Docker Malware Detection

Team. 야자나무
유재겸, 서민재, 이다영, 이유경, 김우종, 남서현, 장혜선

목차

01

프로젝트 소개

1-1. 팀원 소개

1-2. 프로젝트 배경

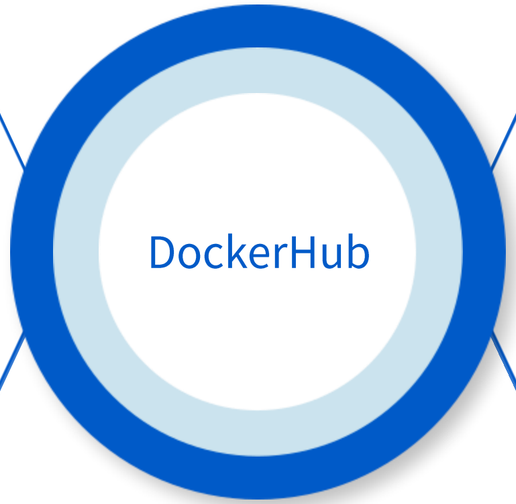
1-3. 프로젝트 목적

1-1. 팀원 소개

이름	수행 파트
유재겸(팀장)	샌드박스 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

1-2. 프로젝트 배경

취약한 도커 이미지
다수 존재



악성 도커 이미지
지속 증가

도커 이미지를
Pull 하여 내려받는
사용자에게 위험 전가

시중에 공개된
도커 이미지
분석 서비스의 부재

1-3. 프로젝트 목적

편리한 분석

웹 서버와 분석 서버 간 연동을 통해
실시간 분석 기능을 제공함으로써
사용자의 **분석 편의성 증대**

악성 도커 이미지 대비

도커 이미지 **정적/동적 분석**을 통해 정확한
탐지 결과를 도출하고,
조치 가이드를 제공하여 **취약한 도커 이미지
및 악성 도커 이미지에 대비**

