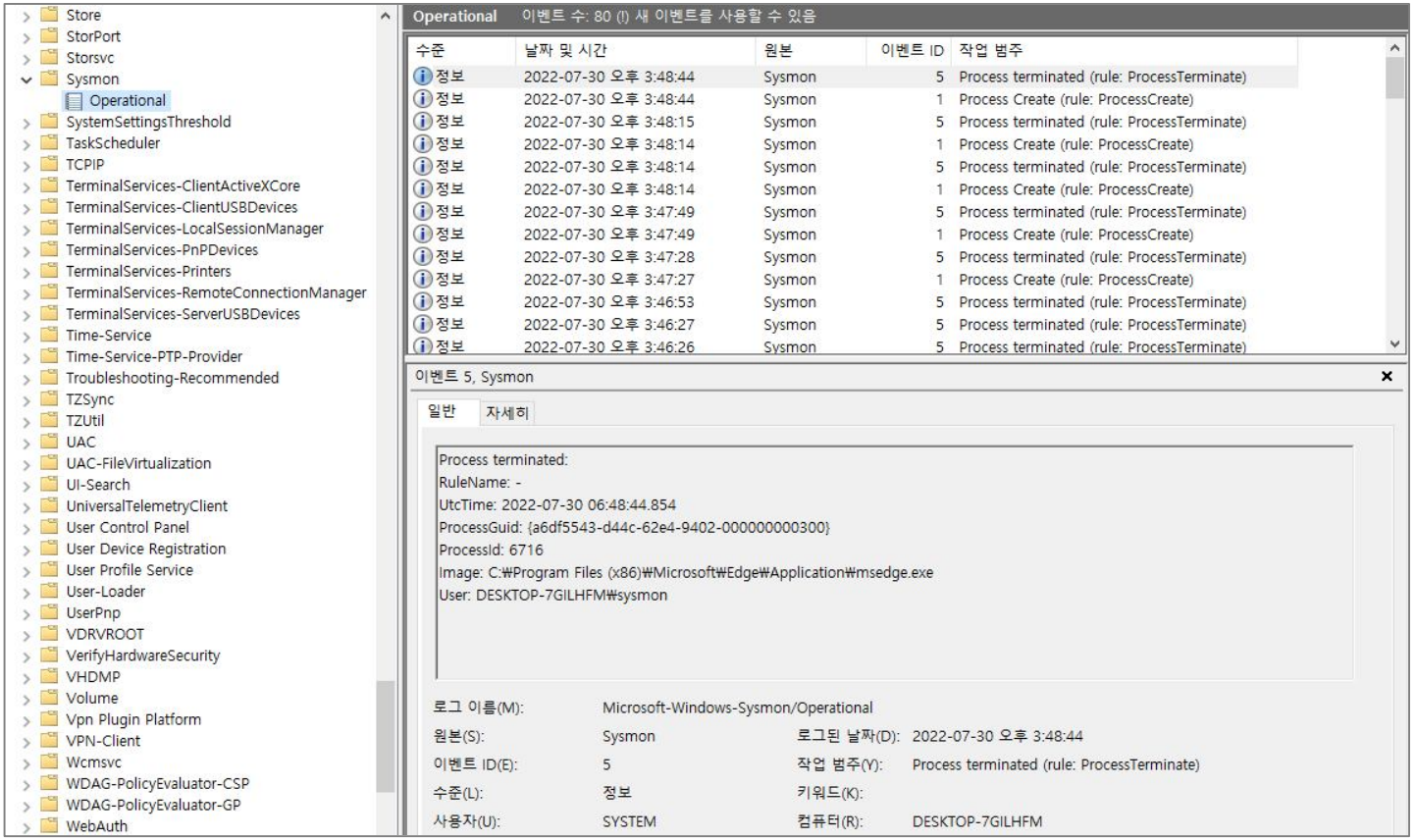
C:₩>cd /user₩sysmon₩desktop₩sysmon

C:₩> sysmon64.exe -accepteula -i



❸ 이벤트뷰어 확인


이벤트 뷰어
파일(F) 동작(A) 보기(V) 도움말(H)
이벤트 뷰어 (로컬)
사용자 지정 보기
Windows 로그
응용 프로그램 및 서비스 로그
Internet Explorer
Microsoft
AppV
User Experience Virtualization
Windows
OpenSSH
Windows PowerShell
키 관리 서비스
하드웨어 이벤트
구독


