

네트워크 공격 분석 및 트래픽 시각화 서비스 (aDDoS)

지도 교수 : 이병천 교수님

팀명 : 늑엇조

CONTENTS LIST

1. 프로젝트 배경 및 목적



2. 개발 환경



3. 웹사이트 구성



4. 결론 및 기대효과



5. 팀원소개



CHAPTER 2 프로젝트 배경 및 목적

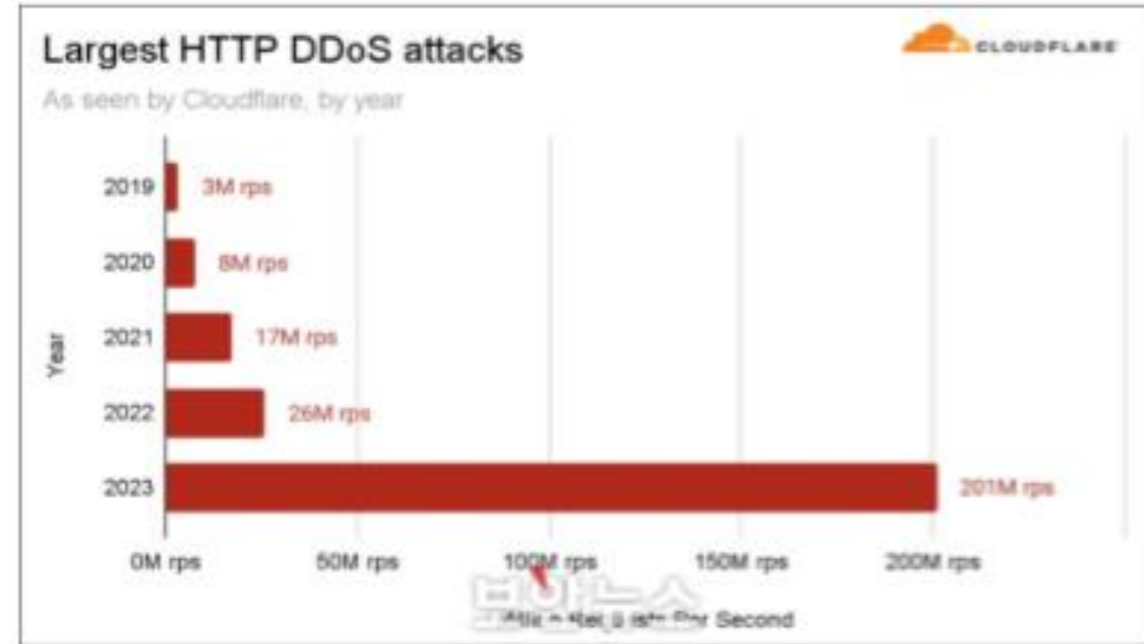
2023년 4분기 네트워크 계층 DDoS 공격, 전년 동기 대비 117% 증가

SECON 2024 통합 보안 솔루션의 새로운 시대가 온다. **suprema #H001** [더 알아보기 >](#)

2024. 03. 20(수) - 22(금) KINTEX 제1전시관 3 - 5동

네트워크 계층 DDoS 공격, 전년 동기 대비 117% 증가...연말연시 전반적으로 증가 추세
 대안 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.

Weekly Security PREMIUM REPORT
 매일, 매주 제공하는 보안뉴스 프리미엄 리포트
 결산리 서비스 중!!
[자세히보기](#)

- 제23회 세계 보안 엑스포 **SECON 2024** 2024년 3월 28(수)-29(목) 경기도 KINTEX 제1전시관
- 제12회 전자정부 정보보호 솔루션 페어 **eGISEC 2024** 2024년 3월 28(수)-29(목) 경기도 KINTEX 제1전시관
- 제13회 개인정보보호페어 & CPO워크숍 **PISFAIR 2024** 2024년 8월 시흥(수)-9(목) 서울 코엑스 그랜드홀
- 제18회 국제 시큐리티 콘퍼런스 **ISEC 2024** 2024년 10월 16(수)-17(목) 서울 코엑스

- 가장 많이 본 기사 [주간]
- [테크칼럼] UWB 기술로 여는 출입 보안 산업
 - [한 주간의 보안이슈 돋보기] 전 세계 개인정보
 - VMware, EAP 플러그인 취약점 발견... 위...
 - 은, 국내 반도체 기업 해킹으로 설계도면과 현
 - Weekly Security Premium Repo...
 - [bnTV] 개인정보 보호법에서 말하는 '개인정보'
 - 아이돌 그룹 아이브-몬스타엑스-크레디티 유
 - 새학기를 맞은 자녀들에게 꼭 알려줘야 할 계
 - 최근 '브라우저 자동 로그인' 기능 악용한 계정
 - 공로별 합영을 노선 설치파일로 위장한 MSX

