

Windows Sentinel

실시간 네트워크 보안 프로그램

2416110232 김기원 · 2416110242 정재윤 · 2416110252 안지훈



팀원 소개

김기원

프로젝트 리드 및 기획

시스템 아키텍처 설계 및
개발 프로세스 구축
통합 및 테스트

정재윤

코어 시스템 개발

패킷 분석 시스템 구축,
실시간 모니터링 기능 개발,
자동 차단 메커니즘 구현

안지훈

UI/UX 디자인 및 프론트엔드

사용자 인터페이스 설계,
대시보드 시각화,
직관적인 사용자 경험 구축

프로젝트 개요

프로젝트 목적

- 실시간 네트워크 위협 탐지 및 차단
공격을 즉시 식별하고 대응
- 사용자 친화적인 보안 대시보드 제공
복잡한 데이터를 직관적으로 시각화
- 자동화된 방어 시스템 구축
수동 개입 없이 자동으로 위협 차단

핵심 목표

- DDoS 공격 실시간 탐지
비정상 트래픽 패턴 즉각 감지
- 악성 IP 자동 차단
위협 소스를 자동으로 차단
- 위협 인텔리전스 통합
글로벌 위협 데이터베이스 연동 (AbuseIPDB)



현재 보안 위협 현황

35%

DDoS 공격 증가율

2024년 전년 대비 급격한 상승세

1,200

일일 랜섬웨어

매일 발생하는 평균 공격 건수

4.5조원

연간 데이터 유출 손실

국내 기업들의 총 피해액

! 수동 탐지의 한계

사람이 직접 모니터링하는 방식은 공격 속도를 따라잡을 수 없으며, 24시간 감시가 불가능합니다.

! 늦은 대응 속도

위협을 발견한 후 차단까지 평균 수 시간이 소요되어 이미 큰 피해가 발생한 후입니다.

! 복잡한 보안 도구

기존 보안 솔루션은 전문가만 사용할 수 있어 일반 관리자의 접근성이 낮습니다.



Windows Sentinel 솔루션



실시간 자동 탐지

DDoS 공격, 의심스러운 연결을 실시간으로 감지하고 자동으로 차단하여 사용자를 보호합니다.



즉각적인 차단 시스템

탐지된 위협을 자동으로 차단하여 피해를 최소화하고, 방화벽 규칙을 동적으로 업데이트합니다.



직관적인 UI/UX

전문 지식 없이도 누구나 쉽게 사용할 수 있는 깔끔한 인터페이스와 명확한 시각적 피드백을 제공합니다.



통합 보안 대시보드

모든 보안 정보를 한눈에 파악할 수 있는 종합 대시보드로 실시간 차트와 알림을 제공합니다.

핵심 모듈

DDoS 방어 시스템

- 패킷 분석 및 임계값 감지 - 비정상 활동 탐지
- 자동 IP 차단 - 공격 소스를 즉시 차단하여 서비스 보호
- 실시간 트래픽 모니터링 - 네트워크 상태를 지속적으로 감시

위협 인텔리전스

- 악성 IP 데이터베이스 - AbuseIPDB 연동으로 10,000개 이상의 악성 IP 정보 활용
- 실시간 위협 정보 업데이트 - 전 세계 보안 커뮤니티의 최신 위협 정보 동기화
- 지능형 분석 엔진 - 패턴 매칭과 임계값 기반 실시간 위협 탐지

기술 스택

C# (.NET 6.0)

Windows 보안 프로그램 개발에 최적화된 플랫폼으로, 풍부한 보안 라이브러리와 안정적인 성능을 제공합니다.

WPF

복잡한 UI를 쉽게 구현할 수 있으며, 실시간 차트 업데이트와 전문적인 디자인 구현이 가능합니다.

비동기 프로그래밍

공격 탐지 중에도 UI가 반응하며, 여러 공격을 동시에 처리하여 사용자 경험을 크게 향상시킵니다.

이벤트 기반 구조

Toast 알림이 자동으로 발생하고, 모듈 간 느슨한 결합으로 유지보수가 편리한 확장 가능한 아키텍처입니다.



Windows Sentinel

실시간 시연

지금부터 Windows Sentinel의
실제 작동 모습을 시연하겠습니다.

□ **시연 내용:** 통합 대시보드 기능, 실시간 DDoS 공격 탐지,
악성 IP 자동 차단

감사합니다!

프로젝트 저장소

github.com/gkwp1216/WindowsSentinel

소스 코드와 상세 문서를 확인하실 수 있습니다

문의하기

rabbia1216@gmail.com

질문이나 피드백을 환영합니다

Windows Sentinel과 함께
더 안전한 네트워크 환경을 만들어주세요.