네트워크 공격 분석 및 트래픽 시각화 서비스 (aDDoS)

지도 교수 : 이병천 교수님

팀명 : 늙었조

CONTENTS LIST

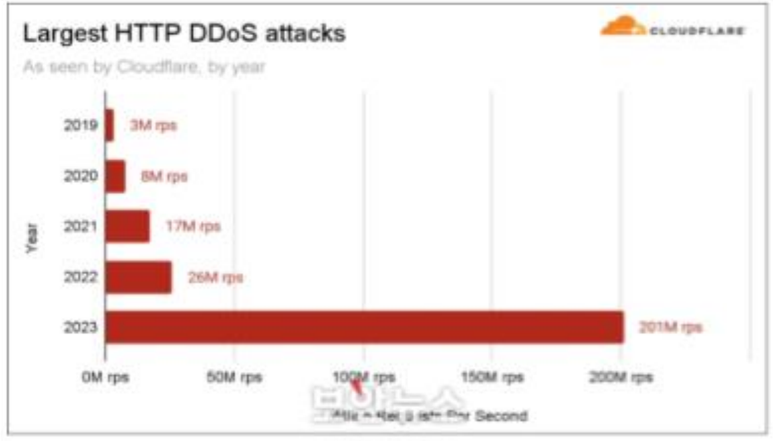
CHAPTER 2 프로젝트 배경 및 목적

2023년 4분기 네트워크 계층 DDoS 공격, 전년 동기 대비 117% 증가

입력 : 2024-01-20 09:14

네트워크 계층 DDoS 공격, 전년 동기 대비 117% 증가...연말연시 전반적으로 증가추세
대만 겨냥한 DDoS 공격 트래픽, 전년 대비 3,370% 증가
팔레스타인 웹사이트 겨냥 DDoS 공격 트래픽 비율, 전 분기 대비 1,126% 증가

[보안뉴스 김경애 기자] 지난해 4분기 전 세계적으로 디도스(DDoS) 공격이 급증한 것으로 조사됐다. 연말연시 전후로는 소매, 배송 등 웹사이트를 노린 공격이 크게 늘었고, 국가간 전쟁 및 갈등의 이유로 DDoS 공격이 증가했다.



클라우드플레어(Cloudflare)가 발표한 '2023년 4분기 DDoS 위협 보고서'에 따르면 "4분기에는 네트워크 계층 DDoS 공격이 전년 동기 대비 117% 증가했다"며 "특히 블랙 프라이데이와 연말연시를 전후해 소매, 배송, 홍보 웹사이트를 겨냥한 DDoS 활동이 전반적으로 증가했다"고 밝혔다.

디도스 공격을 받을 경우 발생하는 피해액은 적지 않다. 지난해 12월 KISA가 발표한 '사이버 침해사고의 경제·사회적 비용 추정 연구'에 따르면 사이버 공격 유형별 평균 피해액은 ▲랜섬웨어 13억8000만원 ▲디도스 12억9000만원 ▲코드서명 유출 10억6000만원 ▲개인정보유출 4억9000만원 ▲악성코드 유포가 3억원이었다.