주요 기업별 기사

ISC2 tp-link

중소기업 사이버대피소 누적이용 현황 (단위: 건)



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

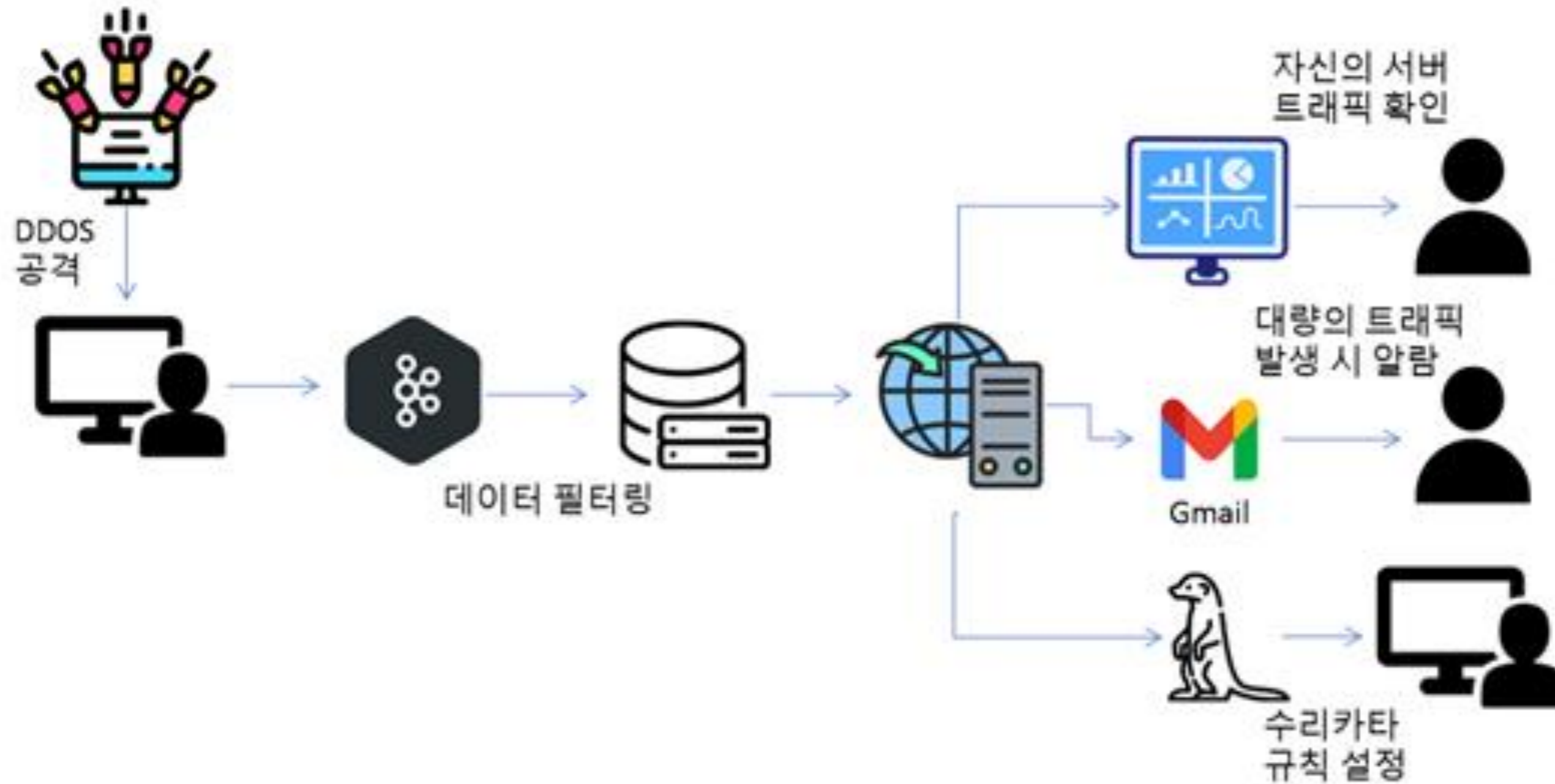
CHAPTER 3 개발 환경

프레임 워크 및
도구



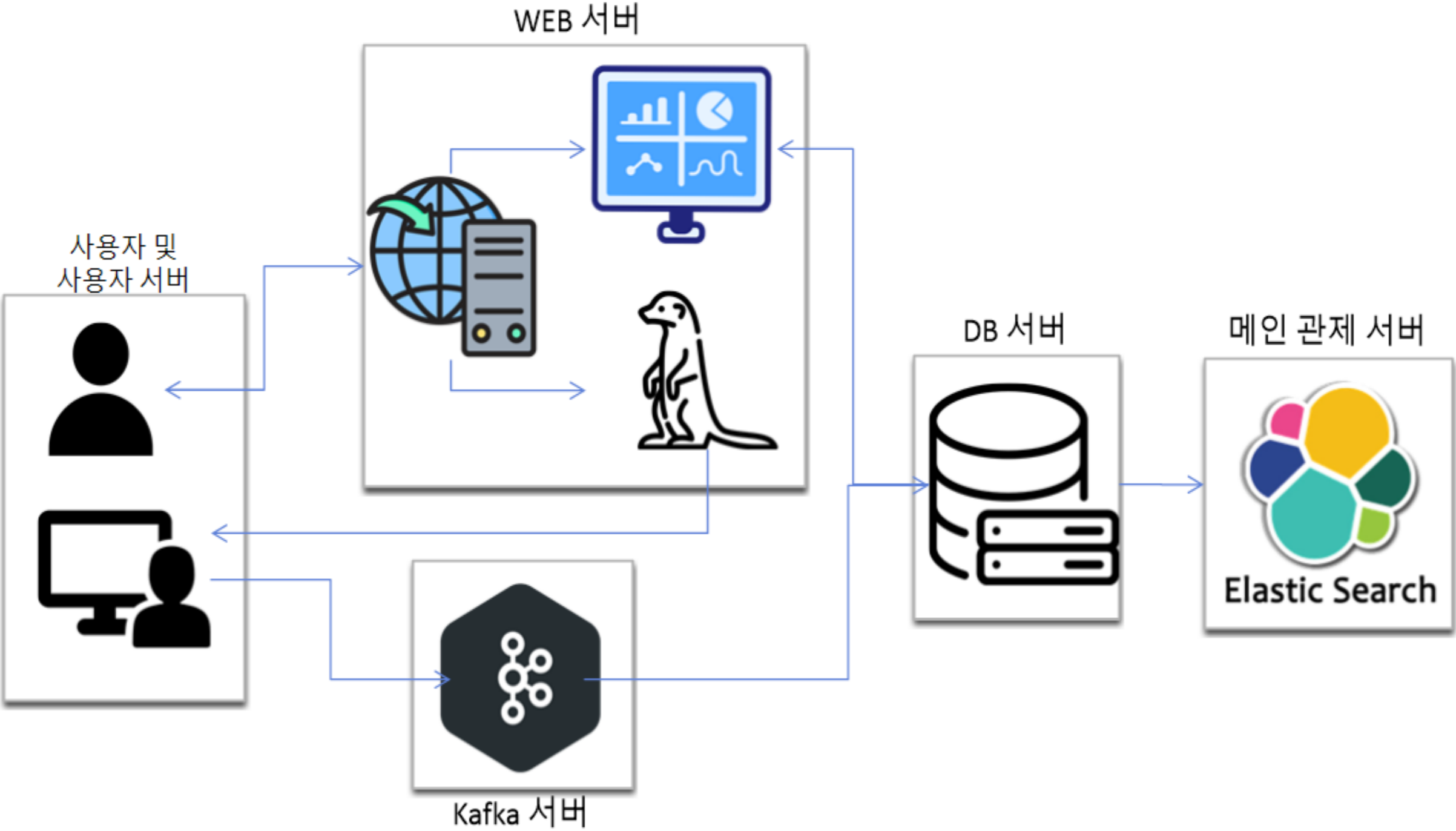
