45 사용자 행동 기반 동적 네트워크 접근 제어 시스템 연구

소속 정보컴퓨터공학부 분과 D 팀명 CtrlAltDefend 참여학생 이광훈, 조유진, 신해진 지도교수 최윤호

과제 개요

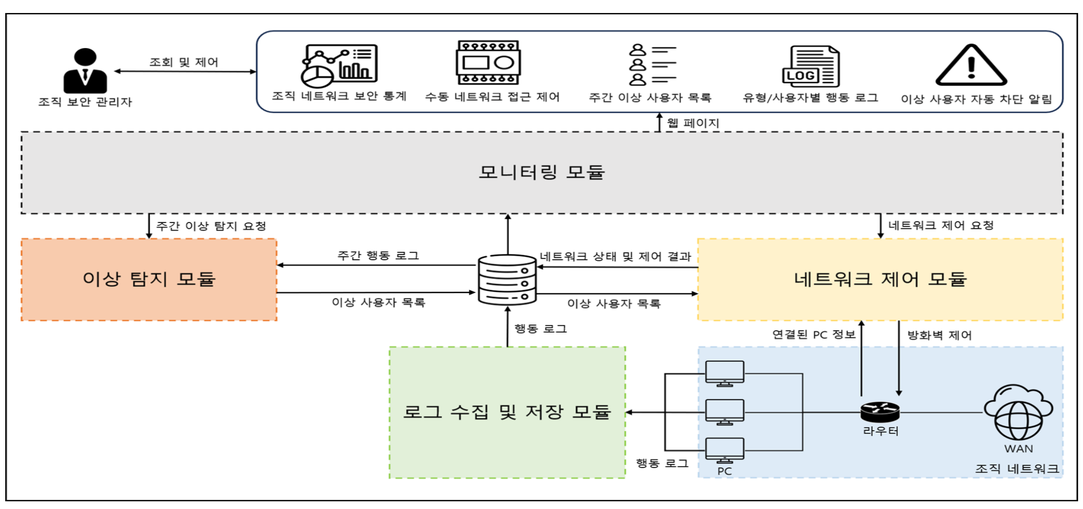
과제 배경

- 원격 근무 및 클라우드 환경 확대로 인해, 기존 보안 방식으로는 탐지가 어려운 **내부자 위협(Insider Threat)** 증가
- "절대 신뢰하지 않고 항상 검증"하는 **제로 트러스트(Zero Trust)** 보안 모델의 중요성 부각

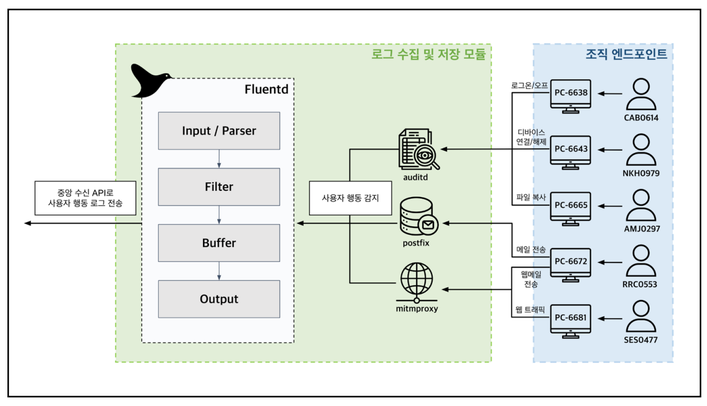
과제 목표

- 특정 조직의 네트워크에서 사용자 활동 로그를 실시간으로 수집하고, **머신러닝 기반으로 분석**하여 이상 행위 사용자를 자동 탐지
- 탐지된 사용자가 이용 중인 PC를 **네트워크에서 원격으로 격리**하는 보안 시스템 구현
- 이를 위해 전체 시스템은 **로그 수집 및 저장**, **이상 탐지**, **네트워크 제어**, **모니터링**의 4가지 핵심 모듈로 구성하여 개발

