

S E M O

Security Monitoring Platform

# 목차

## INDEX

1<sup>st</sup>

프로젝트 개요

2<sup>nd</sup>

프로젝트 소개

3<sup>rd</sup>

기대효과

4<sup>th</sup>

역할분담

**1.프로젝트 개요**

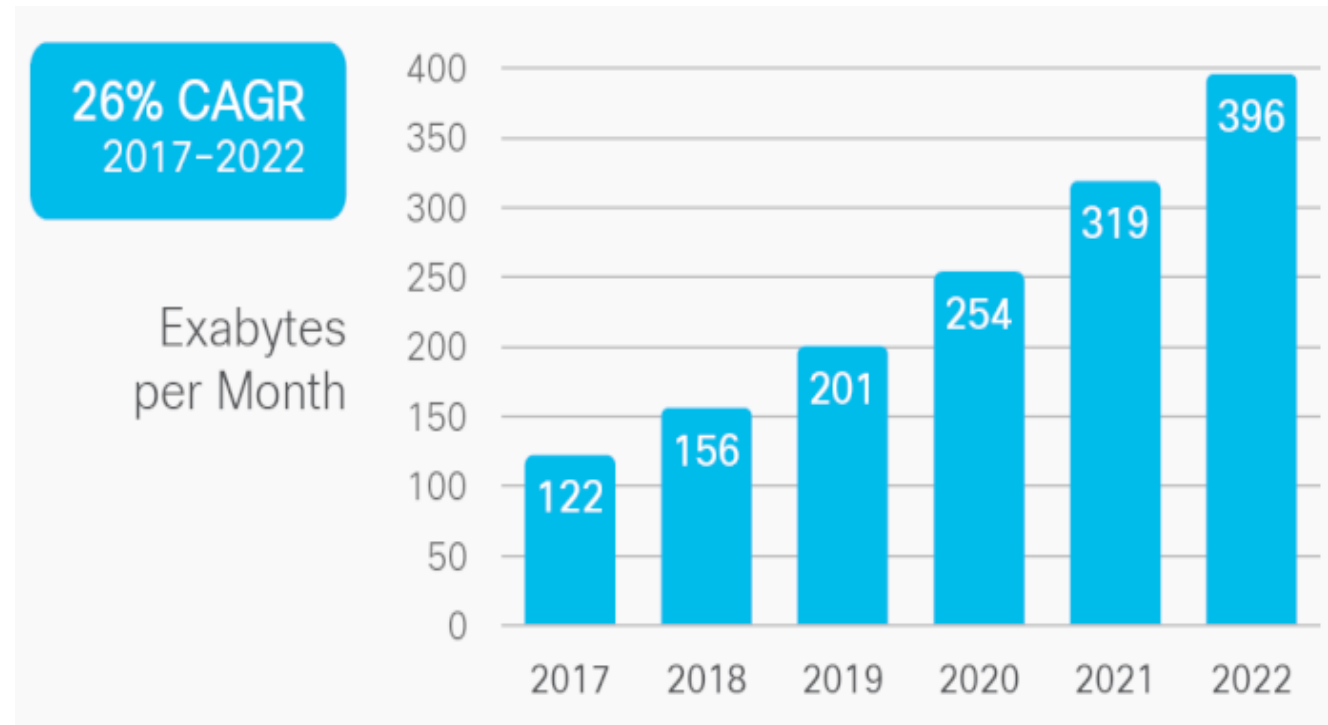
2.프로젝트 소개

3.기대효과

4.역할분담

# 프로젝트 개요

## 네트워크 트래픽 & 보안관제 서비스 증가



전세계 월별 IP 트래픽 전망

출처: Cisco VNI Global IP Traffic Forecast, 2017-2022

# 프로젝트 개요

## 네트워크 트래픽 & 보안관제 서비스 증가

[표 3-10] 정보보안산업 중분류 매출 현황

(단위 : 백만원, %)