02

프로젝트 개발

2-1. 구상도

2-2. 정적분석

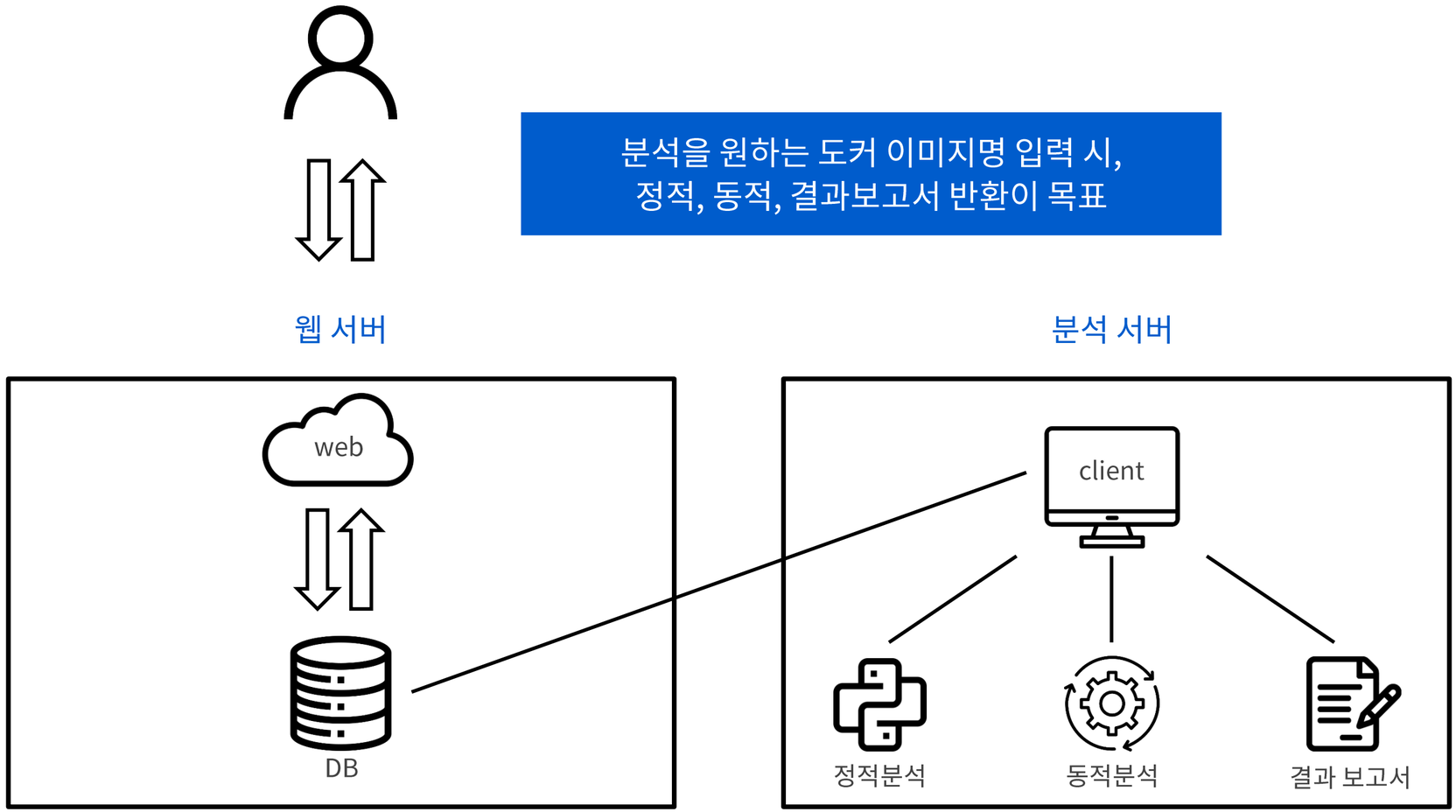
2-3. 샌드박스 및 동적분석

2-4. 웹 사이트

2-5. 컨설팅

2-1. 구상도

분석을 원하는 도커 이미지명 입력 시,
정적, 동적, 결과보고서 반환이 목표



2-2. 정적분석

Trivy를 이용한 CVE 진단

```
centos:latest (centos 8.4.2105)
================================
Total: 439 (UNKNOWN: 0, LOW: 158, MEDIUM: 253, HIGH: 28, CRITICAL: 0)

┌──────────────────────────┬──────────────────┬──────────┬──────────────────┬──────────────────────┬──────────────────────────────────────────────────────────────┐
│         Library          │  Vulnerability   │ Severity │ Installed Version │    Fixed Version     │                            Title                             │
├──────────────────────────┼──────────────────┼──────────┼──────────────────┼──────────────────────┼──────────────────────────────────────────────────────────────┤
│ bind-export-libs         │ CVE-2021-25215   │ HIGH     │ 32:9.11.26-3.el8 │ 32:9.11.26-4.el8_4   │ bind: An assertion check can fail while answering queries    │
│                          │                  │          │                  │                      │ for DNAME records...                                         │
│                          │                  │          │                  │                      │ https://avd.aquasec.com/nvd/cve-2021-25215                   │
│                          ├──────────────────┤          │                  ├──────────────────────┼──────────────────────────────────────────────────────────────┤
│                          │ CVE-2022-38177   │          │                  │ 32:9.11.36-3.el8_6.1 │ bind: memory leak in ECDSA DNSSEC verification code           │
│                          │                  │          │                  │                      │ https://avd.aquasec.com/nvd/cve-2022-38177                   │
│                          ├──────────────────┤          │                  │                      ├──────────────────────────────────────────────────────────────┤
│                          │ CVE-2022-38178   │          │                  │                      │ bind: memory leaks in EdDSA DNSSEC verification code         │
│                          │                  │          │                  │                      │ https://avd.aquasec.com/nvd/cve-2022-38178                   │
│                          ├──────────────────┼──────────┤                  ├──────────────────────┼──────────────────────────────────────────────────────────────┤
│                          │ CVE-2021-25214   │ MEDIUM   │                  │ 32:9.11.26-6.el8     │ bind: Broken inbound incremental zone update (IXFR) can      │
│                          │                  │          │                  │                      │ cause named to terminate...                                  │
│                          │                  │          │                  │                      │ https://avd.aquasec.com/nvd/cve-2021-25214                   │
```

