팀 프로젝트 발표

SEMI-PROJECT

서비스 포트 스캐너 구현

K-Digital Training

고용노동부 KOREATECH 직업능력심사평가원

구름 딥다이브 정보보호 11회차
김지은 | 이우진 | 이순우 | 조수민

목차

01 프로젝트 개요

프로젝트 주제

내부망 내 자산에 대해 **포트 스캔** 수행 .

예상 외 포트/서비스의 오픈 여부, 위험한 서비스, 문서화되지 않은 자산 등을 자동 식별

보안 관리자 입장에서의 위험도 **분석 정보를 제공**하는 웹 사이트 개발

“SecSights” = “Security + Insights”

01 프로젝트 개요

프로젝트 목표

이 프로젝트는 **기업 내부 자산의 IP와 열린 포트를 등록**하면,
각 포트에 대한 **위험도를 자동 분석**하고 **시각화**된 **보안 인사이트**를 제공합니다.

관리자는 전체 자산의 보안 상태를 한눈에 파악할 수 있고,
자산별 위험 정보를 직접 관리하거나 CSV로 내보내기도 가능합니다.
단순한 포트 스캔을 넘어, 보안 리스크 관리와 의사결정을 지원하는 인텔리전스 플랫폼을 목표로 합니다.

01 프로젝트 개요

프로젝트 개발 환경

Front-end

FastAPI

Back-end

python™

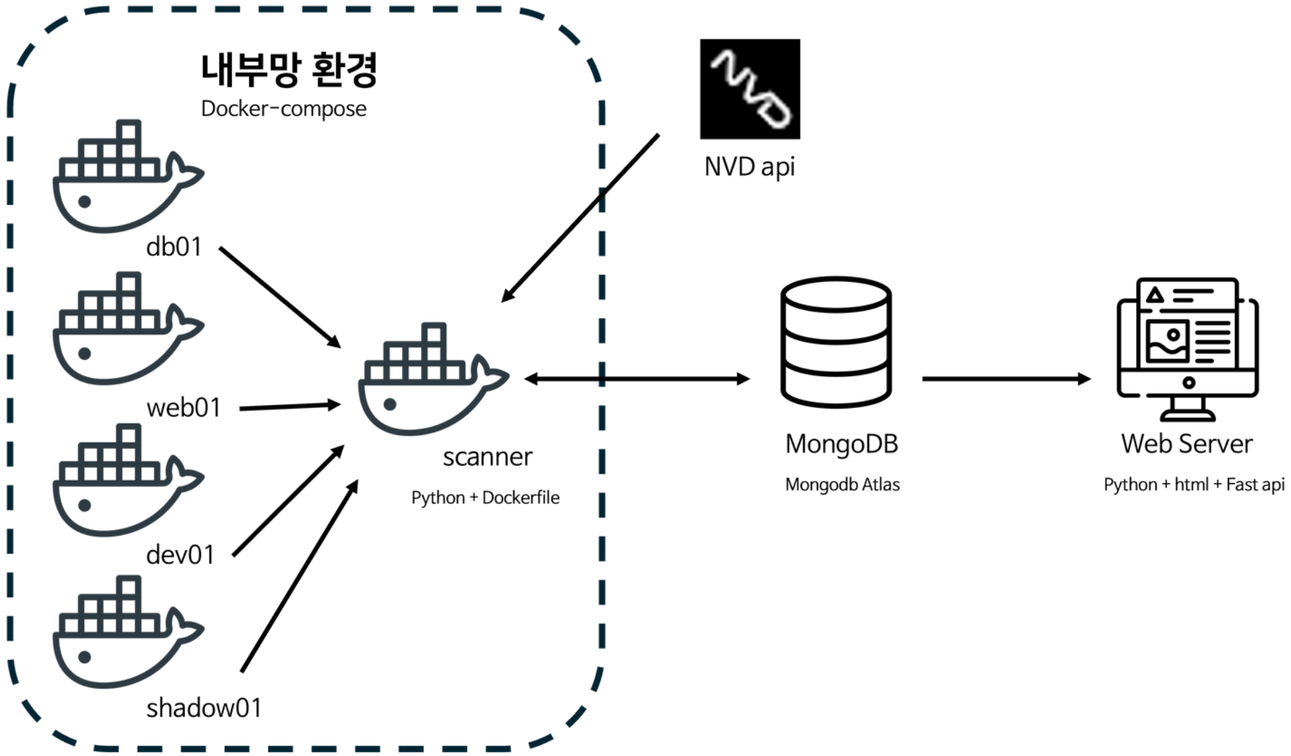
mongoDB

Scanner

NVD

01 프로젝트 개요

프로젝트 구조



01 프로젝트 개요

프로젝트 기능 명세서

기능 ID	화면 ID	Category	Depth1	Depth2	Depth3	중요도	지원 환경	기능 설명	비고
V1-001	Overview	위험 자산	자산 리스트	정렬 기능	날짜/점수 기준	중	웹	최신순, 오래된 순, 위험도 점수순으로 정렬 가능	
V1-002			상세 보기	팝업창	상세 취약점 정보	상	웹	[상세보기]클릭 시 해당 IP의 취약점 상세 정보 표시	
V1-003	Shadow IT	탐지 목록	미등록 포트 탐지	등록 여부 확인	조치 필요 분류	상	웹	등록되지 않은 포트를 탐지하여 표시	
V1-004	Insights	데이터 시각화	Shadow IT 기기 변화	선 그래프	Shadow IT 기기의 변화	중	웹	최근 3일간의 분석한 Shadow IT 변화 추이 시각화	
V1-005			평균 위험도 추이	선 그래프	기간별 평균 위험도	중	웹	최근 3일간의 평균 위험도 변화 추이 시각화	