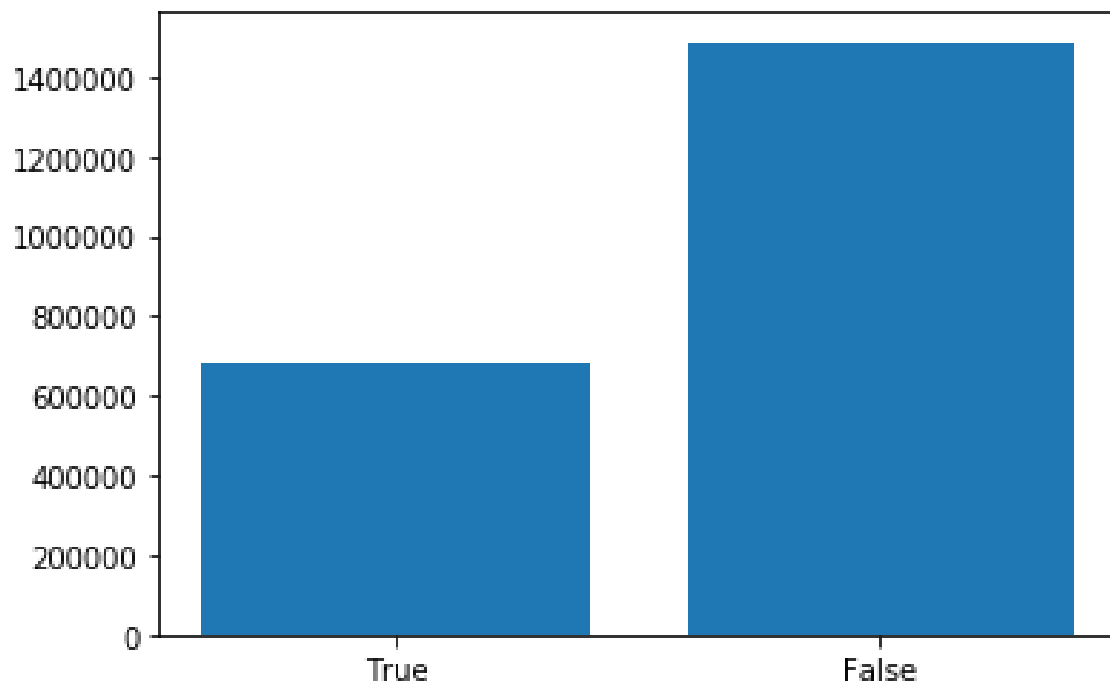
구분		2018년	2019년(E)	증감율(%)
정보보안 시스템 개발 및 공급	네트워크보안 시스템 개발	729,393	771,656	5.8
	시스템보안 솔루션 개발	488,402	523,115	7.1
	정보유출방지 시스템 개발	426,128	456,251	7.1
	암호/인증 시스템 개발	151,879	161,760	6.5
	보안관리 시스템 개발	297,920	327,790	10.0
	소계	2,093,723	2,240,572	7.0
정보보안 관련 서비스	보안컨설팅 서비스	302,099	321,478	6.4
	보안시스템 유지관리/ 보안성 지속 서비스	351,942	359,645	2.2
	보안관제 서비스	273,927	286,880	4.7
	보안교육 및 훈련 서비스	1,740	2,990	71.8
	공인/사설 인증서	59,496	66,122	11.1
	소계	989,203	1,037,115	4.8
합계		3,082,926	3,277,687	6.3

2019 국내 정보보호산업 실태조사 보고서

출처: 2019 국내 정보보안 산업, 매출 3조 2천 700억원... 수출액은 1천 80억원 기록

## 프로젝트 개요

빅데이터 보안관제 걸림돌, 오탐(False Positive)



Event Log데이터 정탐/오탐 비율  
출처: KISTI(한국과학기술정보연구원)