시스템 개요

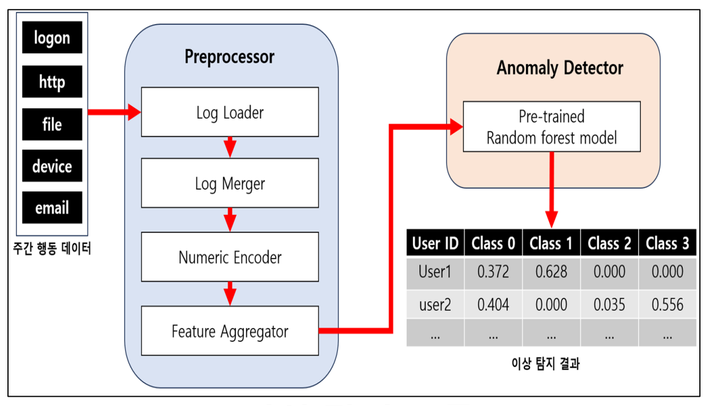


- 가상 조직 네트워크 환경 내 PC에 설치된 로그 수집 에이전트가 사용자 PC의 **활동 로그를 실시간으로 수집**하여 데이터베이스에 저장
- 백엔드 서버는 저장된 로그 데이터를 **XGBoost** 모델로 분석하여, **학습된 정상 행위 패턴과 다른 이상 사용자를 식별**
- 이상 행위가 탐지되면 WebSocket을 통해 관리자 화면에 실시간 알림이 전송되며, 관리자는 이를 통해 탐지된 사용자의 상세 로그를 직접 확인
- 백엔드 서버는 탐지 결과를 바탕으로 OpenWRT 라우터에 **원격 제어** 명령을 보내, **위협으로 판단된 PC를 네트워크로부터 즉시 격리**



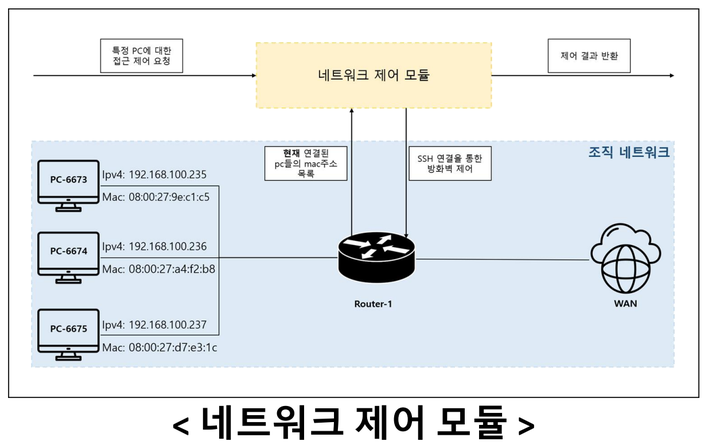
< 로그 수집 및 저장 모듈 >

- 엔드포인트 PC 에이전트가 이벤트 로그 실시간 수집
- Fluentd 파이프라인으로 원본 로그 전처리 및 필터링
- 표준 스키마로 정규화 후 중앙 수신 API로 전송



< 이상 탐지 모듈>

- 데이터베이스에서 주 단위 사용자 활동 데이터 조회
- 전처리기가 로그 병합, 숫자 변환, 피처 추가 수행
- 사전 학습된 XGBoost 모델이 전처리된 데이터로 사용자의 이상 클래스별 확률 분포 반환
- 이상 확률이 임계값을 넘는 사용자는 탐지 목록에 추가 후 데이터베이스에 저장



< 네트워크 제어 모듈 >

- 탐지된 이상 사용자 PC의 네트워크 연결 허용 및 차단 역할 수행
- 라우터에서 주기적으로 현재 연결된 PC의 목록을 스캔하여 메인 프레임에 보고
- 특정 PC에 대한 접근 제어 요청 발생 시 라우터의 SSH 서버에 접속하여 방화벽 규칙 자동 적용

과제 결과

이상 탐지 성능

	pred_0	pred_1	pred_2	pred_3
true_0	13370	0	1	0
true_1	0	10	0	0
true_2	0	0	51	0
true_3	0	0	0	2

class	precision	recall	F1-score
0	1.0000	0.9999	1.0000
1	1.0000	1.0000	1.0000
2	0.9808	1.0000	0.9903
3	1.0000	1.0000	1.0000

기대효과

- **802.1X 한계 보완**: 접속 시점 인증을 통과한 내부자의 악성 행위까지 행동 패턴 분석 기반으로 탐지 및 격리 가능
- **조기 위협 차단**: 이상 사용자 로그온 감지 시 정책에 따라 해당 사용자가 사용 중인 PC를 자동 격리하여 피해 확산을 선제적으로 차단 가능
- **실시간 가시성 확보**: 대시보드·WebSocket 알림·경고 이메일로 보안 이벤트를 즉시 파악하고 신속한 후속 조치 가능