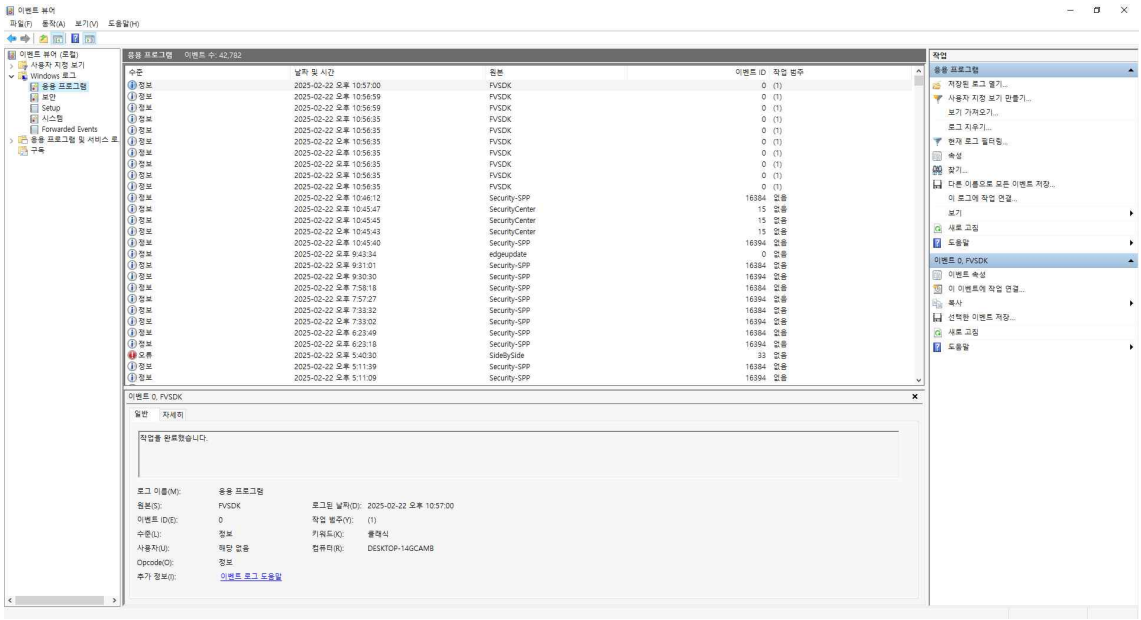
윈도우 이벤트 로그란?

윈도우 이벤트 로그는 윈도우 운영 체제에서 발생하는 다양한 이벤트를 기록하는 시스템.
이벤트 로그는 시스템, 보안, 애플리케이션 등 다양한 카테고리로 나뉘며, 각 이벤트는 로그에 기록되어 시스템 관리자가 시스템 상태를 모니터링하고 문제를 진단하는 도움을 제공.

Win + R 키를 눌러 실행 창을 열고 eventvwr.msc를 입력 후 실행



시스템 로그에서 Error 또는 Warning 레벨의 이벤트를 확인하여 시스템 문제를 진단할 수 있음.

Sysmon이란?