정탐 : 오탐  $\approx$  3 : 7

1.프로젝트 개요

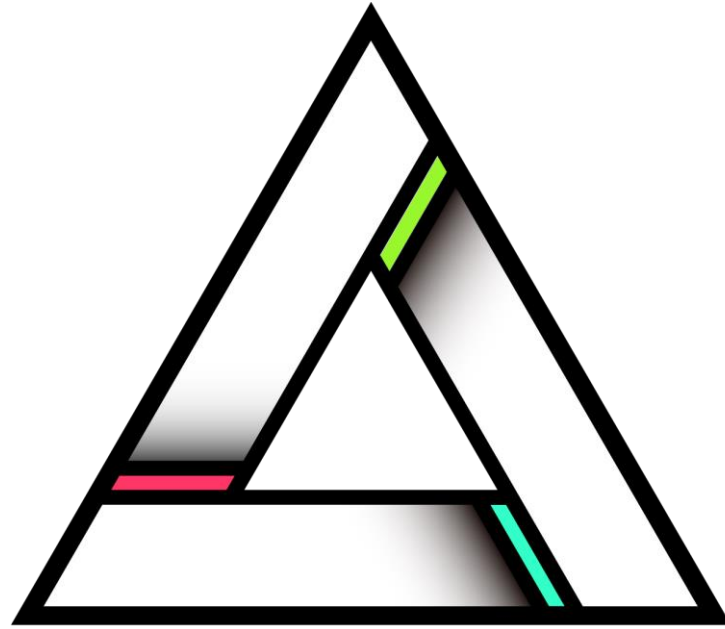
2.프로젝트 소개

3.기대효과

4.역할분담

# 프로젝트 소개

## 프로젝트 로고 및 이름 소개



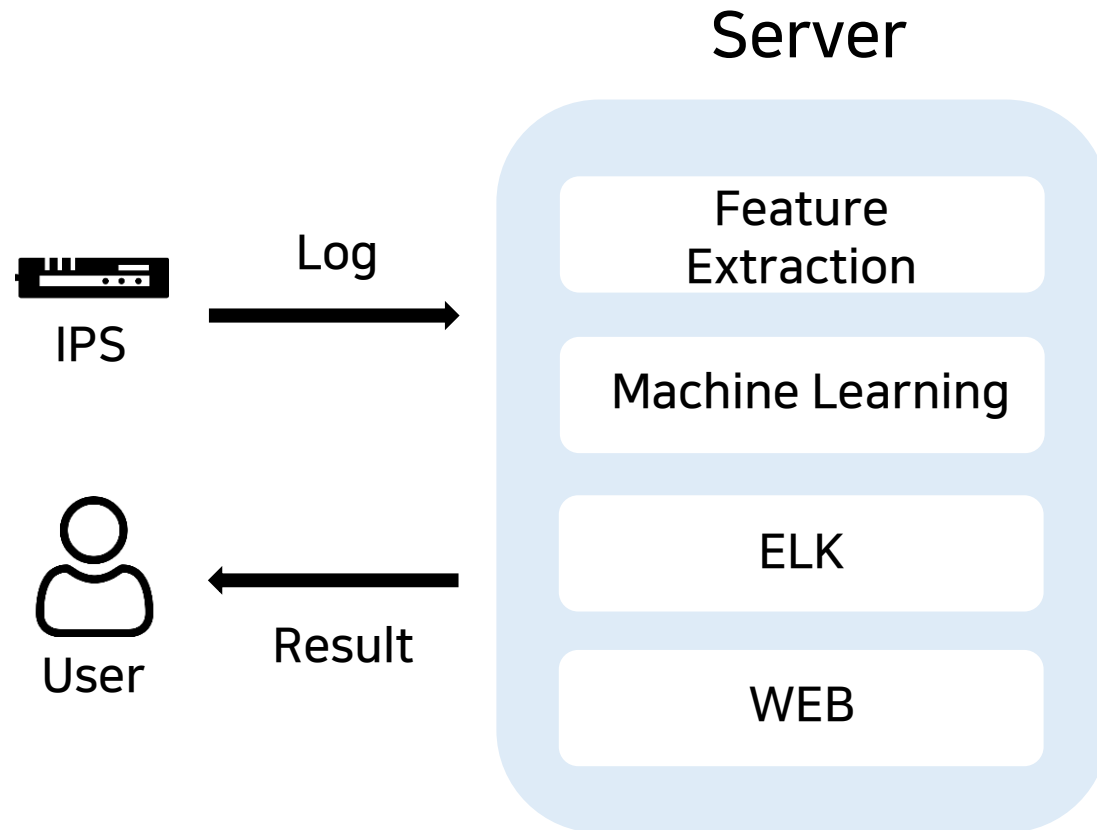
S E M O