V1-006			포트 개수 시각화	막대 그래프	열려있는 포트 개수 시각화	중	웹	자산별 열려있는 포트 개수 시각화	최근 분석일자 기준(1일)
V1-007			취약점 발생	도넛 그래프	취약점 발생 서비스	중	웹	취약점이 발생한 서비스를 시각화(http 3개, Telnet 5개 등)	
V1-008			조치 필요 자산	텍스트	조치 필요 자산(상위 3개)	중	웹	위험 점수가 높은 자산을 조사해 조치가 필요한 자산으로 분류 후 텍스트로 표현	
V1-009	CSV	csv 내보내기	출력 날짜 선택	날짜 선택	시작일/ 종료일 선택	중	웹	달력 UI를 이용해 시작일과 종료일 지정 가능	
V1-010			csv 내보내기	csv 내보내기 버튼		중	웹	버튼 클릭 시 선택한 기간 DB 데이터 csv 파일 다운로드	
V1-011			csv 미리보기	csv 미리보기		중	웹	선택된 날짜 구간에 해당하는 DB 데이터를 화면에 미리 출력 (DB 조회 후 표시)	
V1-012	All Pages	공통기능	검색/필터링	날짜 필터링		하	웹	달력 UI를 통해 날짜를 선택하고, 해당 일자의 데이터만 조회 가능	
V1-013				IP 검색		하	웹	사용자가 IP 주소를 입력하거나 선택하여 해당 자산 정보 및 관련 데이터를 조회	
V1-014	Scan	스캔	스캔 기능	자산에 대한 스캔	스캔 옵션 선택	중	웹	사용자가 선택한 스캔 옵션에 따라서 스캔 수행	

02 팀 구성 및 역할

팀장

김지은

프로젝트 기획 및 총괄
발표 준비
내부망 및 db 구성
데이터 셋업
시나리오 구상

부팀장

이우진

프로젝트 부총괄
프론트엔드
웹 페이지 구현
‘인사이트‘ 세팅
cve 대응법 데이터 세팅
로고 제작

조수민

Scanner 총괄
스캐너 기능 개발
db 연동 및 데이터 삽입
NVD api 연계
위험도 로직 설계
cve 리스트업

이순우

프론트엔드 총괄
전체 웹페이지 구현
DB 연동 및 데이터 가공
기능 명세 작성
FE 기술 스택 선택
웹 서버 구동

03 시장 조사 - Nmap과의 차이점을 중점으로

기능 항목	nmap	우리 프로젝트
포트 스캔	O	O
서비스/버전 식별	O	O
CVE 위험도 자동 분석	X	O
위험 점수 산정 (예: 85/100)	X	O
시각화(차트/그래프) 제공	X	O
웹 기반 UI 제공	X	O
자산 관리 기능 (IP/포트 등록/수정)	X	O
CSV 자동 리포트 출력	X	O
비기술자(보안 관리자, 임원) 대상	X	O
실시간 인사이트 제공	X	O