CHAPTER 2 프로젝트 배경 및 목적

소프트웨어 기반 시스템 구축

네트워크 장비 없이
소프트웨어로 구축한
모니터링 시스템

트래픽 시각화

데이터 가시화를 통한
편리한 모니터링

네트워크 공격 분석

네트워크 트래픽 분석
시각화 데이터 확인

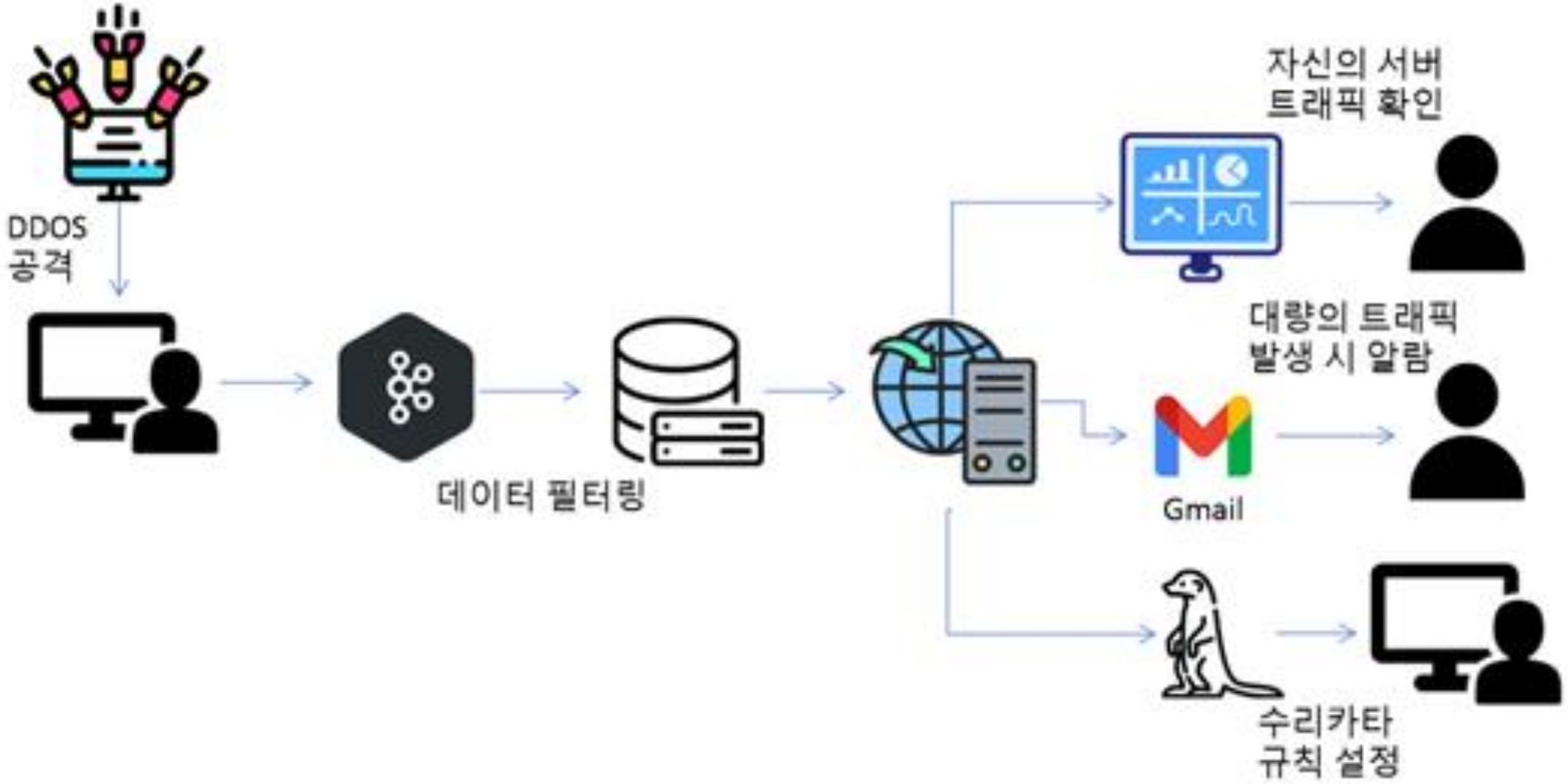