**SE**curity **MO**nitoring Platform Using Event Logs



# 프로젝트 소개

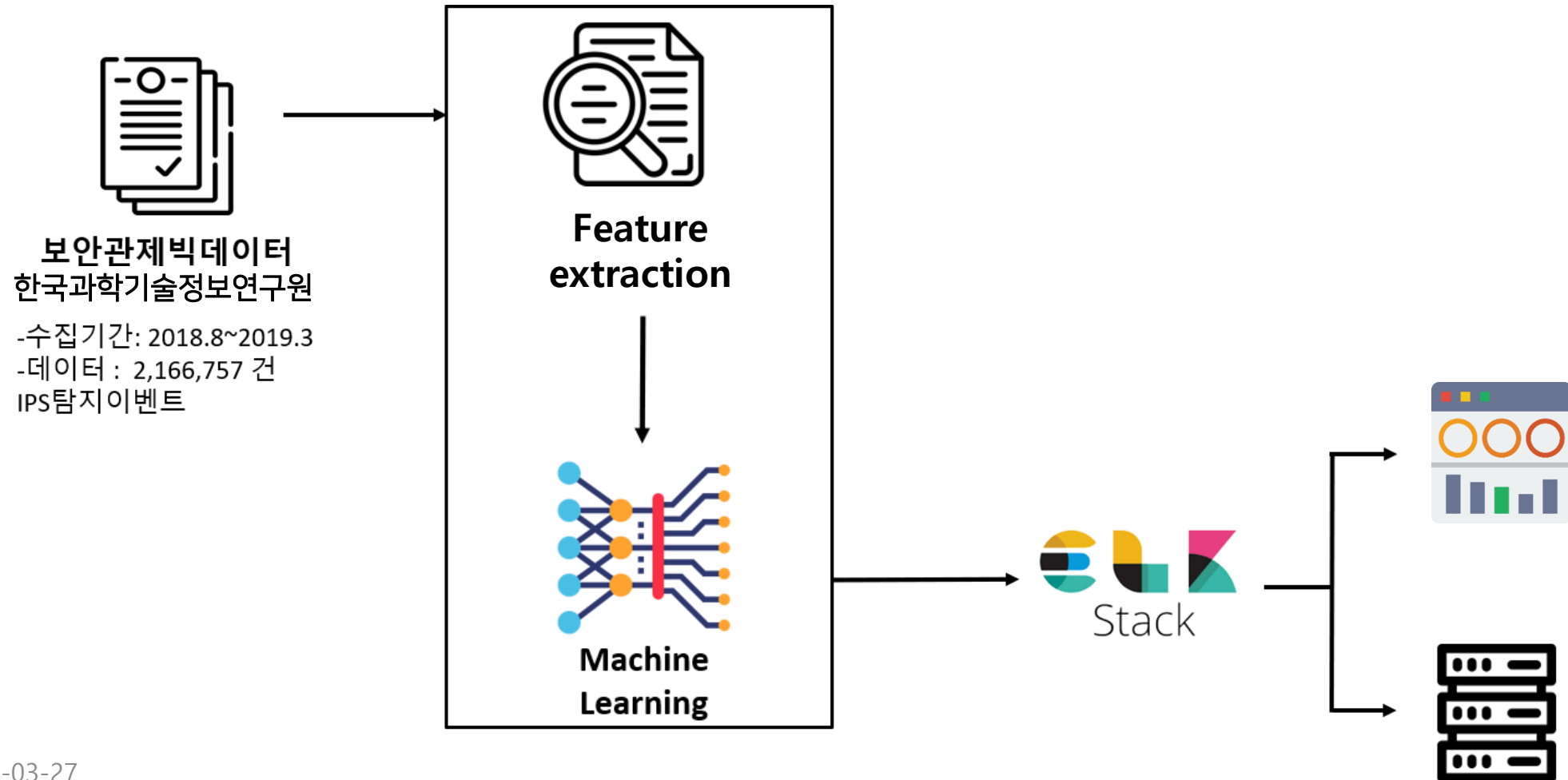
## 프로젝트 개발 목표



- IPS: Intrusion Prevention System  
→ 침입 방지 시스템
- ELK: Elastic + Logstash + Kibana