Store
StorPort
Storsvc
Sysmon
Operational
SystemSettingsThreshold
TaskScheduler
TCPIP
TerminalServices-ClientActiveXCore
TerminalServices-ClientUSBDevices
TerminalServices-LocalSessionManager
TerminalServices-PnPDevices
TerminalServices-Printers
TerminalServices-RemoteConnectionManager
TerminalServices-ServerUSBDevices
Time-Service
Time-Service-PTP-Provider
Troubleshooting-Recommended
TZSync
TZUtil
UAC
UAC-FileVirtualization
UI-Search
UniversalTelemetryClient
User Control Panel
User Device Registration
User Profile Service
User-Loader
UserPnp
VDRVROOT
VerifyHardwareSecurity
VHDMP
Volume
Vpn Plugin Platform
VPN-Client
Wcmsvc
WDAG-PolicyEvaluator-CSP
WDAG-PolicyEvaluator-GP
WebAuth
Operational 이벤트 수: 80 (!) 새 이벤트를 사용할 수 있음
수준 날짜 및 시간 원본 이벤트 ID 작업 범주
정보 2022-07-30 오후 3:48:44 Sysmon 5 Process terminated (rule: ProcessTerminate)
정보 2022-07-30 오후 3:48:44 Sysmon 1 Process Create (rule: ProcessCreate)
정보 2022-07-30 오후 3:48:15 Sysmon 5 Process terminated (rule: ProcessTerminate)
정보 2022-07-30 오후 3:48:14 Sysmon 1 Process Create (rule: ProcessCreate)
정보 2022-07-30 오후 3:48:14 Sysmon 5 Process terminated (rule: ProcessTerminate)
정보 2022-07-30 오후 3:48:14 Sysmon 1 Process Create (rule: ProcessCreate)
정보 2022-07-30 오후 3:47:49 Sysmon 5 Process terminated (rule: ProcessTerminate)
정보 2022-07-30 오후 3:47:49 Sysmon 1 Process Create (rule: ProcessCreate)
정보 2022-07-30 오후 3:47:28 Sysmon 5 Process terminated (rule: ProcessTerminate)
정보 2022-07-30 오후 3:47:27 Sysmon 1 Process Create (rule: ProcessCreate)
정보 2022-07-30 오후 3:46:53 Sysmon 5 Process terminated (rule: ProcessTerminate)
정보 2022-07-30 오후 3:46:27 Sysmon 5 Process terminated (rule: ProcessTerminate)
정보 2022-07-30 오후 3:46:26 Sysmon 5 Process terminated (rule: ProcessTerminate)
이벤트 5, Sysmon
일반 자세히
Process terminated:
RuleName: -
UtcTime: 2022-07-30 06:48:44.854
ProcessGuid: {a6df5543-d44c-62e4-9402-000000000300}
ProcessId: 6716
Image: C:₩Program Files (x86)₩Microsoft₩Edge₩Application₩msedge.exe
User: DESKTOP-7GILHFM₩sysmon
로그 이름(M): Microsoft-Windows-Sysmon/Operational
원본(S): Sysmon
로그된 날짜(D): 2022-07-30 오후 3:48:44
이벤트 ID(E): 5
작업 범주(Y): Process terminated (rule: ProcessTerminate)
수준(L): 정보
키워드(K):
사용자(U): SYSTEM
컴퓨터(R): DESKTOP-7GILHFM