Trivy를 이용하여 Docker image의 **CVE** 정보를 추출하는 Python 자동화 스크립트 작성

2-3. 샌드박스 및 동적분석

샌드박스 동적분석 동작 흐름

1 정적분석 종료

2 샌드박스 실행
- VirtualBox 실행
- 스냅샷 실행
- SSH 연결
- 대상 컨테이너 실행

3 동적분석 수행
- Root 권한 체크
- 네트워크 검사
- 열린 프로세스 검사
- 자동 실행파일 검사

4 결과 DB 저장

2-3. 샌드박스 및 동적분석

동적분석 과정

```
['49.12.80.40', '91.189.91.38']
49.12.80.40 검사 시작
Fortinet                : malware site
Xcitium Verdict Cloud   : malware site
2 engines detected this file


91.189.91.38 검사 시작
BitDefender             : malware site
G-Data                  : malware site
2 engines detected this file
```

네트워크 검사

netstat 명령 수행 후
IP 추출하여 악성 검사 진행

```
lsof 탐지
[['minerd', '1', 'root', '4u', 'IPv4', '164536', '0t0', 'TCP',
```

열린 프로세스 검사

lsof 명령을 통해
컨테이너 내의 열린 프로세스에 대한 정보 획득

```
컨테이너가 실행될 때 다음 프로세스가 자동 실행됩니다. : /bin/minerd
Lionic                  : Riskware.Linux.BitCoinMiner.1!c
Elastic                 : Linux.Cryptominer.Camelot
```

자동 실행 파일 검사

docker history 명령을 통해 도커 이미지 레이어 추출 후
자동 실행 파일 확인 (ENTRYPOINT)
-> 해당 파일 컨테이너 외부로 복사하여 검사 진행

2-4. 웹 사이트

구조도

메인 페이지

▲ docker image명을 전달받는 페이지

결과 페이지

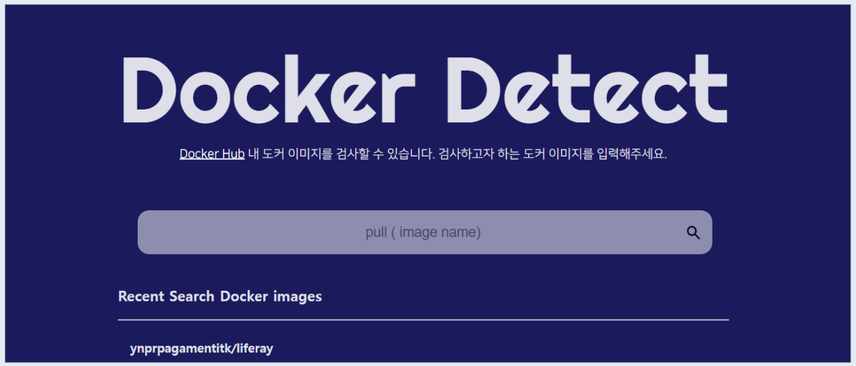
▲ 분석 결과를 사용자에게 보여주는 페이지

Docker web

- docker_img [분석 대기 리스트]
- static [정적분석 결과]
- dynamic [동적분석 결과]
- fs [결과 보고서]
- recent_search [최근 검색한 도커 이미지]