CHAPTER 3 개발 환경

서비스 구상도



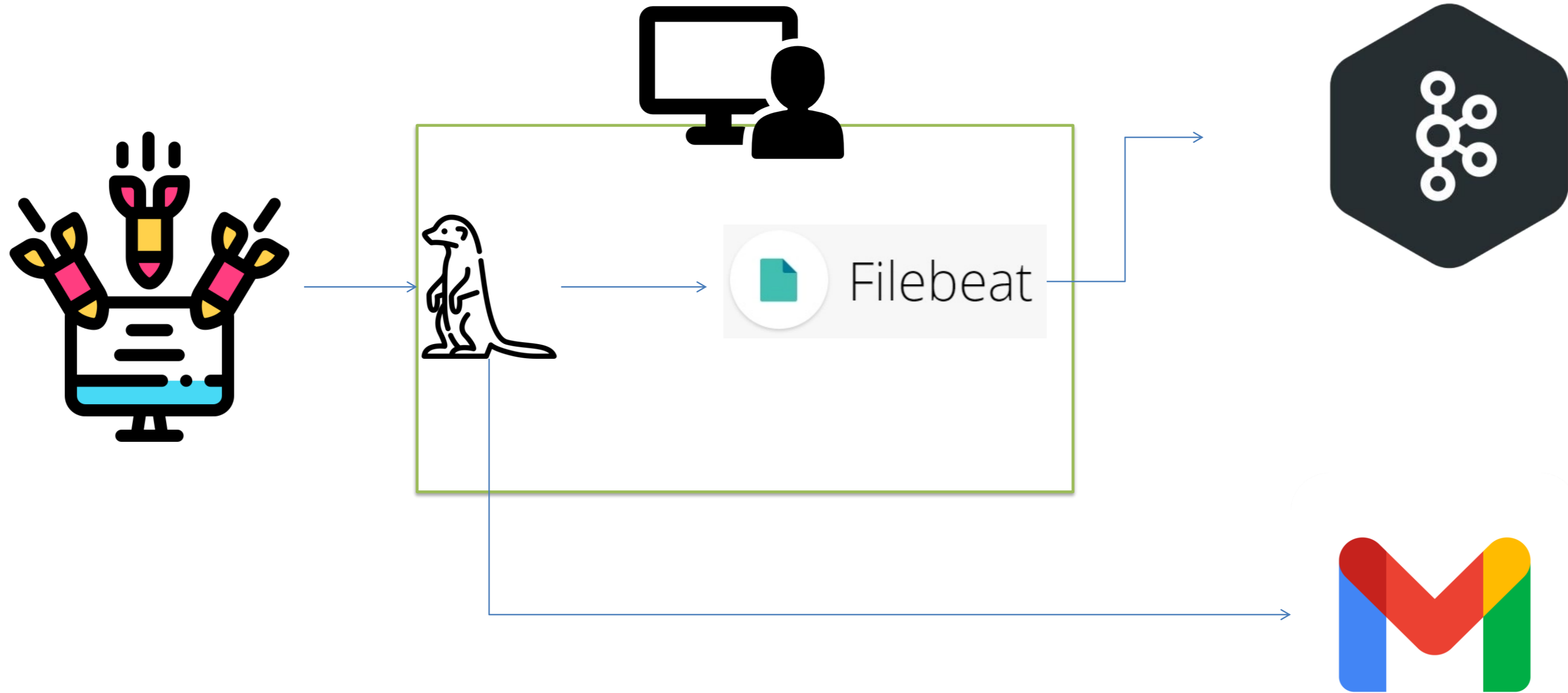
CHAPTER 3 개발 환경

아키텍처 구상도



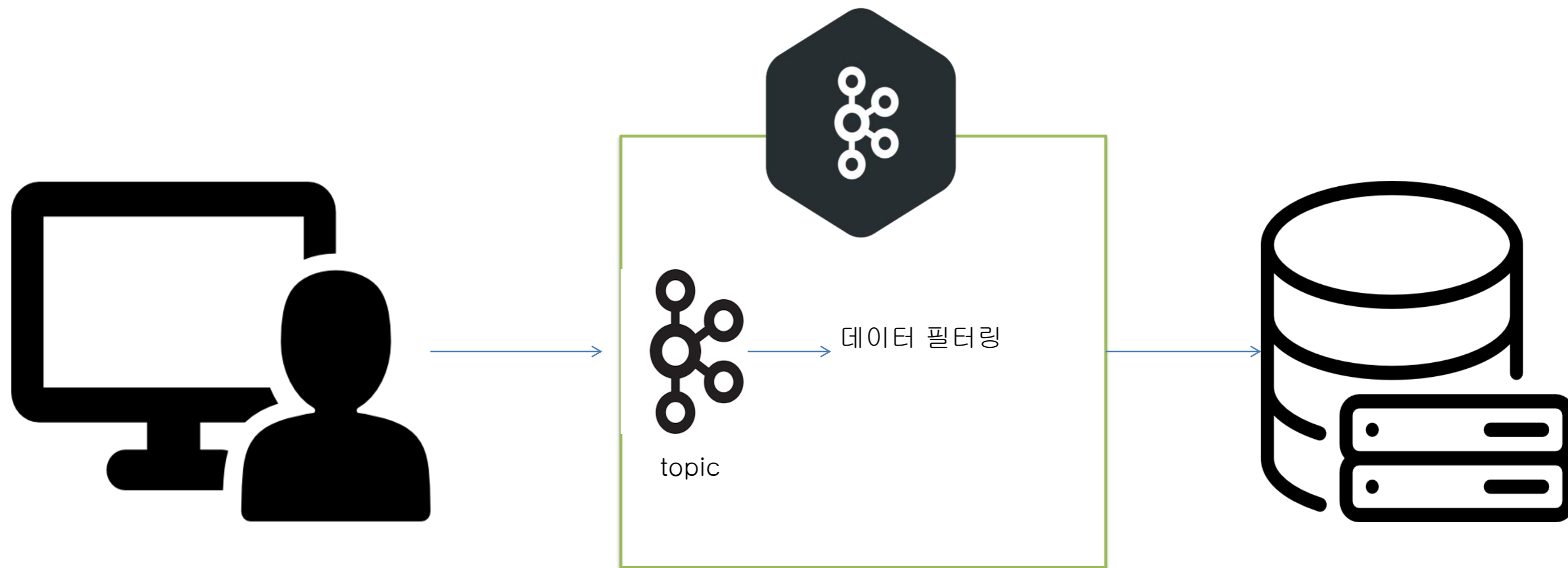
CHAPTER 3 개발 환경

피해자 서버



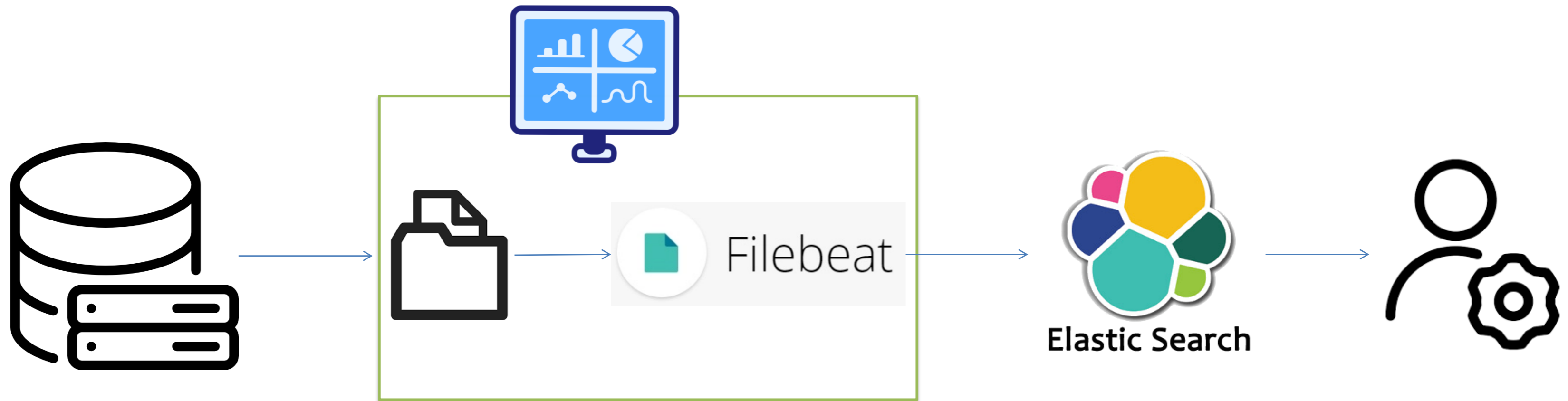
CHAPTER 3 개발 환경

카프카 서버



CHAPTER 3 개발 환경

메인관제 서버



CHAPTER 4 웹사이트 구성



CHAPTER 4 웹 사이트 구성

aDDoS

ELK Kafka Python Django

4가지 기술로 만들어진 네트워크 탐지 서비스입니다

웹서비스로 제공되어 사용자의 편리한 네트워크 보안을 제공합니다

[About Us](#) [Usage](#) [Login](#)



© aDDoS. All rights reserved.

