## 김채원

- 프로젝트 팀장
- 악성코드 및 Elasticseach 쿼리문 제작
- 모의해킹 및 침해사고 분석보고서 작성
- 팀원 통솔

## 곽화종

- 프로젝트 팀원
- 악성코드 제작 및 프로젝트 진행

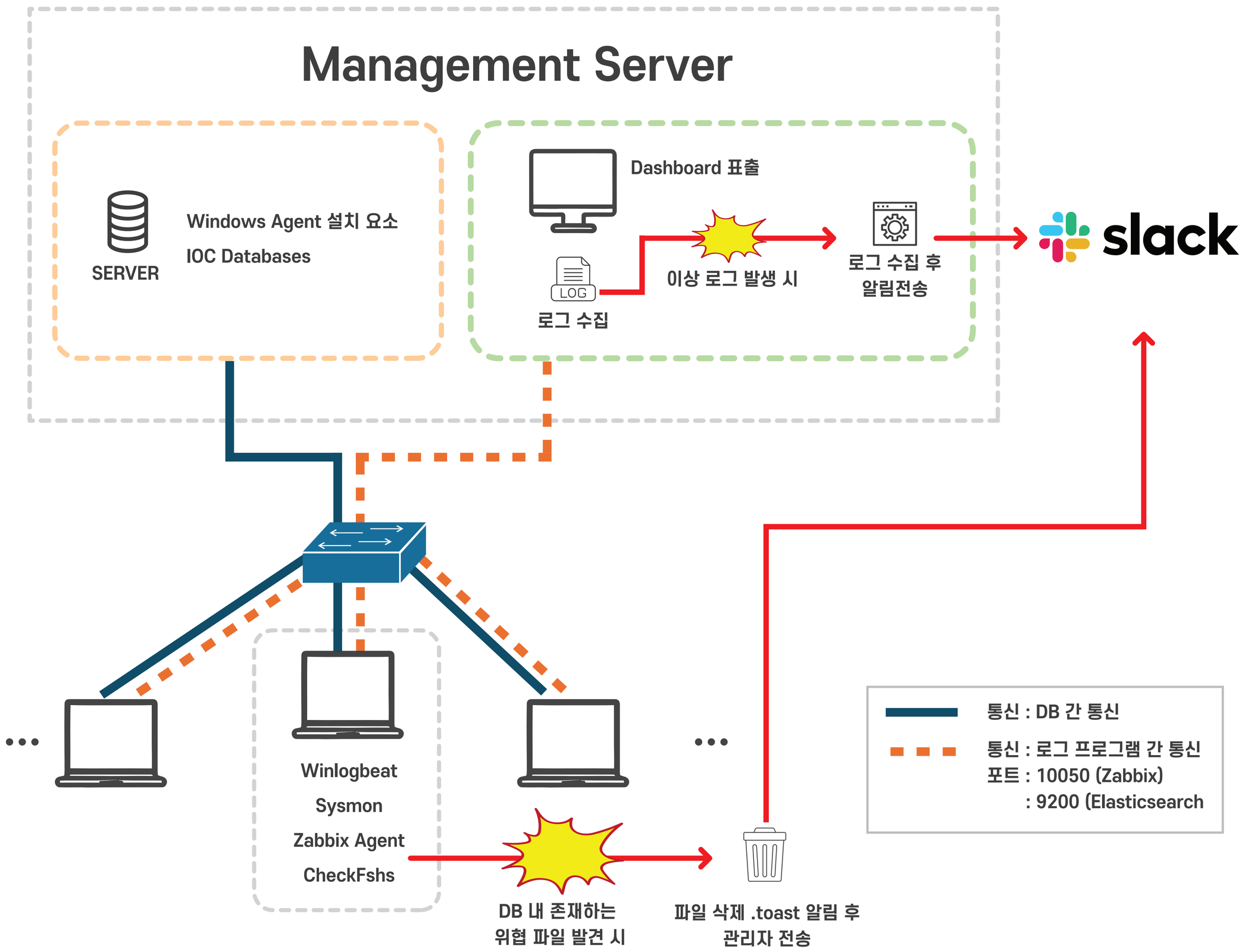
## 손경현

- 프로젝트 팀원
- Linux 관리 서버 제작
- Windows Agent Installer 제작
- IOC 기반  악성 파일제거 프로그램 제작

## 박세연

- 프로젝트 팀원
- 프로젝트 진행

## 01 구성도




## 02 주요기능

- 엔드포인트 주요 이벤트 로그 자동수집
- IOC 기반 및 관리자 정의를 통한 악성 프로그램 방지
- 실시간 엔드포인트 모니터링 가능
- 위협 발생 시 Slack 등을 통한 알림 서비스 제공

## 03 기대효과

| | |
|---|---|
| 기대효과 1 | 실시간 위협 탐지 및 모니터링 강화 |
| 기대효과 2 | 중앙 집중식 로그 분석으로 보안 인사이트 향상 |
| 기대효과 3 | 커스텀 IOC 기반 탐지로 특정 위협에 대한 대응력 증대 |
| 기대효과 4 | 자동화된 설치 및 구성으로 배포 효율성 개선 |
| 기대효과 5 | 다양한 데이터 소스 통합으로 포괄적인 보안 분석 가능 |
| 기대효과 6 | 확장 가능한 구조로 향후 새로운 보안 도구 추가 용이 |

## 04 시현 영상

시현 영상