**윈도우 로그 관리 및 분석 방법**

필요성

1. 해킹의 흔적을 찾기 위해서
2. 공격기법을 알기 위해서 -> 취약점을 제거할 수 있다.
3. 공격 근원지를 찾아서 법적 소송 증거로 사용할 수 있다.

로그 : 시스템의 모든 기록

로그분석: 로그 데이터를 분석하여 필요로 하는 유용한 정보를 만들어내는 행위

eventvwr