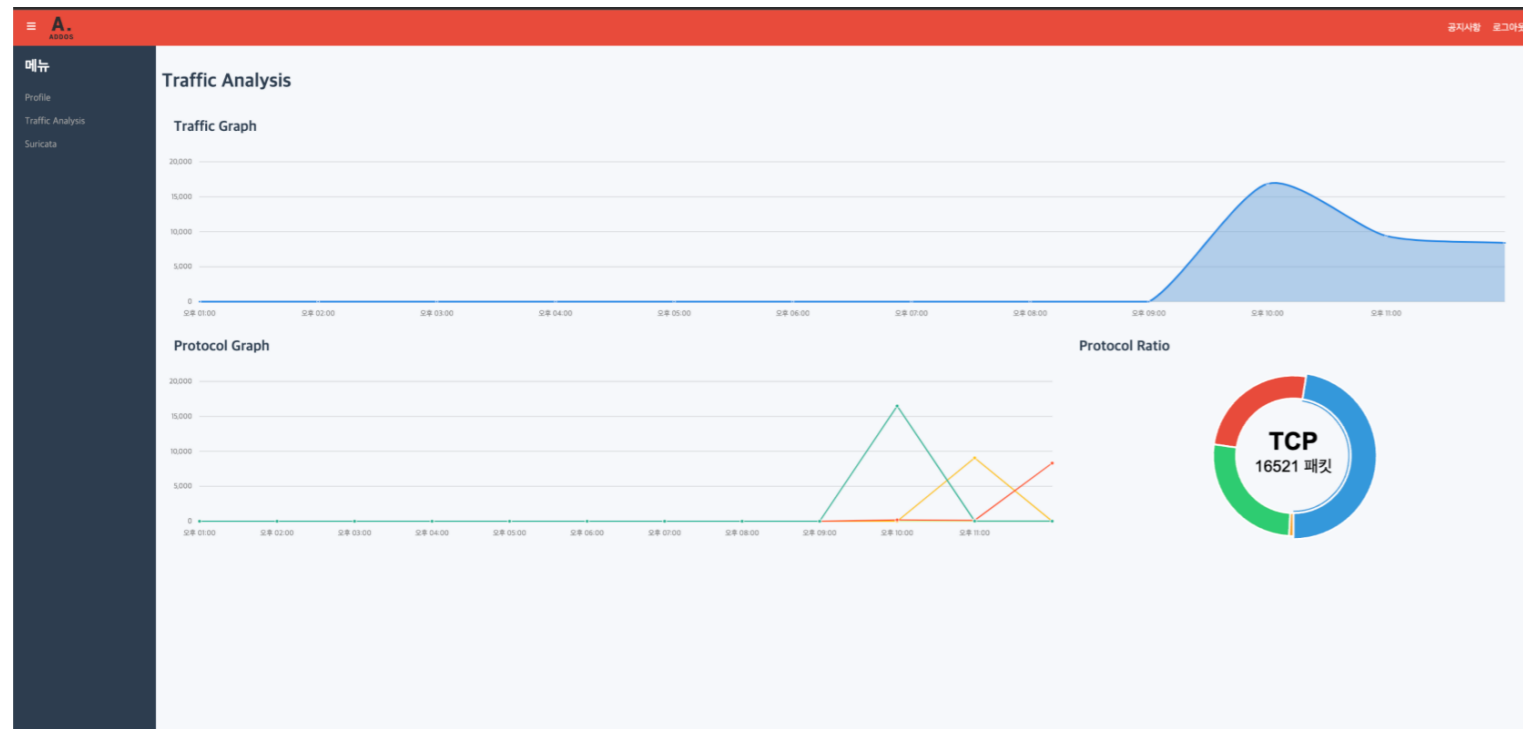
서비스 이용 방법

아래의 이메일 폼에 이메일을 입력하시면 세팅 스크립트가 포함된 메일이 발송됩니다. 메일을 받으신 후 스크립트를 실행하시면 됩니다.

당신의 이메일:

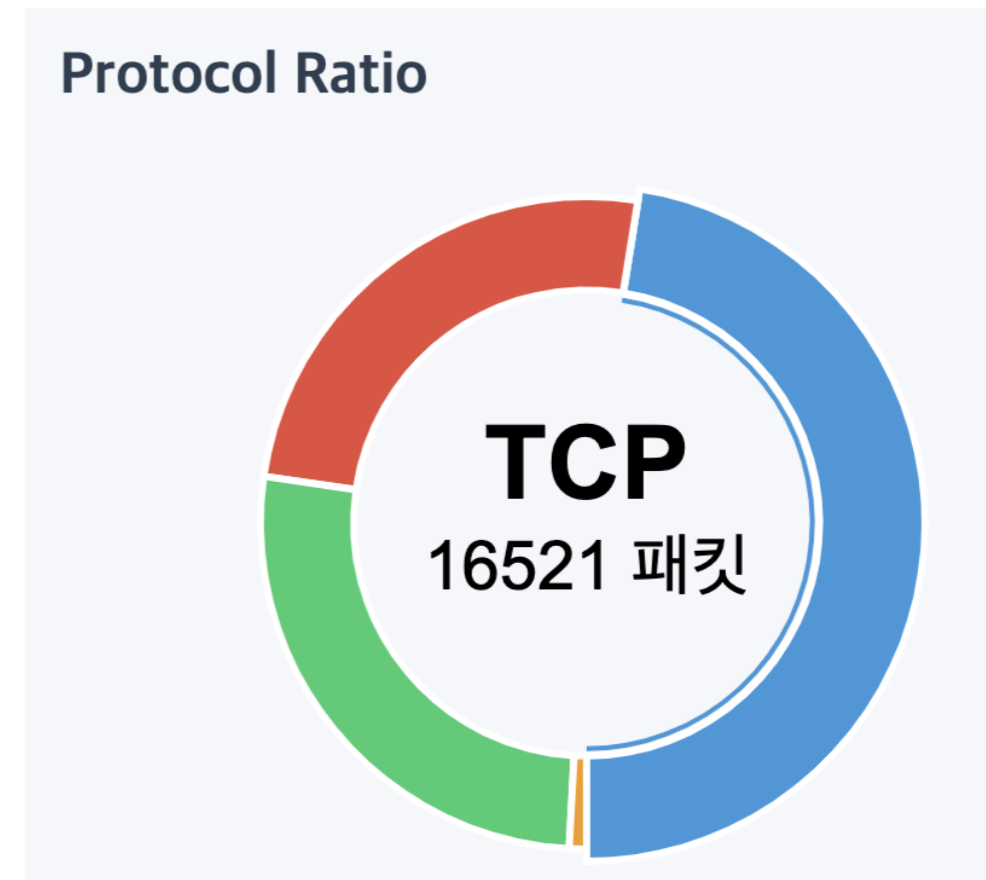
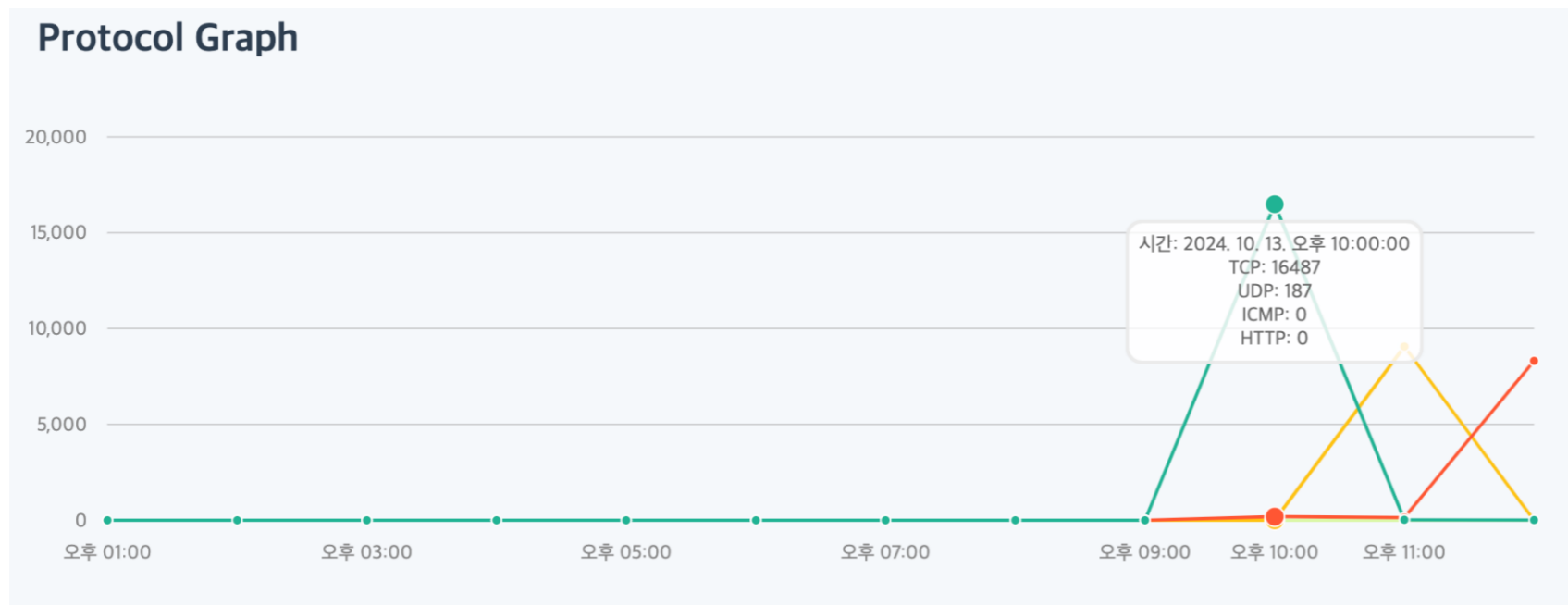