04 프로젝트 진행 과정(회의)

Notion 평일 15시 회의, 개별 진행도 공유

Meeting

날짜	Name	참석자	파일과 미디어
2025년 3월 29일	1일차 보고	조수민 이우진 이순우 김지은	
2025년 3월 31일	1차 중간점검	조수민 이우진 이순우	
2025년 3월 31일	2일차 보고	조수민 이우진 이순우 김지은	
2025년 4월 1일	3일차 보고	조수민 이우진 이순우 김지은	
2025년 4월 2일	4일차 보고	조수민 이우진 이순우 김지은	
2025년 4월 3일	5일차 보고	조수민 이우진 이순우	
2025년 4월 4일	6일차 보고	조수민 이우진 이순우 김지은	
2025년 4월 7일	2차 중간점검	조수민 이우진 이순우	
2025년 4월 7일	7일차 보고	조수민 이우진 이순우 김지은	
2025년 4월 8일	8일차 보고	조수민 이우진 이순우 김지은	
2025년 4월 9일	9일차 보고	조수민 이우진 이순우	
2025년 4월 10일	10일차 보고	조수민 이우진 이순우 김지은	

04 프로젝트 진행 과정

1

주제 및 목표 설정

프로젝트 기획,
프로젝트 기간별 계획

2

사전 조사

기술 스택 및
환경 설정, Nmap 실행

3

코드 개발

웹 페이지 및
Nmap 스캐너 코드 개발

4

테스트

코드 통합 및 실행 테스트

04 프로젝트 진행 과정

2025년 3~4월	28	31	1	2	3	4	7	8	9	10	11
프로젝트 주제 선정 및 기획											
개발 환경 설정, 인프라 구축											
개발											
테스트 및 코드 병합											
발표 자료 제작											
최종 발표											

05 프로젝트 수행 결과

95%

리포트

자산 분석 결과를
기반으로 보안 리포트(웹 페이지) 완성

90%

자동화

분석/보고 시간 단축
(스크립트 및 시각화 자동화)
실시간 데이터 연동을 위한
web socket 구현 X

99%

목표 달성률

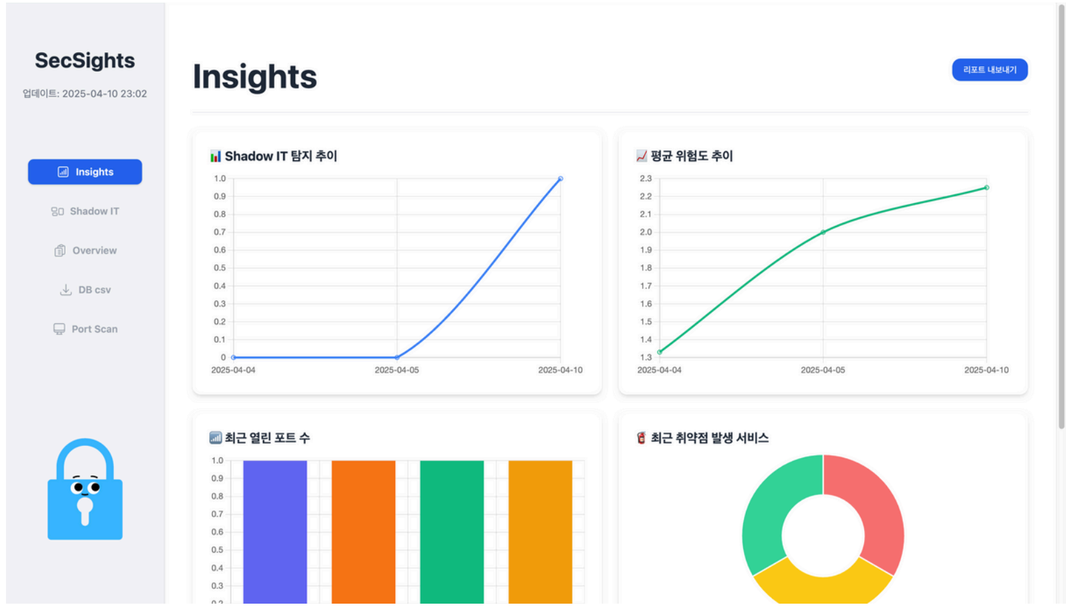
초기 계획 대비 모두 구현

05 프로젝트 수행 결과

웹 페이지 구현 - Insights

조직의 보안 자산 데이터를 정리해 5가지 주요 지표를 시각화한 분석용 리포트 페이지입니다.

