제목 : 보안 시그니처 탐지를 위한 필터링 우선순위 알고리즘 구현

1.연구 배경:

보안 이벤트 처리에 있어서 능동적이고 효율적인 대응이 필요한데, 이를 위해서는 보안 이벤트의 위험성을 정량화하고 우선순위를 부여하는 방법이 필요

CVE나 CVSS와 같은 기준을 활용하여 이벤트에 대한 점수를 매기고, 이를 기반으로 우선순위 알고리즘을 구현하여 이벤트 스케줄링을 수행하는 것이 중요

그래서 우선순위 알고리즘을 구현함.

2.연구 내용:

-보안 이벤트 위험성을 평가하기 위한 표준 기준인 CVE나 CVSS를 활용하여 보안 이벤트의 점수를 매김

-CVE나 CVSS를 바탕으로 이벤트 스케줄링을 수행하는 우선순위 알고리즘을 개발

-우리나라의 보안 이벤트 상황에 맞게 우선순위 알고리즘을 조정

-> 국내 기관 및 기업의 정보보호 신뢰성을 확보하고 산업 발전에 기여

3.향후 방향:

본 연구를 바탕으로 보안 이벤트 데이터베이스를 구축

이 DB를 활용하여 실시간으로 이벤트 스케줄링을 수행하는 시스템을 개발할 예정

또한, 보안 이벤트 스케줄링 우선순위 알고리즘을 꾸준히 개선하여 보다 효율적인 보안 이벤트 처리를 실현해야 함.