# 프로젝트 소개

## 프로젝트 개발 과정



# 프로젝트 소개

## 데이터

### DATA

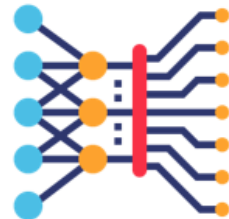


보안관제빅데이터  
한국과학기술정보연구원

-수집기간: 2018.8~2019.3  
-데이터 : 2,166,757 건  
IPS탐지이벤트



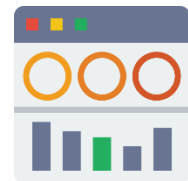
Feature  
extraction



Machine  
Learning

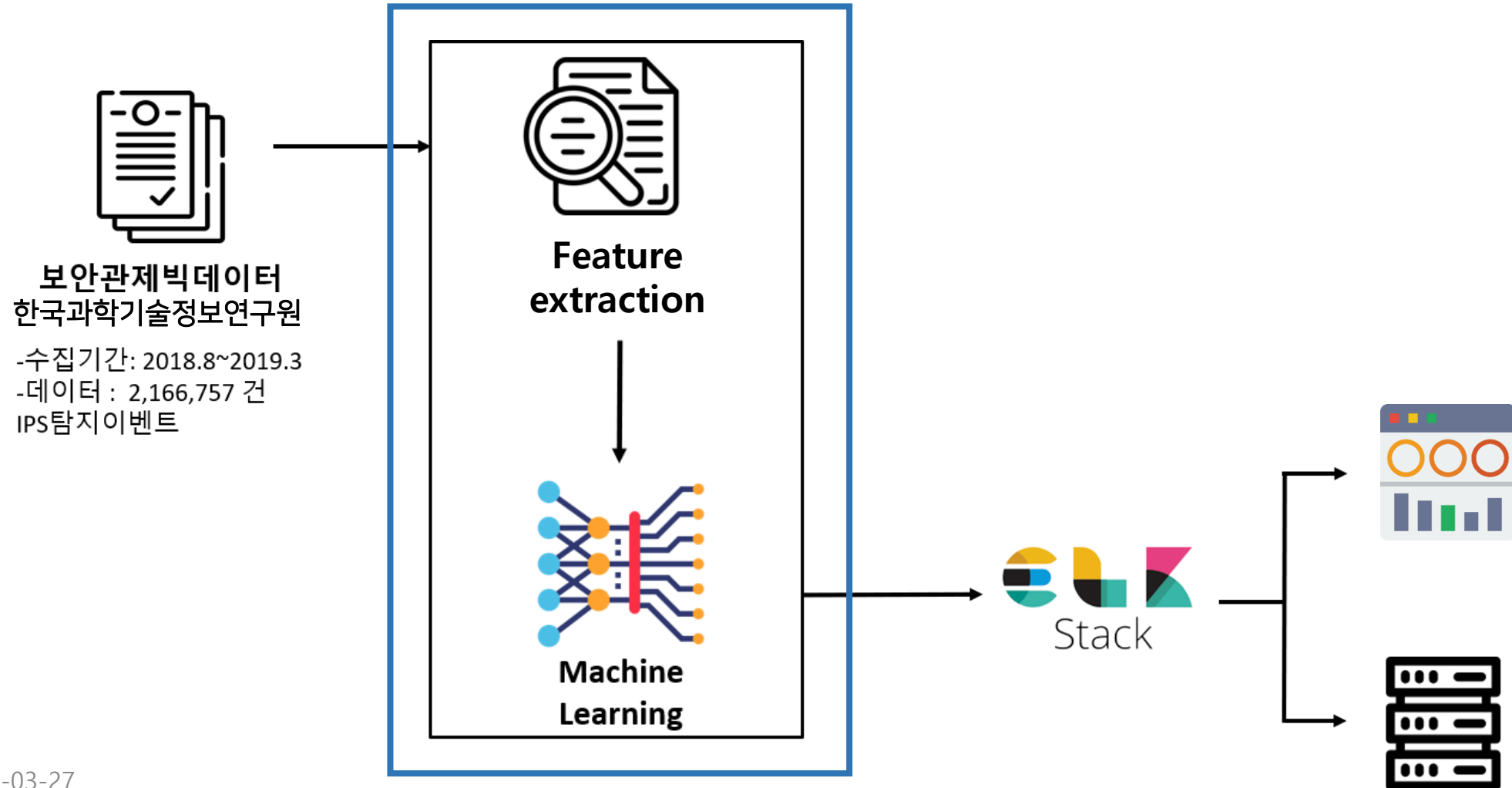


Stack



# 프로젝트 소개

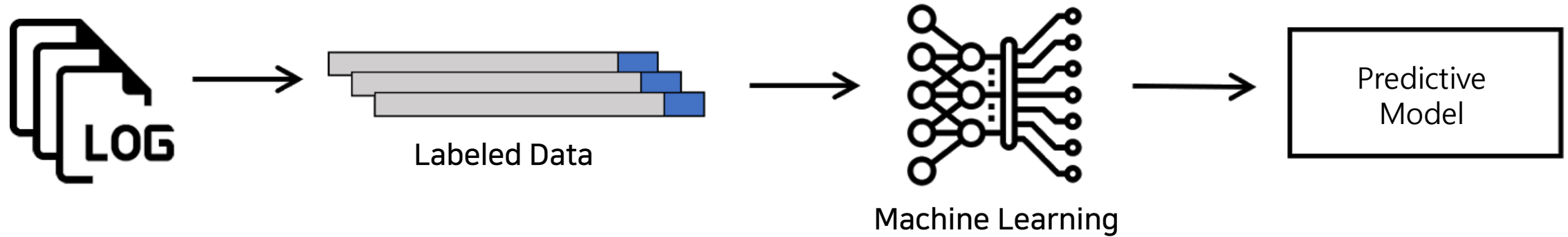
## 머신러닝



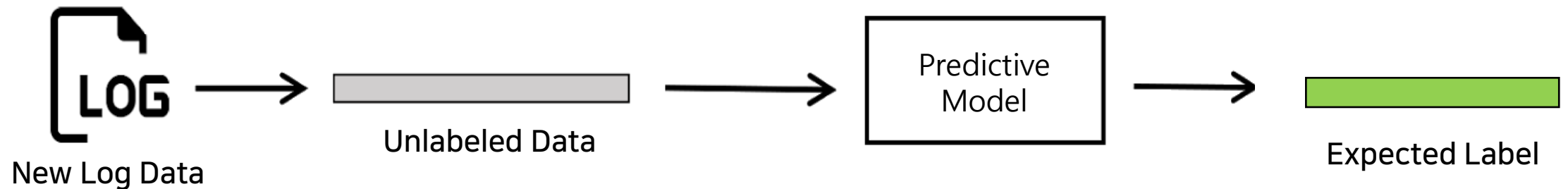