핵심 기능	기능 설명
SHADOW IT 발견 추이 (막대그래프)	날짜별 Shadow IT 자산 개수 변화
평균 위험도 추이 (꺾은선 그래프)	리포트 기준 평균 위험도 점수 변화
포트 개수 시각화 (막대그래프)	자산별 열린 포트 수 비교
취약점 발생 (도넛 그래프)	서비스별 취약점 비율
조치 필요 자산 TOP 3 (표)	위험 점수가 가장 높은 상위 3개 자산을 표시

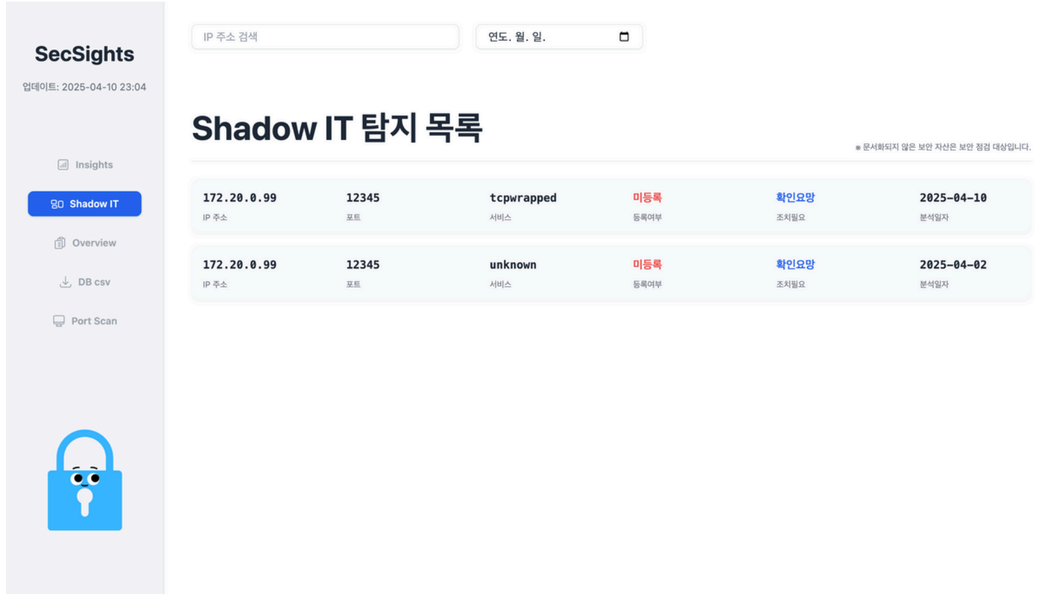


05 프로젝트 수행 결과

웹 페이지 구현 - Shadow IT

등록되지 않은 비인가 자산을 탐지하고, 위험 수준과 분석 일자 기준으로 선별할 수 있도록 구성된 탐지 전용 페이지입니다.

핵심 기능	기능 설명
날짜 필터	자산의 분석일자(스캔일자)를 기준으로 필터링
자산 카드 렌더링	Shadow IT 자산들을 카드 형태로 시각적으로 표시
위험도 판단	포트별 CVE 개수를 기준으로 조사필요/확인요망 상태 판단