CHAPTER 3 개발 환경

프레임 워크 및 도구

elastic

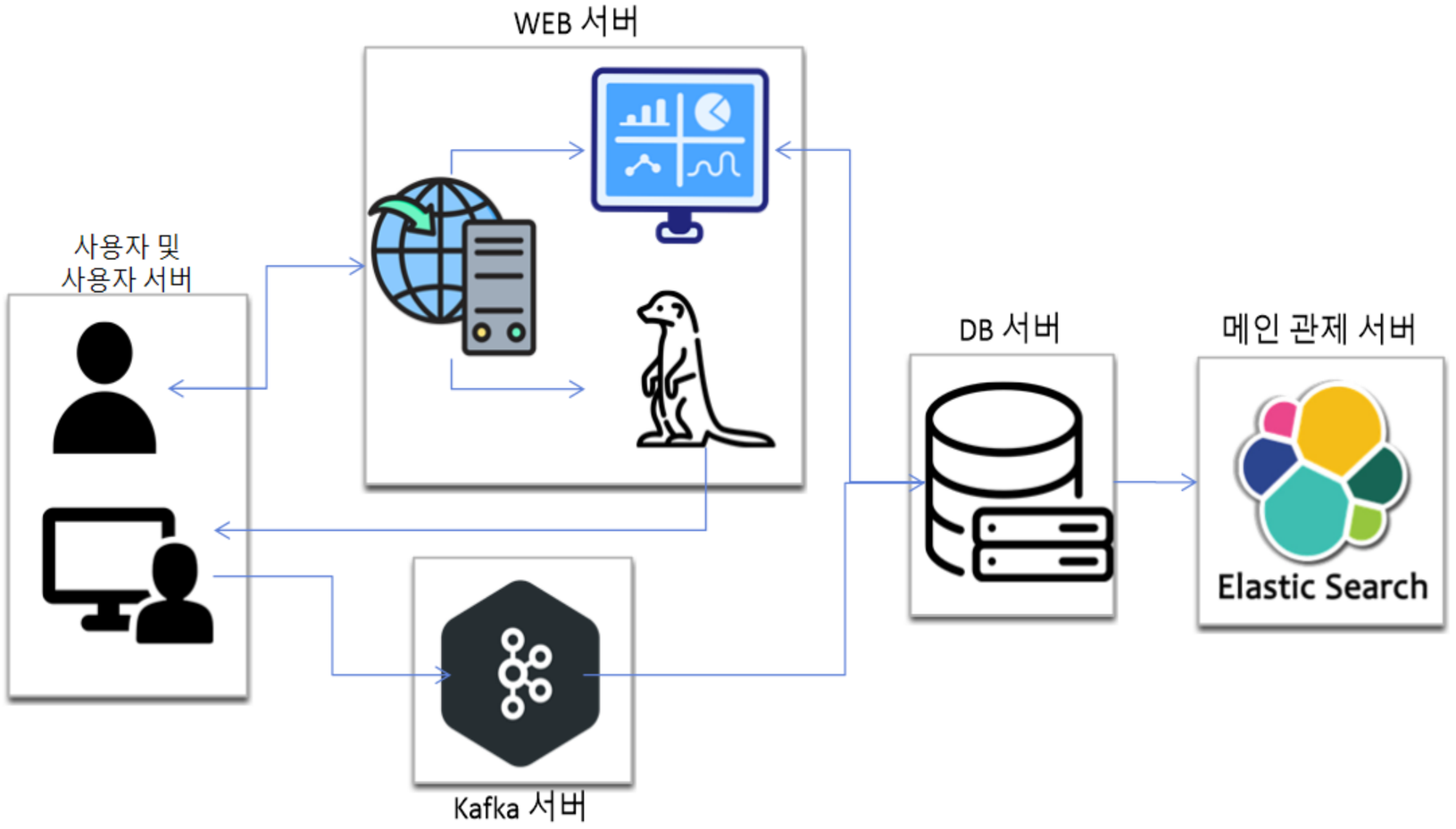
CHAPTER 3 개발 환경

서비스 구상도

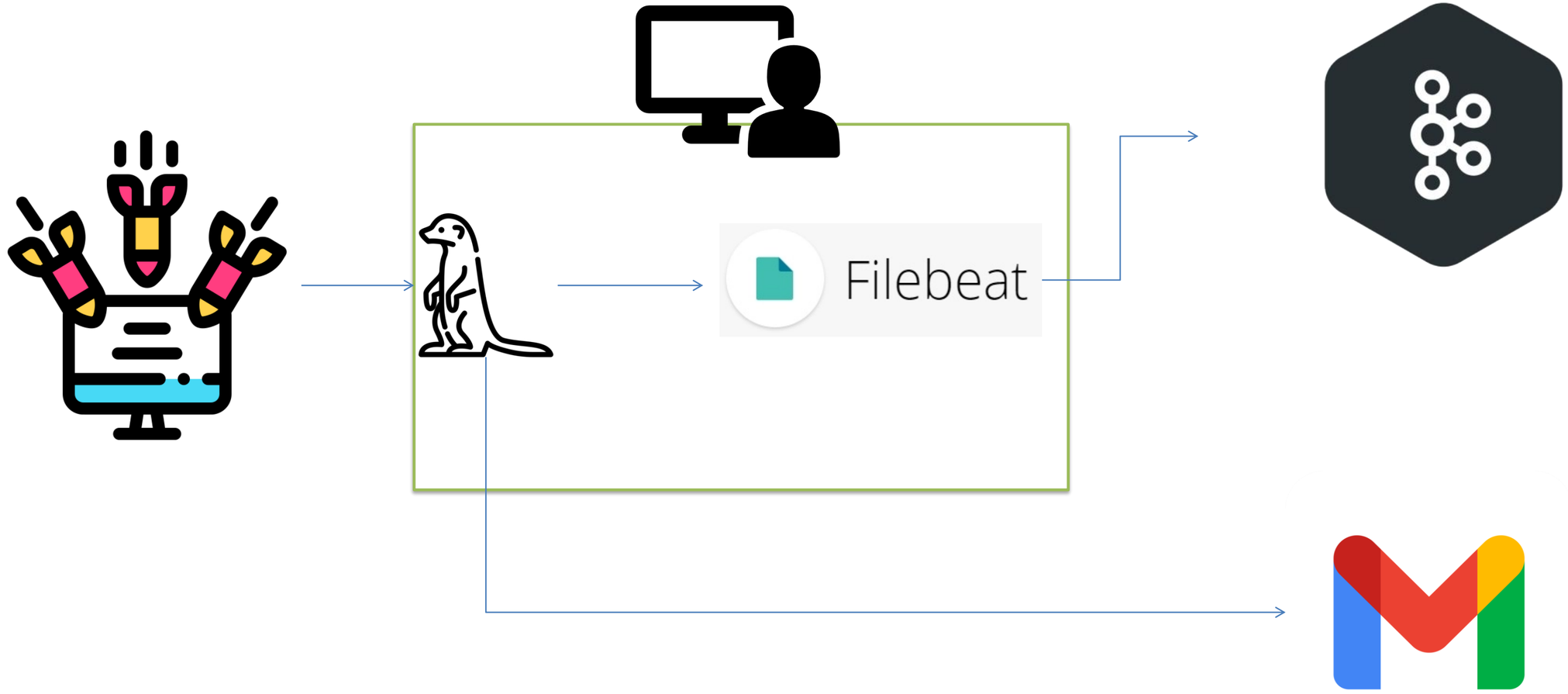


CHAPTER 3 개발 환경

