SEMO

딥러닝 기반 보안관제 플랫폼[Security Monitoring Platform]

7조
Do Mo!

연구 배경

정보화 시대를 맞아 **네트워크 트래픽의 양이 방대**해지면서, 대량의 이벤트 로그데이터를 수동으로 정오탐을 분류하고 있는 **보안관제사들이 어려움**을 겪고 있습니다. Do Mo는 이러한 문제를 해결하기 위해 오탐을 **자동으로 분류**하고 **정오탐 분석을 용이**하게 해 줄 SEMO를 제작하였습니다.

현재 기술 시장의 문제점

정오탐 판별 능률 문제

IPS 장비에서 나오는 이벤트 로그 데이터의 정오탐 비율을 봤을 때, 약 3:7로 오탐의 비율이 매우 높습니다. 따라서 수동 분류 방식은 오탐 분류에 할애되는 시간이 높아 능률이 낮습니다.

AI 보안관제 서비스 제공의 어려움

AI 보안관제 서비스를 제공하고 싶은 기업도 전문 인력이 없다면 다른 기업의 도움을 받아야 합니다.

기대효과

딥러닝을 통한 이벤트 분류 자동화

매일 새롭게 생성되는 방대한 보안 이벤트 분류를 자동화 함으로써 보안 업무의 능률이 증가합니다.

자체적인 시스템 구축을 위해 Best Practice 제공

자체적인 보안관제 시스템이 구축되어 있지 않은 회사들은 자체적인 시스템을 구축하여 활용할 수 있습니다.

프로젝트 구현

SEMO는 이벤트 로그 데이터를 딥러닝을 통해 **자동으로 정오탐 분류**하고 데이터 분석을 위해 WEB을 통해 데이터 **분석 결과를 시각화** 합니다.

Model

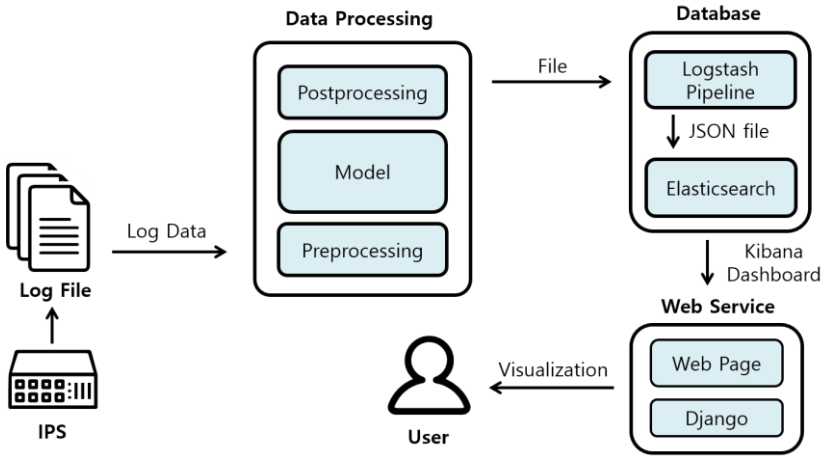
이벤트 로그 데이터의 정오탐 분류를 위한 주요 필드 분석
Pre-Now 모델을 구현하여 정오탐 판별

ELK

시스템 환경에 맞는 ELK 설치 및 구축
시각화를 위한 Kibana Dashboard 구성
Best Practice 배포를 위한 ELK 구축 가이드라인 작성

Web

Django 기반 웹서버 구현
Embed code를 이용하여 Kibana Dashboard 임베딩

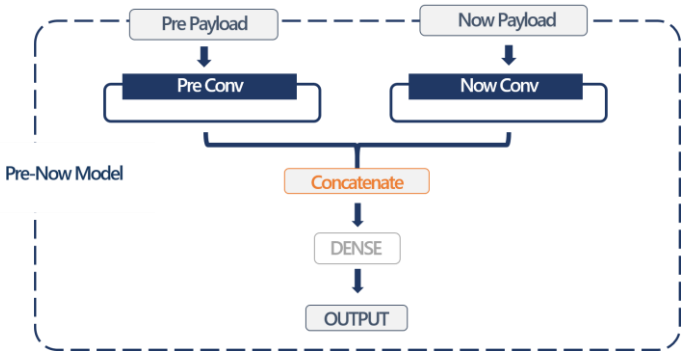


주요 기술

더 좋은 보안관제 플랫폼을 제공하기 위해 적용한 SEMO만의 기술을 소개합니다.

Pre-Now Model

주기적으로 생성되는 로그 데이터에서 직전 페이로드 값이 현재 페이로드 값과 연관성이 있다고 생각하여 직전 데이터 값이 현재 데이터의 영향을 주도록 한 SEMO만의 모델 구현 방식입니다.



Kibana Dashboard

Kibana Dashboard는 누구나 데이터를 쉽고 빠르게 시각화 할 수 있는 툴입니다. Best Practice를 제공하는 SEMO는 사용자의 효율적인 시각화를 위해 Kibana Dashboard를 활용하였습니다.

Do Mo!

지도교수
윤명근 교수님

전하훈
#Leader #ML
plmokn1007@kookmin.ac.kr

김성은
#Analysis #ML
kimsung97@kookmin.ac.kr

최운호
#Web #Webserver
yms04089@kookmin.ac.kr

최현인
#ELK #Document
gusdlsdlek@kookmin.ac.kr

허윤서
#Web #Dashboard
sally159357@kookmin.ac.kr