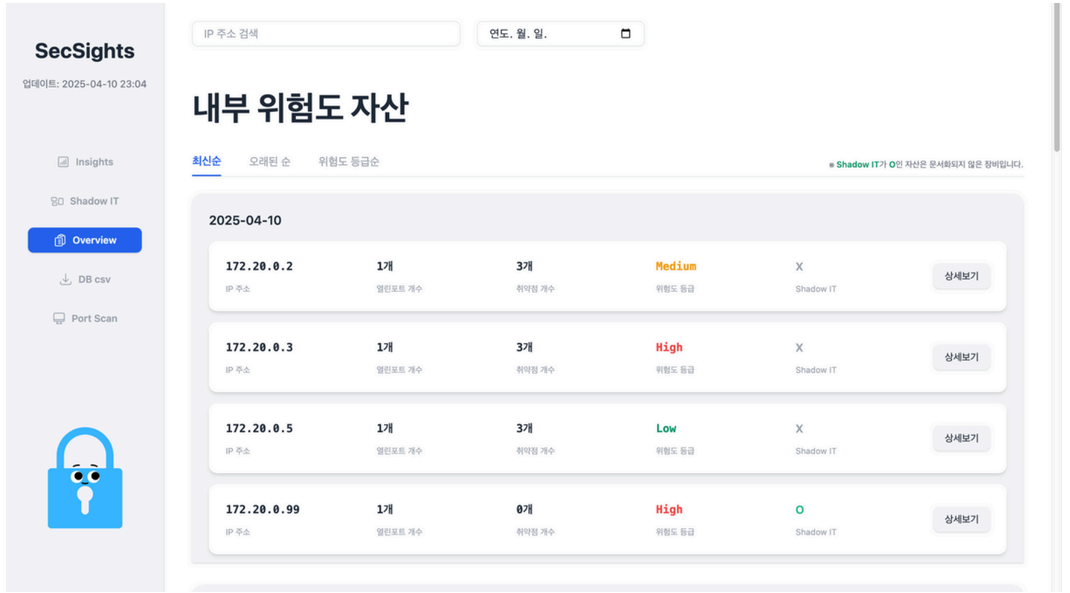


05 프로젝트 수행 결과

웹 페이지 구현 - Overview

조직 내 보안 자산을 날짜별로 정리하고, 위험도·포트·취약점 정보를 카드 형태로 제공하는 요약형 대시보드입니다.

핵심 기능	기능 설명
정렬 탭 (최신/오래된/위험도)	자산 그룹 또는 자산 목록을 정렬
상세보기 모달	자산 상세정보 표시 (포트, 취약점, Shadow IT 여부 등)

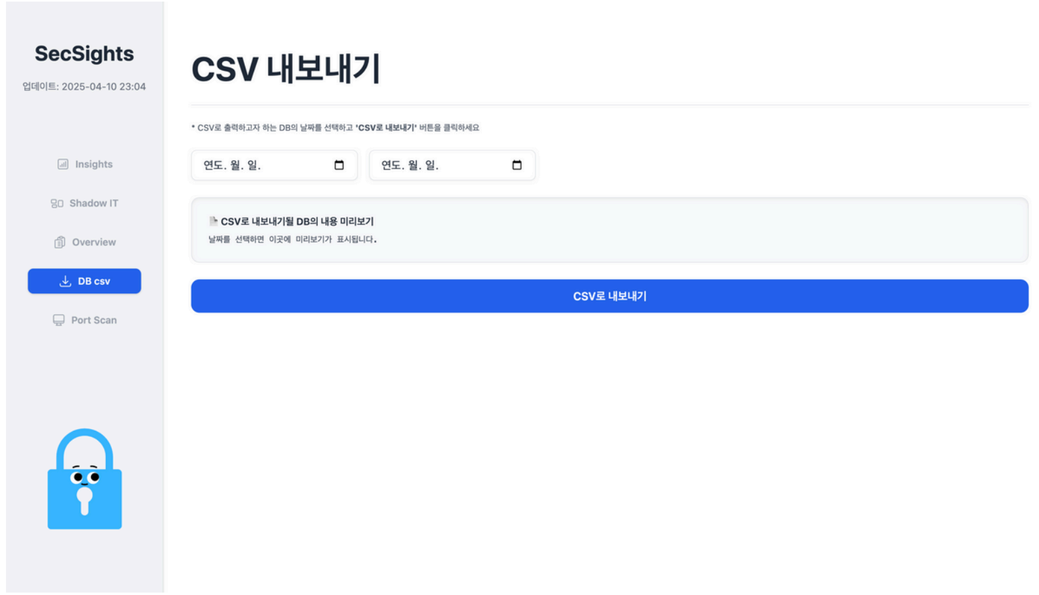


05 프로젝트 수행 결과

웹 페이지 구현 - CSV

선택한 날짜 구간에 해당하는 DB 데이터를 CSV로 내보내는 기능을 제공합니다.