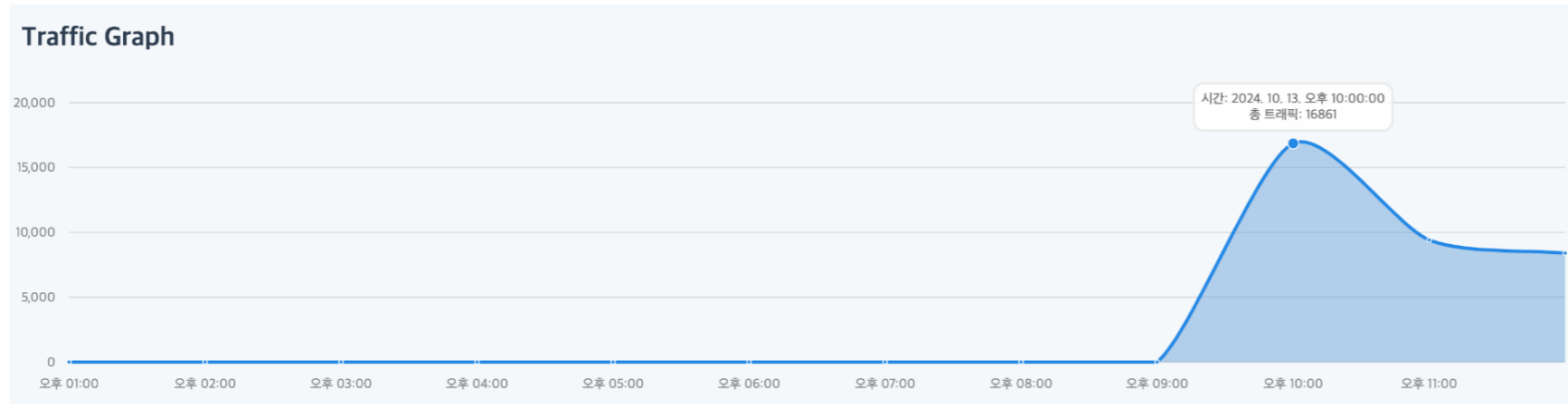
구독하기