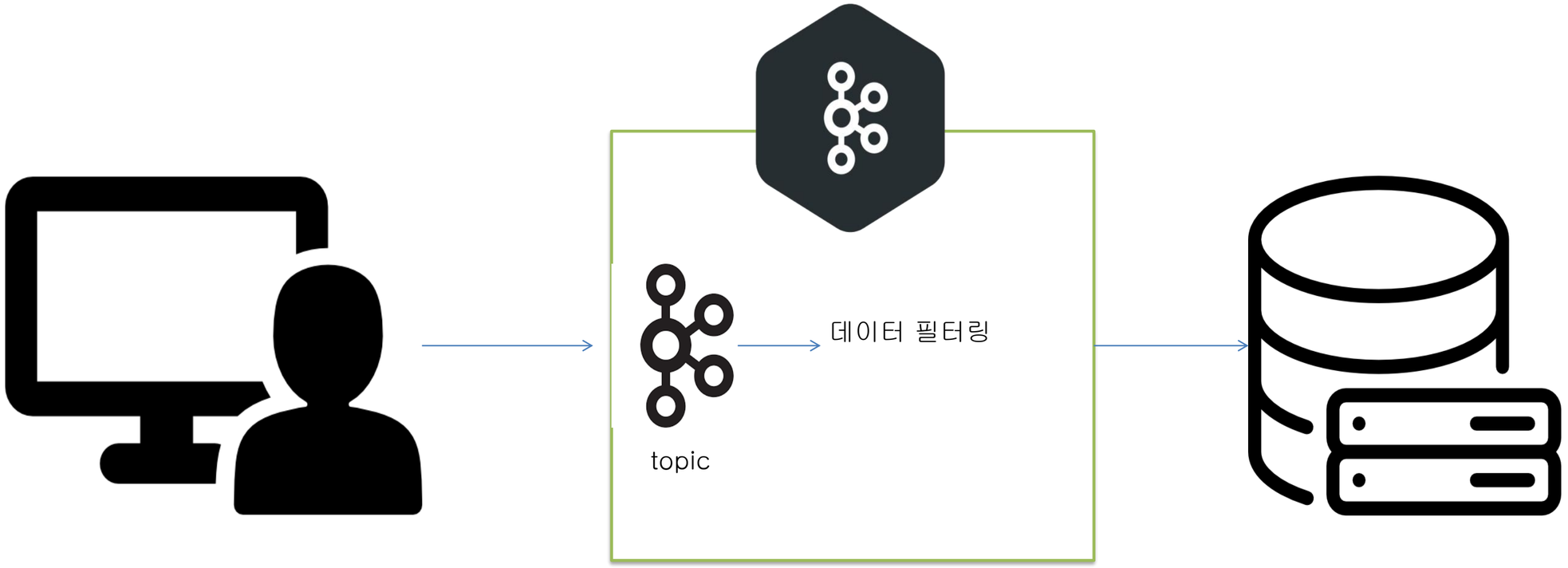
아키텍처 구상도



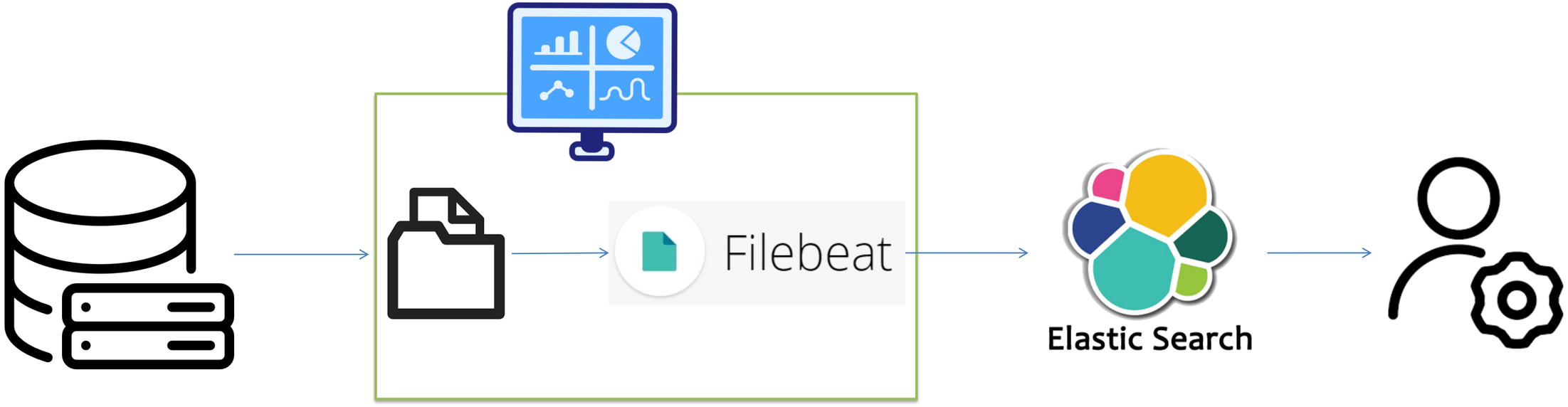
피해자 서버



카프카 서버

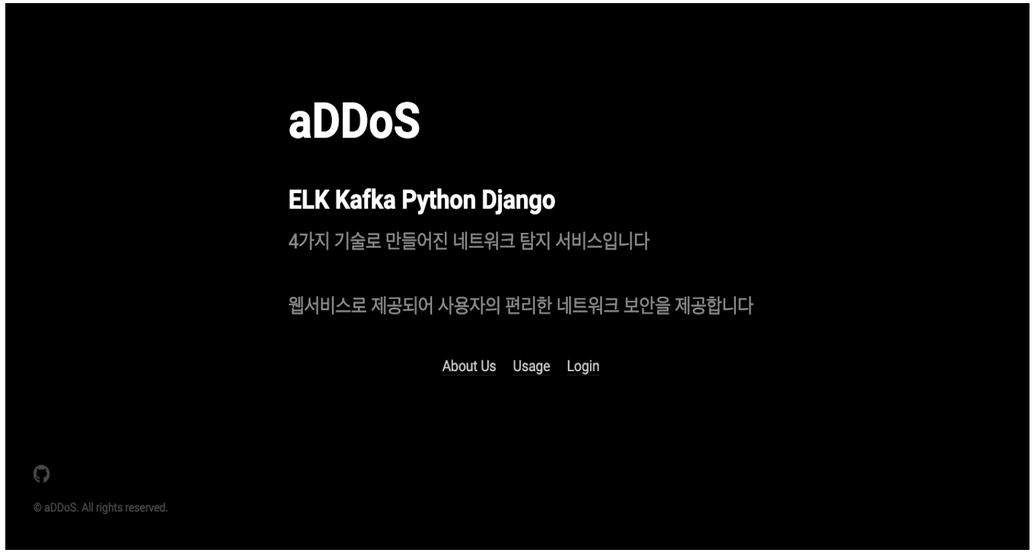