핵심 기능	기능 설명
날짜 선택	가져오고 싶은 데이터의 시작~끝 날짜를 선택
CSV 내보내기	전체 자산 리스트를 CSV 파일로 다운로드
CSV 미리 보기	CSV로 내보내기 될 DB의 데이터를 미리 보여줌

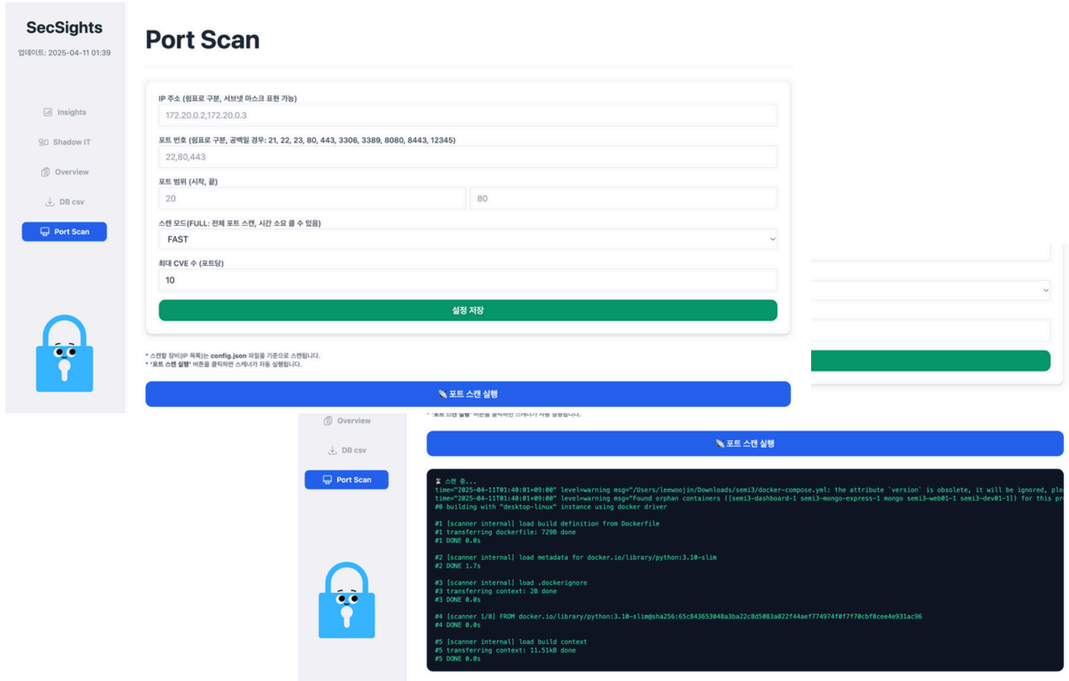


05 프로젝트 수행 결과

웹 페이지 구현 - Port Scan

사용자에게 포트를 스캔하는 기능을 제공합니다.

핵심 기능	기능 설명
포트 스캔하기	포트 스캔하기 버튼 클릭 시 포트 스캔
스캔 결과 미리보기	스캔한 결과를 출력함



05 프로젝트 수행 결과

Scanner

```python
# === 위험도 계산 ===
def calculate_risk(port, cves, is_shadow):
    score = 0
    if port in [21, 23, 12345, 31337]:
        score += 5
    if cves:
        score += len(cves) * 2
        for cve in cves:
            if cve.get("cvss", 0) >= 7.0:
                score += 3
    if is_shadow:
        score += 15

    return "high" if score >= 15 else "medium" if score >= 7 else "low"
```

- PORT = 21, 23, 12345, 31337 → +5점
- cve 개수 * +2 (만약 cvss 〉= 7.0일 시 +3점)
- is_shadow = true 일 경우-〉 +15점