2-4. 웹 사이트

구조도



사용자가 도커 이미지명 입력

1) DB에 분석 결과 존재 시 해당 결과 출력

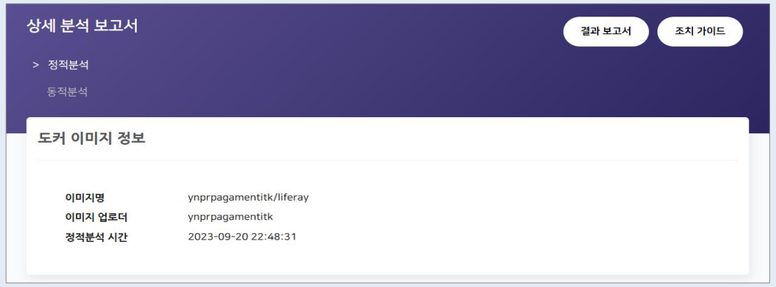
2) docker_img에 없을 시 이미지명 저장

3) docker_img에 존재 시 분석 진행

static

주기적 요청

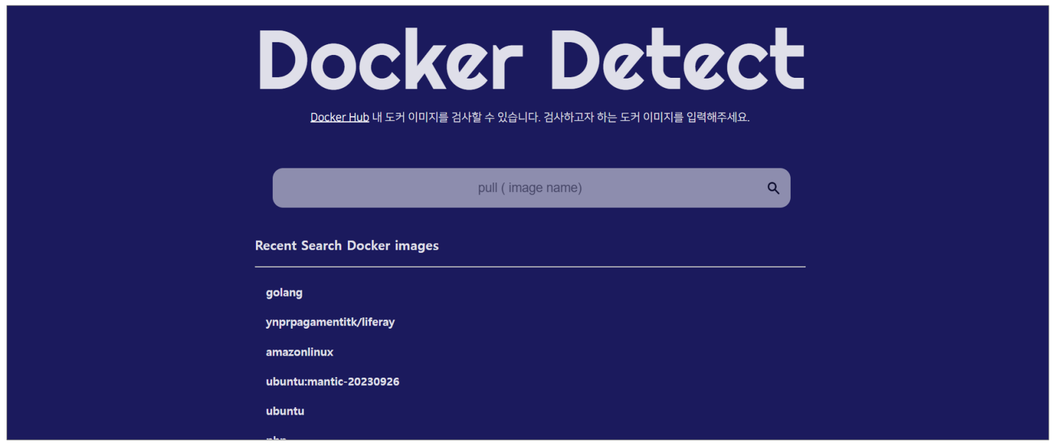
데이터 반환



2-4. 웹 사이트

메인 페이지

도커 이미지 검색창

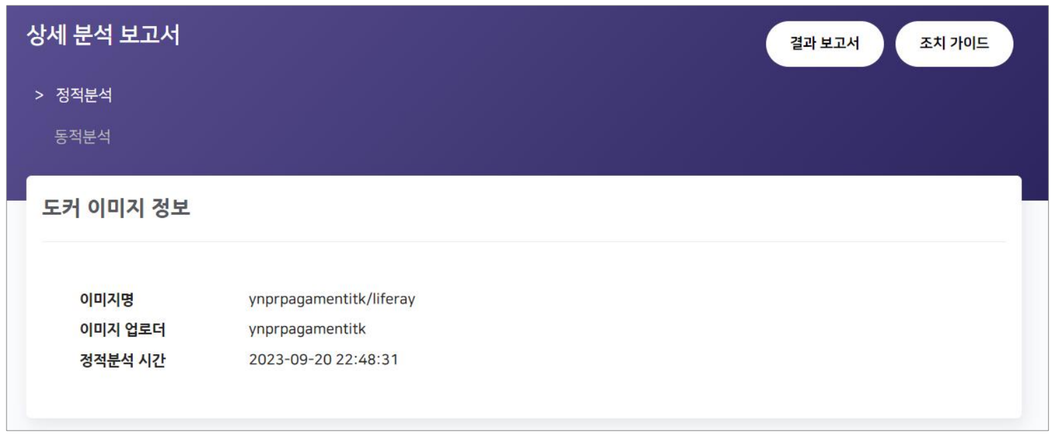


최근 검색한 도커 이미지 리스트

2-4. 웹 사이트

정적분석 결과 페이지

도커 이미지 정보



보안 취약점 (CVE) 검사

2-4. 웹 사이트

동적분석 결과 페이지

Root 실행 여부 검사

Root 실행 여부

* 컨테이너 실행 시 관리자 계정(Root)으로 자동 실행되는지 점검합니다.

본 도커 이미지의 기본 Shell은 Root 권한으로 실행됩니다.

위험도: 중

조치 방법:
- root 계정 사용이 필요한 경우를 내부적으로 정의하여 정책을 수립합니다.
- 주기적으로 root 계정 사용 여부를 점검하여 의도하지 않은 사용을 탐지할 필요가 있습니다.

네트워크 검사

네트워크

* 외부 아이피와의 통신을 탐지하고, 통신한 아이피의 악성 여부를 점검합니다.

91.189.91.81	**0 engines detected**
185.125.190.39	**5 engines detected**
CRDF	malicious site
CyRadar	malicious site
BitDefender	malware site
G-Data	malware site
Criminal IP	malicious site
91.189.91.83	**0 engines detected**