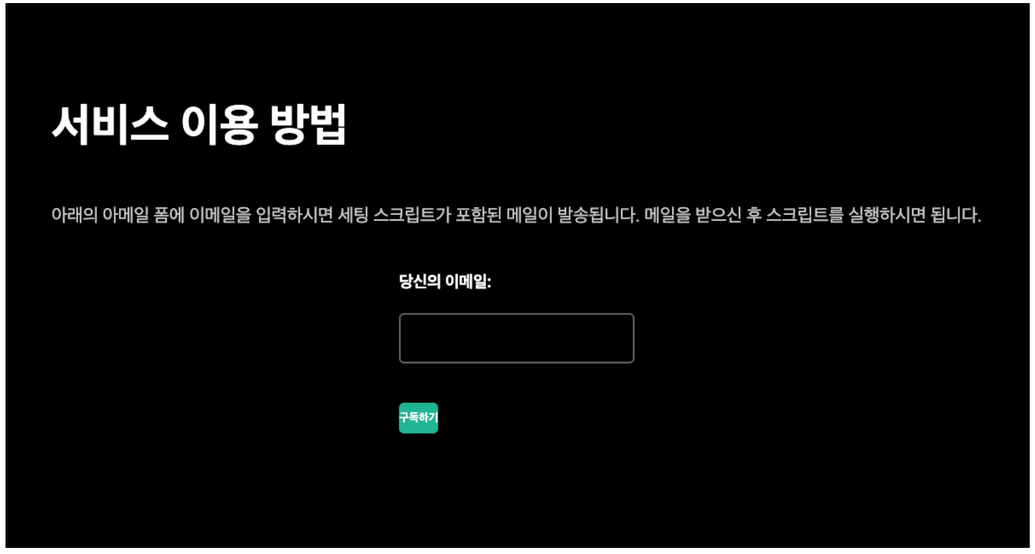
메인관제 서버



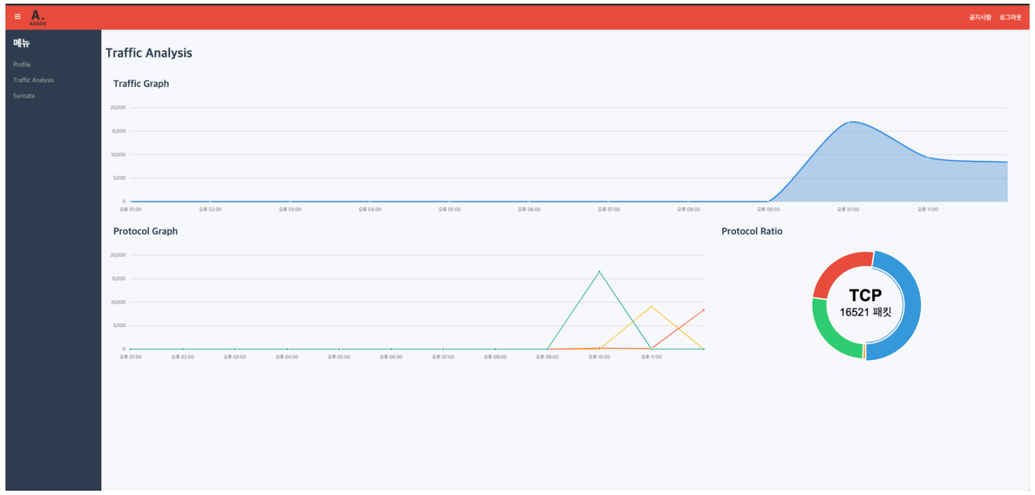
CHAPTER 4 웹사이트 구성

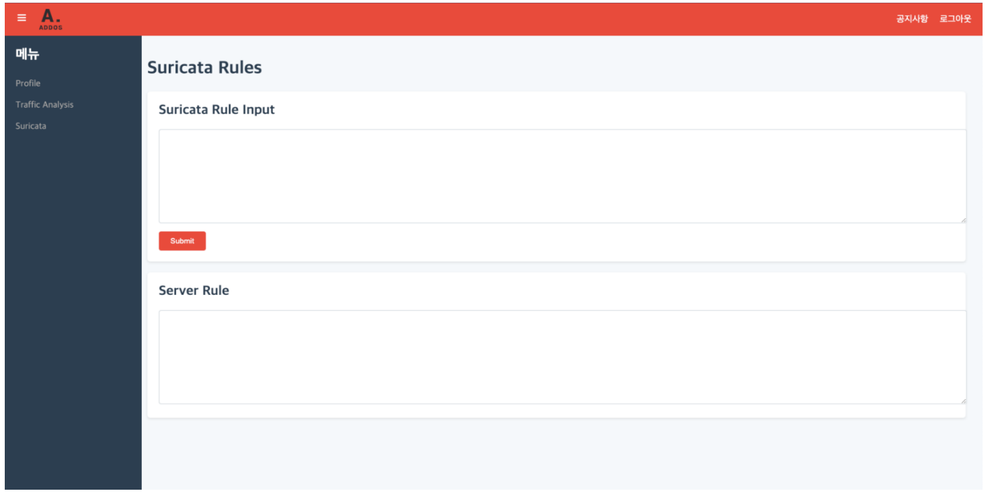
CHAPTER 4 웹사이트 구성