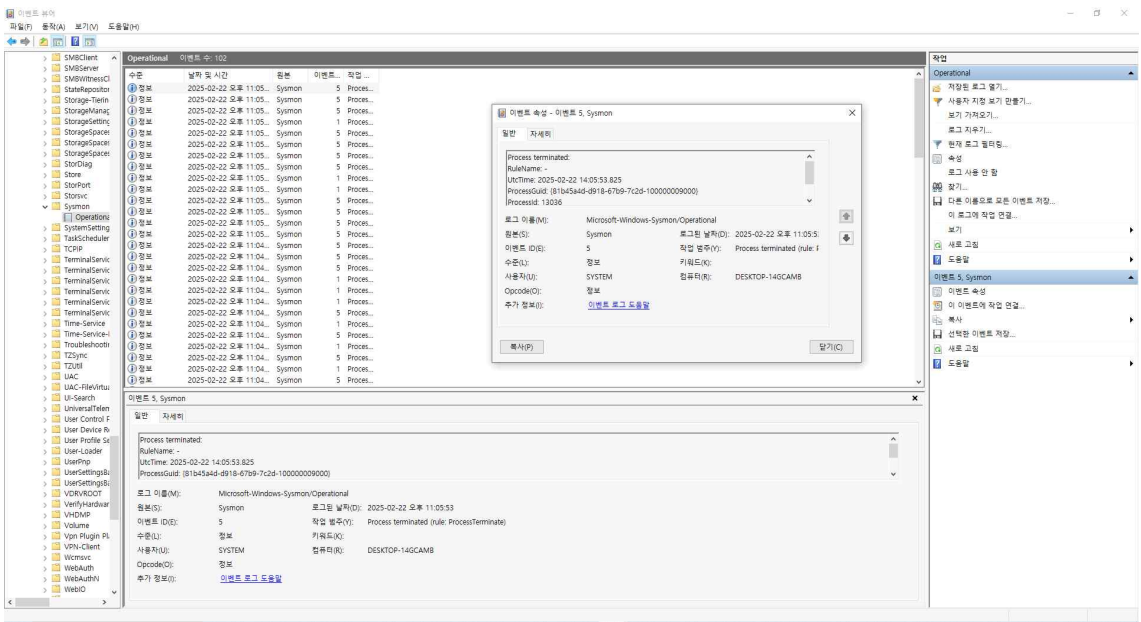
시스템 모니터(Sysmon)는 Windows 시스템 서비스 및 장치 드라이버로, 시스템에 설치되면 시스템 재부팅 후에도 상주하여 시스템 활동을 모니터링하고 Windows 이벤트 로그에 기록합니다. 프로세스 생성, 네트워크 연결, 파일 생성 시간 변경 사항에 대한 자세한 정보를 제공하는 드라이버.
(출처: https://learn.microsoft.com/ko-kr/sysinternals/downloads/sysmon)

Sysmon 기능 개요

Sysmon에는 다음 기능이 포함됩니다.

현재 프로세스와 상위 프로세스 모두에 대한 전체 명령줄을 사용하여 프로세스 생성을 기록합니다.
SHA1(기본값), MD5, SHA256 또는 IMPHASH를 사용하여 프로세스 이미지 파일의 해시를 기록합니다.
여러 해시를 동시에 사용할 수 있습니다.
Windows가 프로세스 ID를 재사용하는 경우에도 이벤트의 상관 관계를 허용하기 위해 프로세

스 생성 이벤트에 프로세스 GUID를 포함합니다.
동일한 로그온 세션에서 이벤트의 상관 관계를 허용하기 위해 각 이벤트에 세션 GUID를 포함합니다.
서명 및 해시와 함께 드라이버 또는 DLL 로드를 기록합니다.
디스크 및 볼륨의 원시 읽기 액세스를 위해 로그가 열립니다.
선택적으로 각 연결의 원본 프로세스, IP 주소, 포트 번호, 호스트 이름 및 포트 이름을 포함하여 네트워크 연결을 기록합니다.
파일이 실제로 생성된 시점을 이해하기 위해 파일 생성 시간의 변화를 검색합니다. 파일 생성 타임스탬프 수정은 맬웨어가 추적을 숨기기 위해 일반적으로 사용하는 기술입니다.
레지스트리에서 변경된 경우 구성을 자동으로 다시 로드합니다.
특정 이벤트를 동적으로 포함하거나 제외하는 규칙 필터링.
부팅 프로세스 초기부터 이벤트를 생성하여 정교한 커널 모드 맬웨어에 의한 활동도 캡처합니다.
(출처:https://learn.microsoft.com/ko-kr/sysinternals/downloads/sysmon)



이벤트 ID: 5 (Process terminated)

프로세스 이름: SearchFilterHost.exe

프로세스 경로: C:\Windows\System32\SearchFilterHost.exe

프로세스 ID (PID): 13036

사용자: NT AUTHORITY\SYSTEM (시스템 권한으로 실행된 프로세스)

종료 시간: 2025-02-22 14:05:53.825 (UTC)