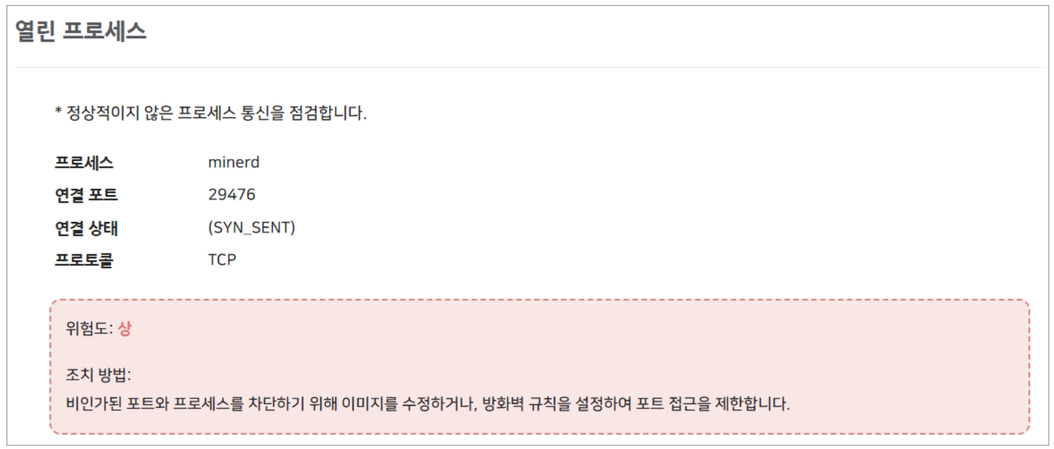
위험도: 상

조치 방법:
악성으로 식별된 아이피와의 통신을 차단하도록 방화벽 규칙을 설정하거나, 이미지를 수정하여 해당 통신을 제거합니다.

2-4. 웹 사이트

동적분석 결과 페이지

열린 프로세스 검사



컨테이너 내 자동 실행되는 파일 검사

2-5. 컨설팅

수행 절차

1 환경 분석
- 요구사항 정의
- 진단 범위 확정
- 컨설팅 목표 수립

2 위험 분석
- 위험도 산정
- 취약점 분석

3 보안 대책
- 대응 방안 제시
- 결과 보고서 작성

2-5. 컨설팅

결과 보고서 및 조치 가이드

결과 보고서

도커 이미지 취약성 결과 보고서

스캔 정보

Image name: ynprpagamentitk/liferay
Start time: 2023-09-20 22:48:31
Finish time: 2023-09-20 22:50:55
Elapsed: 143sec

수행된 항목 목록

구분	진단 항목	개수/결과
CVE 진단	CVE Critical	1
	CVE High	63
	CVE Medium	716
	CVE Low	412
	CVE Unknown	0
권한 설정	Root 계정	탐지
접근 통제	외부 아이피 통신	탐지
	TCP 통신 프로세스	탐지
실행 파일 탐지	자동 실행 파일	탐지

자동화 진행하여 분석 종료 시 보고서 자동 반환

체크리스트 (조치 가이드中)

1. 체크리스트 항목

도커 이미지 취약점 진단에 사용될 체크리스트는 국내외 기술 자료를 바탕으로 작성하였다.
가이드 내 영역은 크게 정적 분석, 동적 분석으로 구성하였으며, 정적 분석은 CVE 진단(5개 항목), 동적 분석은 권한 설정(1개 항목), 접근 통제(2개 항목), 리소스 관리(1개 항목)로 총 9개 항목으로 제작하였다.

구분	진단 코드	진단 항목	위험도
가. CVE 진단	DS 1-1	오래된 소프트웨어 구성	*N/A*
	DS 1-2	안전하지 않은 코딩	*N/A*
	DS 1-3	네트워크 보안	*N/A*
	DS 1-4	잘못 구성된 설정	*N/A*
	DS 1-5	약한 인증 및 엑세스 제어	*N/A*
나. 권한 설정	DD 1-1-1	Root 계정: 탐지	중
	DD 1-1-2	Root 계정: 미탐지	*N/A*
다. 접근 통제	DD 2-1-1	외부 아이피 통신: 악성 아이피로 분류	상
	DD 2-1-2	외부 아이피 통신: 악성 아이피로 미분류	중
	DD 2-1-3	외부 아이피 통신: 미탐지	하
	DD 2-2-1	TCP 통신 프로세스: 탐지	상
	DD 2-2-2	TCP 통신 프로세스: 미탐지	하
라. 실행 파일 탐지	DD 3-1-1	자동 실행 파일: 악성코드로 분류	상
	DD 3-1-2	자동 실행 파일: 악성코드로 미분류	중
	DD 3-1-3	자동 실행 파일: 미탐지	하