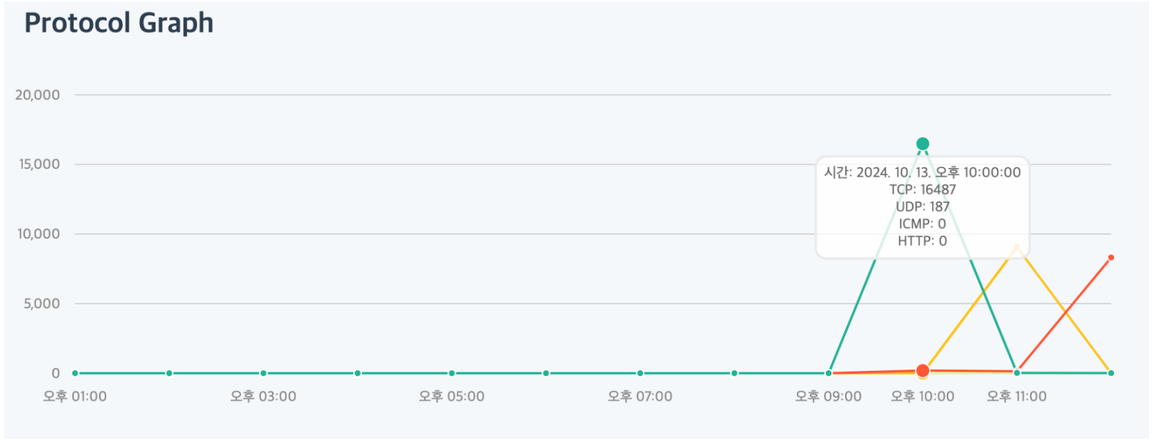


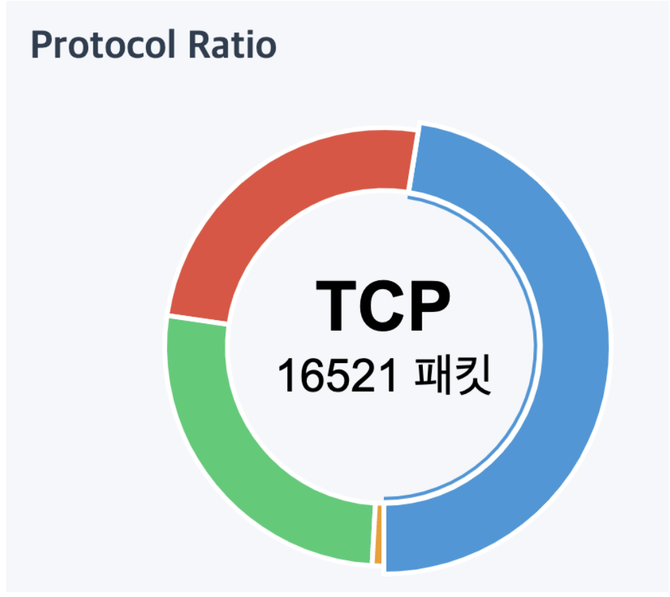
CHAPTER 4 웹사이트 구성





CHAPTER 4 웹사이트 구성





시연 영상

https://youtu.be/5Q0lImQUHgo

CHAPTER 5 결론/기대효과