# 프로젝트 소개

## 머신러닝

### TRAIN

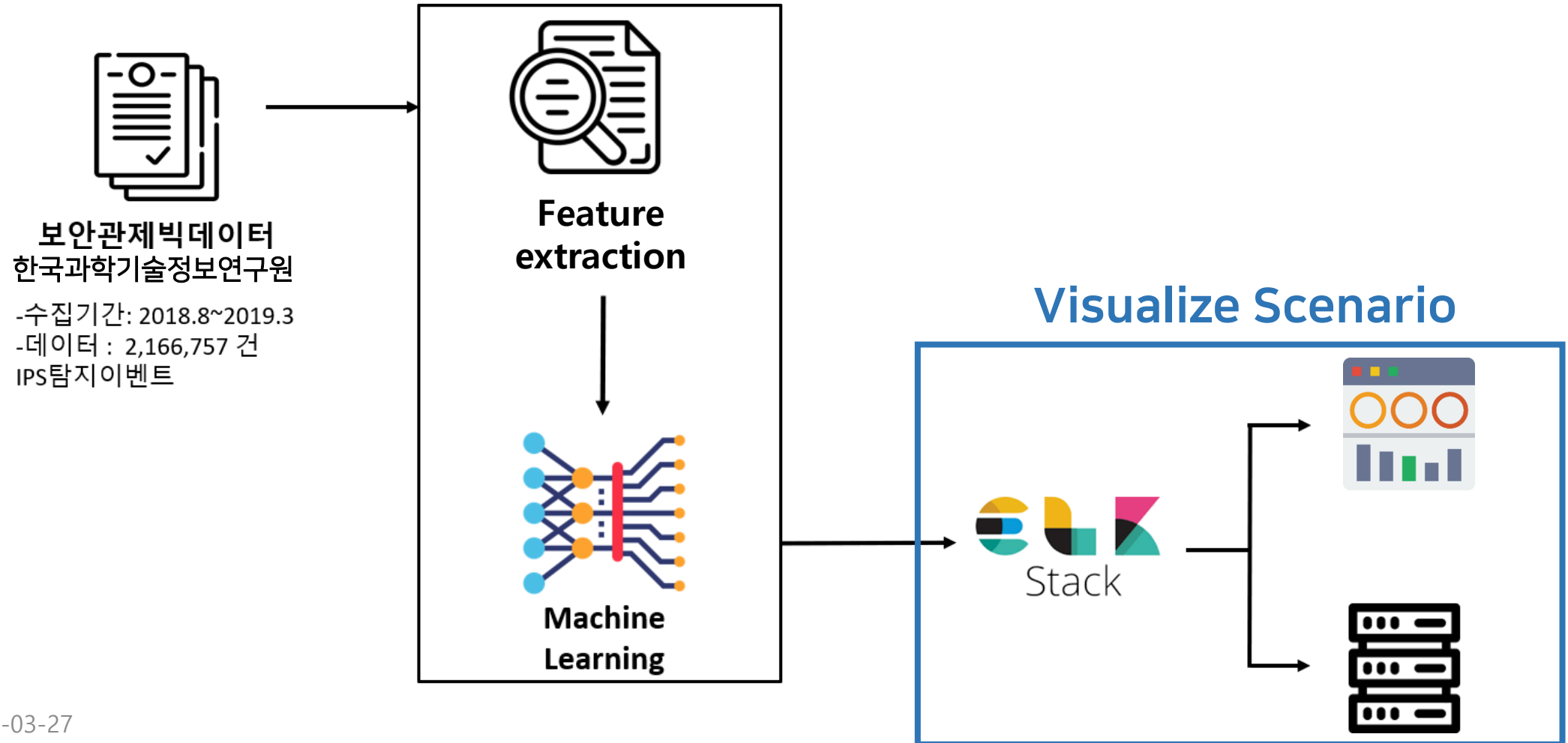


### INFERENCE



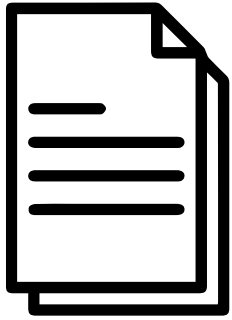
# 프로젝트 소개

## 분석 플랫폼 시연

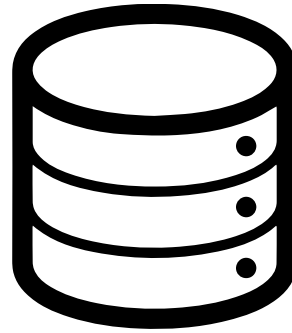
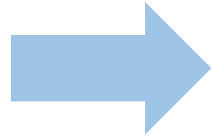