CHAPTER 4 웹사이트 구성



The screenshot shows the 'Suricata Rules' configuration page. It has a dark blue sidebar with a menu containing 'Profile', 'Traffic Analysis', and 'Suricata'. The main content area is titled 'Suricata Rules' and contains two sections: 'Suricata Rule Input' and 'Server Rule'. Each section has a large text input field and a red 'Submit' button.

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

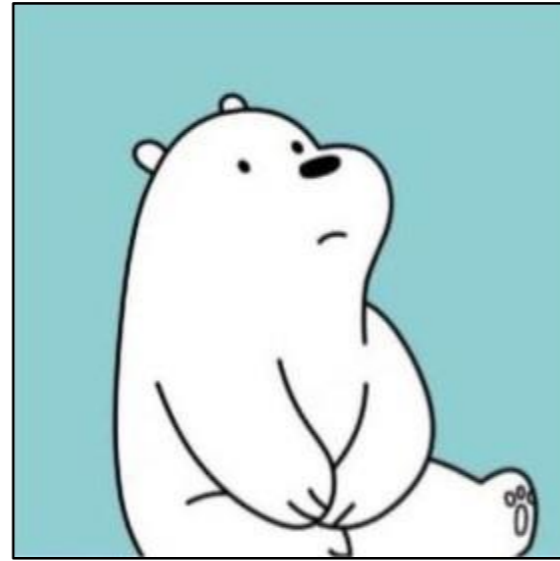
Traffic Analysis

트래픽 시각화를 통한
요소 별 확인 가능
중요한 정보 시각화

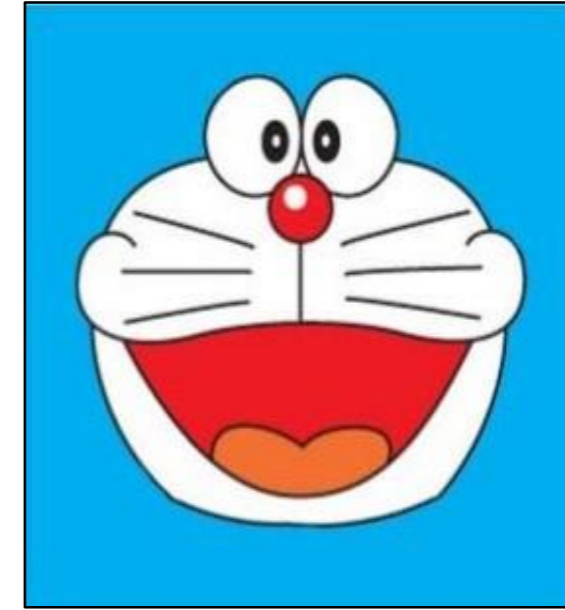
CHAPTER 1 팀원 소개



이두리
팀장



박주형
팀원



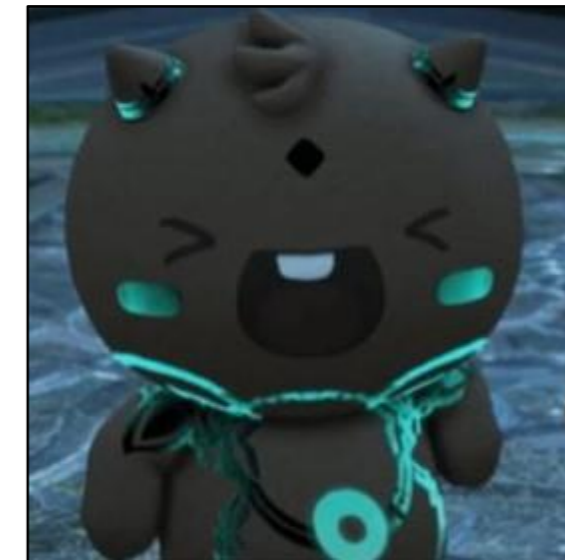
송경선
팀원



김동철
팀원



이라규
팀원



이건우
팀원

네트워크 공격 분석 및 트래픽 시각화
(aDDoS)

감사합니다