Suricata Rule

Suricata Rule 변경
네트워크 공격에 대한
유연한 대처 가능

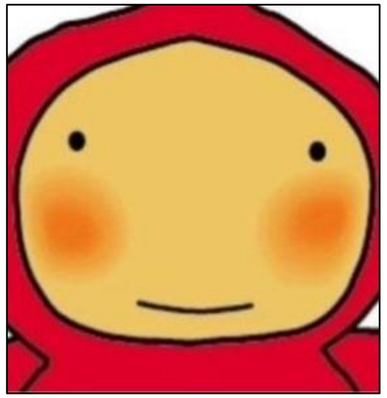
Alert System

사용자 경고 시스템
보안 관리 효율성 증대

Traffic Analysis

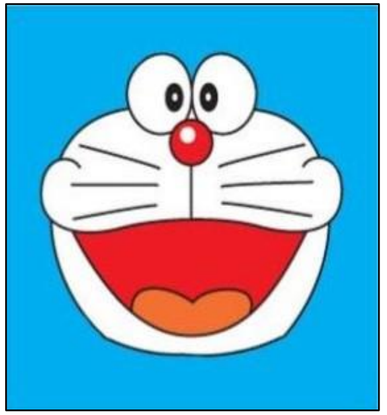
트래픽 시각화를 통한
요소 별 확인 가능
중요한 정보 시각화

CHAPTER 1 팀원 소개



이두리
팀장

박주형
팀원



송경선
팀원

김동철
팀원

이라규
팀원

이건우
팀원

네트워크 공격 분석 및 트래픽 시각화
(aDDoS)

감사합니다