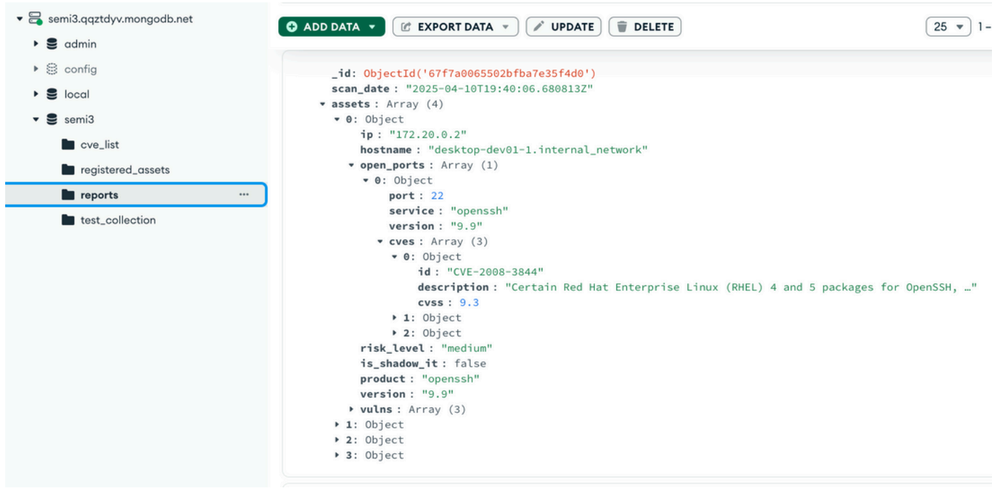
15점 이상 → HIGH
7점 이상 → MEDIUM
7점 미만 → LOW

05 프로젝트 수행 결과

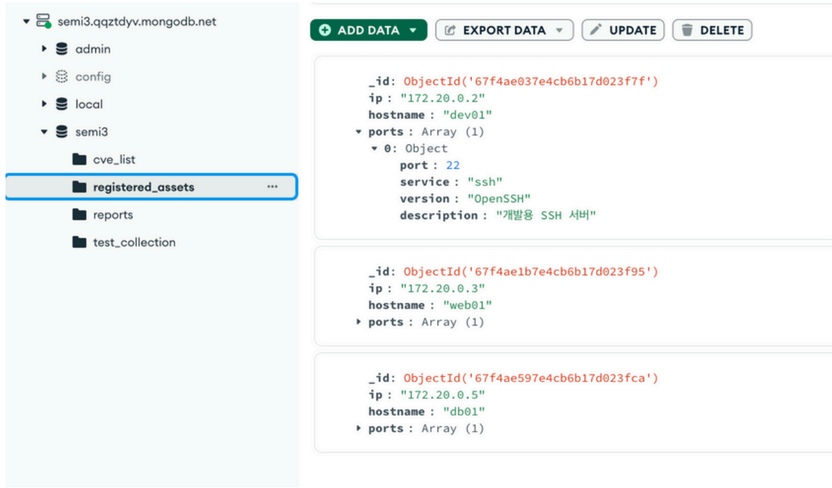
DB

보안 자산의 스캔 결과와 등록 정보를 저장·조회하여 대시보드와 리포트 기능의 핵심 데이터를 제공합니다.

