

# Docker Malware Detection

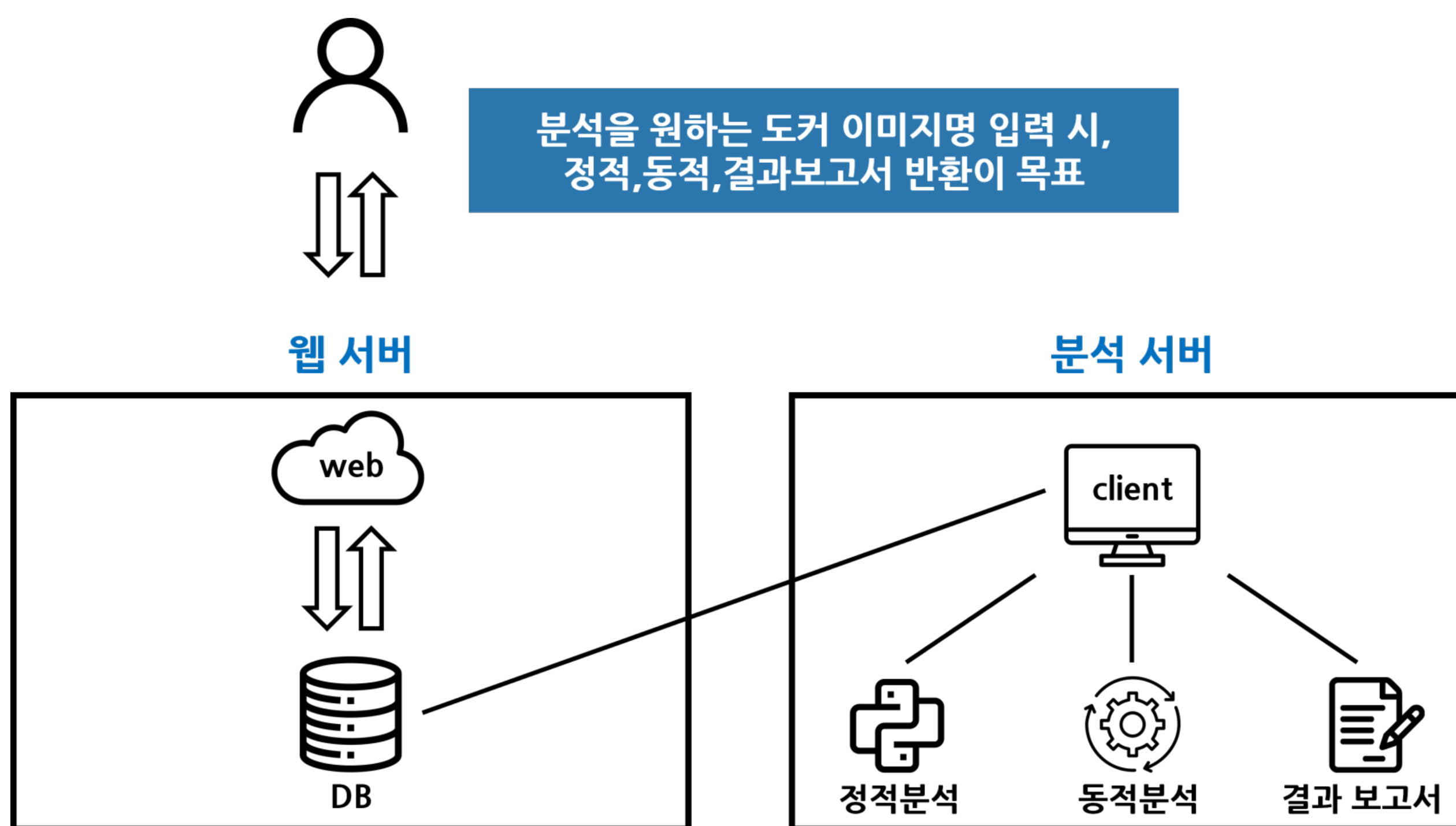
## 개요

도커허브 내 다수의 도커 이미지에는 여러 취약점이 존재하며, 악성 도커 이미지 또한 증가하고 있다. 이로 인한 **피해 예방**을 목표로 악성 도커 이미지 **정적·동적 분석**을 진행하고, **결과 보고서 및 조치 가이드**를 제공하는 웹 서비스를 개발하였다.

## 팀 소개

- 지도교수 | 이병천 교수님
- 유재겸 | 샌드박스 기능 구현
- 서민재 | 도커 이미지 정적분석 기능 구현
- 이다영 | 도커 이미지 동적분석 기능 구현
- 이유경 | 도커 이미지 진단 조치 가이드 제작
- 김우종 | 웹 서비스 개발
- 남서현 | 웹 서비스 개발
- 장혜선 | 웹 서비스 개발

## 서비스 구성도 및 결과물



상세 분석 보고서

> 정적분석

> 동적분석

도커 이미지 정보

이미지명	ynsprpagem
이미지 업로더	ynsprpagem
정적분석 시간	2023-10-11

보안 취약점

\* 도커 이미지 내 보안 취약점이 존재하는지

TOTAL	1192
UNKNOWN	0
LOW	412
MEDIUM	716
HIGH	63
CRITICAL	1

### 2.2. 네트워크 검사

DD 2-1-1	다. 접근 통제 > 외부 아이피 통신: 악성 아이피로 분류	위험도	상
취약점 개요			
점검 내용	■ 외부 아이피와의 통신 탐지 및 통신한 아이피의 악성 여부 점검		
점검 목적	■ 악성 아이피 통신으로 인한 악성코드 다운로드 등 문제를 방지하기 위함		
보안 위협	■ 시스템 해킹, 악성코드 전파, 개인정보 유출 등의 문제를 초래할 수 있음		
판단 기준 및 진단 방법			
판단 기준	■ 외부 아이피와 통신 및 해당 아이피가 악성으로 식별되는 경우		
진단 방법	■ 아래 명령어를 통해 네트워크 연결 상태 확인 및 현재 통신하는 아이피 확인		
	<pre># netstat -an Active Internet connections (servers and established) Proto Recv-Q Send-Q Local Address           Foreign Address         State tcp        0      0 172.17.0.2:49120       49.12.80.39:45560      SYN_SENT Active UNIX domain sockets (servers and established) Proto RefCnt Flags               Type           State         I-Node   Path </pre>		
조치 방법	■ 악성으로 식별된 아이피와의 통신을 차단하도록 방화벽 규칙을 설정하거나, 이미지를 수정하여 해당 통신을 제거함		

도커 이미지 분석 서비스 및 조치 가이드