[표 2] 도커 이미지 취약점 분석·평가 항목

조치 가이드

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
	# netstat -an
	`# netstat -an`
	`Active Internet connections (servers and established)`
	`Proto Recv-Q Send-Q Local Address Foreign Address State`
	`tcp 0 1 172.17.0.2:49120 49.12.80.39:45560 SYN_SENT`
	`Active UNIX domain sockets (servers and established)`
	`Proto RefCnt Flags Type State I-Node Path`
	■ 검출된 외부 아이피에 대해 VirusTotal를 이용하여 진단 후, 악성 아이피로 확인됨		

조치 방법			
조치 방법	■ 악성으로 식별된 아이피와의 통신을 차단하도록 방화벽 규칙을 설정하거나, 이미지를 수정하여 해당 통신을 제거함		

[표 11] 세부 항목 설정

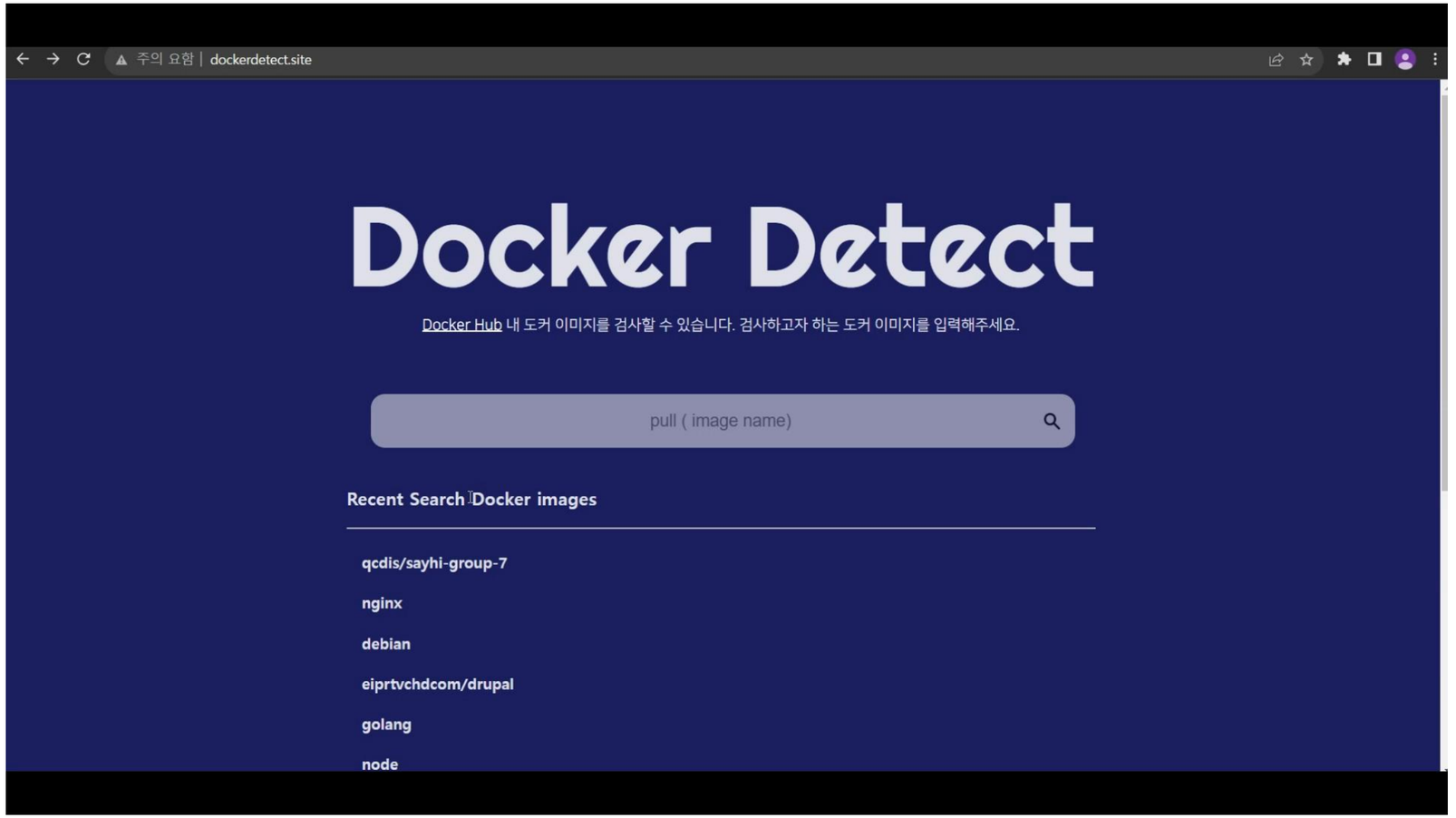
03

프로젝트 결과

3-1. 시연 영상

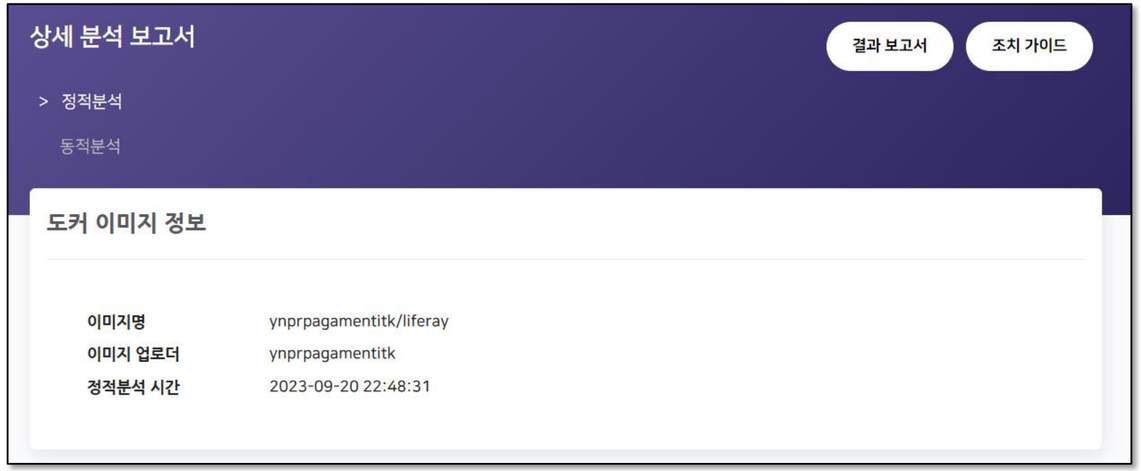
3-2. 결론 및 기대효과

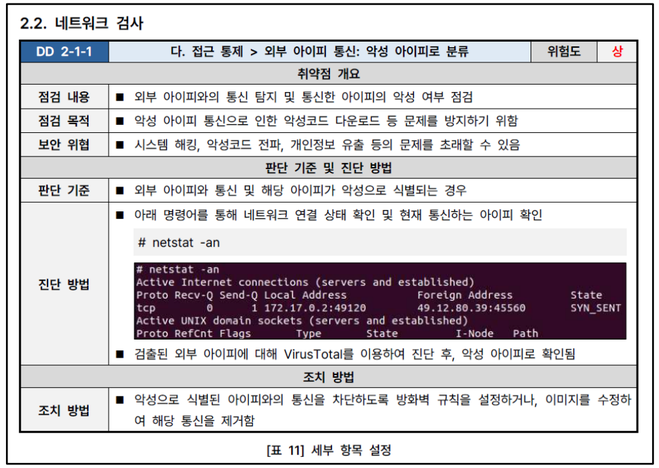
3-1. 시연 영상



시연 영상 주소: https://youtu.be/97UO16rSicY | 웹 서비스 주소: http://dockerdetect.site

3-2. 결론 및 기대효과





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 # netstat -an ■ 검출된 외부 아이피에 대해 VirusTotal를 이용하여 진단 후, 악성 아이피로 확인됨		
조치 방법			
조치 방법	■ 악성으로 식별된 아이피와의 통신을 차단하도록 방화벽 규칙을 설정하거나, 이미지를 수정하여 해당 통신을 제거함		

```
# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      1 172.17.0.2:49120        49.12.80.39:45560       SYN_SENT
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
```

[표 11] 세부 항목 설정

도커 이미지 분석 서비스 개발 및 조치 가이드 제작

1. 웹을 통해 분석 서비스를 제공함으로써 분석 용이성 증대
2. 샌드박스를 활용한 도커 이미지 동적분석 방안 연구
3. 조치 가이드를 통해 사용자에게 발생할 수 있는 2차 피해 예방

감사합니다

Team. 야자나무

유재겸, 서민재, 이다영, 이유경, 김우종, 남서현, 장혜선