# 프로젝트 소개

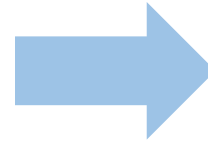
## 시연방법



Data Processing



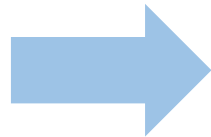
Save & Manage



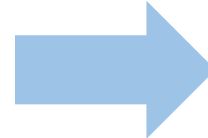
Visualization



Logstash



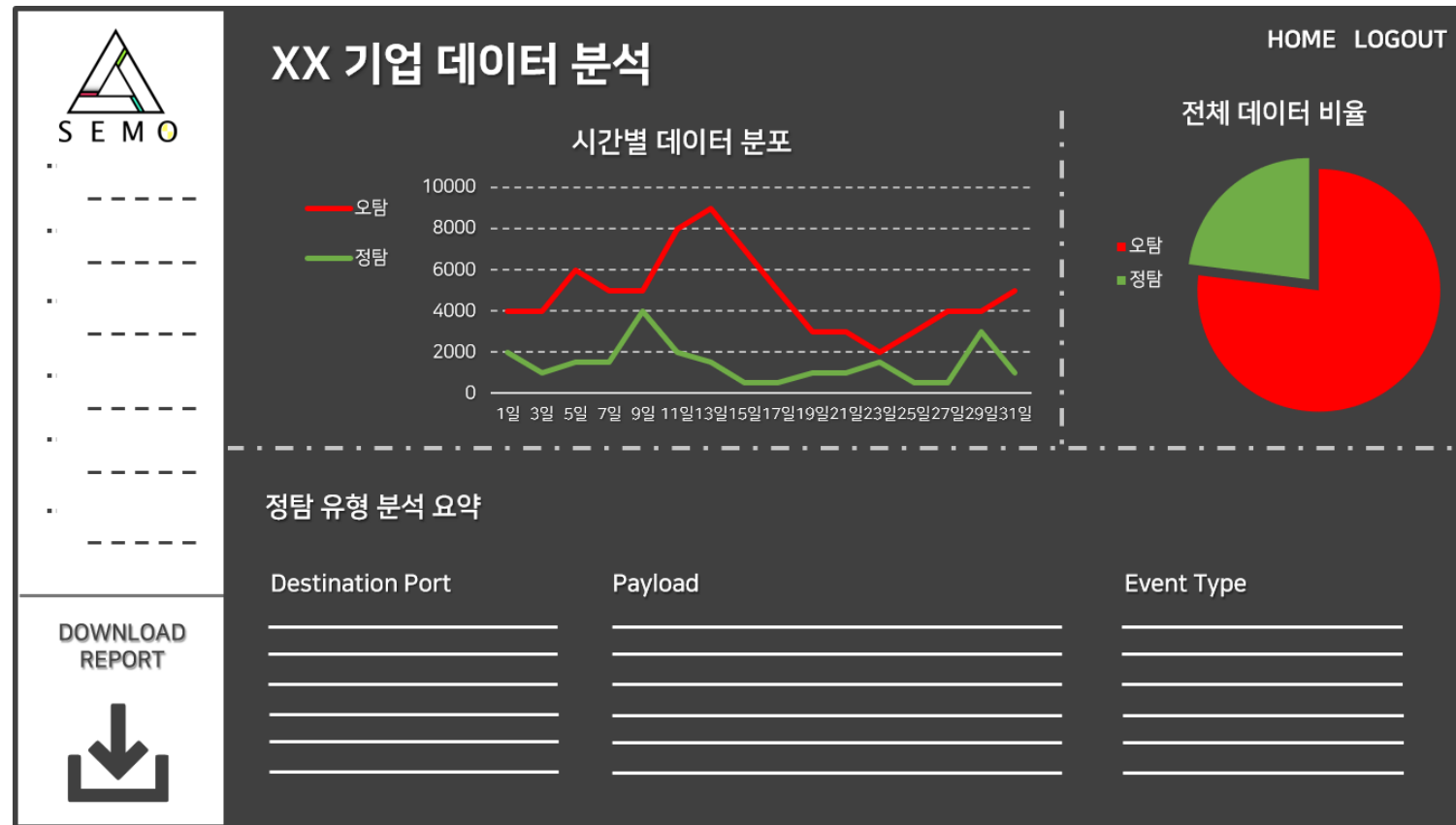
Elasticsearch



Kibana

# 프로젝트 소개

## 플랫폼 예시



<플랫폼 예시 화면>



1.프로젝트 개요

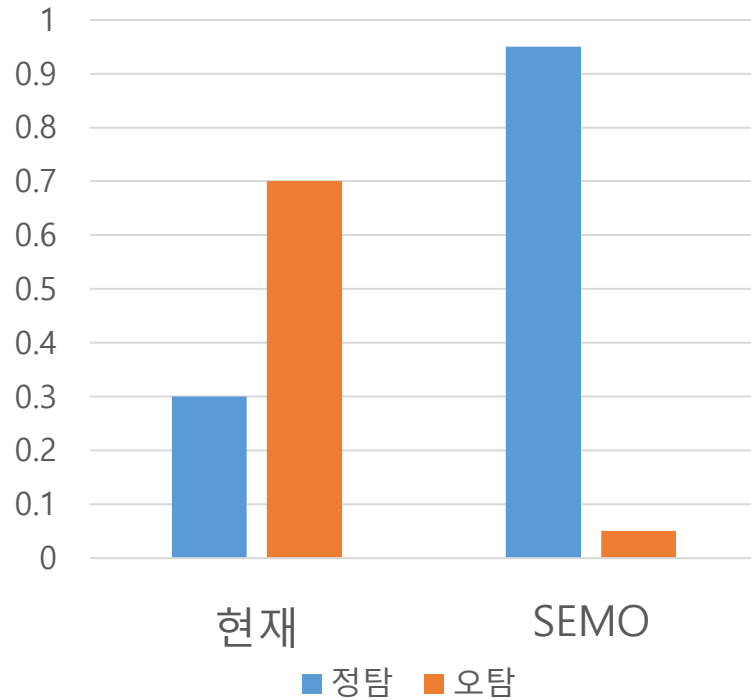
2.프로젝트 소개

3.기대효과

4.역할분담

## 기대 효과

### 목표 기대 효과



SEM0의 정/오탐 분류

→ 보안관제사의 업무 효율성 증가



오픈소스 기반 보안관제 플랫폼 제공

→ 자체적 보안관제 가능

1.프로젝트 개요

2.프로젝트 소개

3.기대효과

4.역할분담

# 역할분담

## 팀원 소개



### 전하훈(팀장)

머신 러닝 모델 설계 및 구축  
논문 분석



### 김성은

데이터 분석 및 시각화  
피쳐 엔지니어링



### 최현인

ELK 구축 및 문서 작업  
서버 안정화

### 최운호


웹 서버 구축  
웹 서버-모델 연동



### 허윤서

웹 프론트 구축  
웹-ELK 연동





감사합니다

- Capstone 7. SEMO -