reports

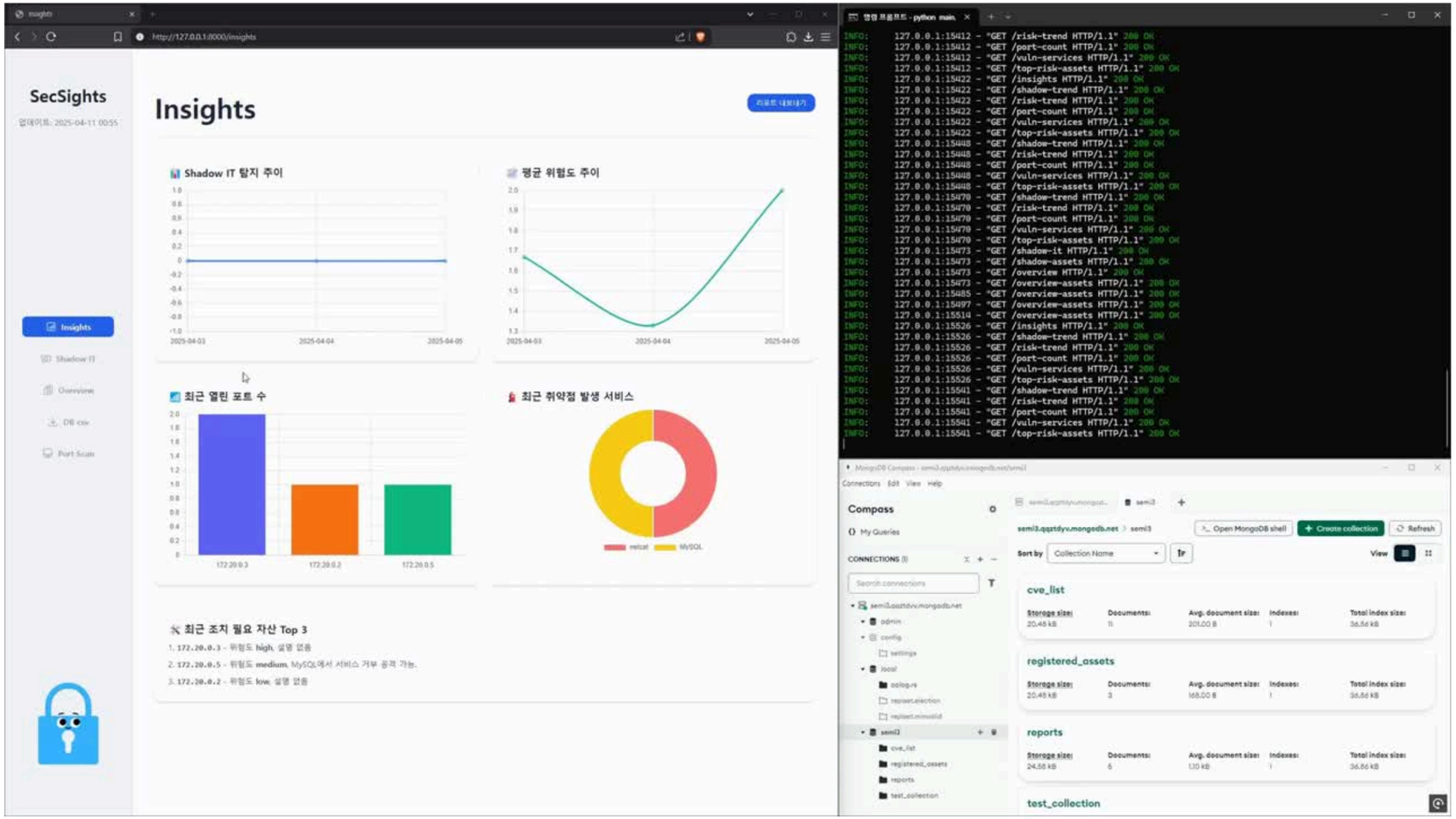


registered_assets



05 프로젝트 수행 결과

- 시연 동영상



06 시행착오 및 해결방안

시행착오

- 시각화 데이터 구성
- 스캐너 실행 위치
- 적절한 CSV 정보량

해결방안

- 회의 + 기능 명세를 통한 확정
- 실행 환경의 통일성 확보
- 사용성과 분석 편의성을 고려

07 향후 개선 방향

정보 처리 기능 개선

신뢰 가능한 API 추가 → 최신 및 양질의 정보 획득 가능
CVE 처리 로직 개선 → 필터링 등 필요한 정보만 골라 사용

관리자 계정

관리자 계정을 도입하여 자산을 직접 관리할 수 있는 기능을 구현
웹 기능 구현을 통한 웹 상에서의 식별 자산 관리

개인 RISK SOCRE

리스크 결과를 사용자에게 맞추어, 개별 위험도 점수 계산 기능 제공

포트 스캔 기능 개선

다양한 포트 스캔 옵션 제공 + 스케줄러 활용 → 정기 검사 개념

08 프로젝트 후기

김지은(팀장)

기획 원툴로 팀원분들에게
고생만 끼쳐드린 것이 아닌지...
모의 해킹이라는 주제와의 연관점을
찾기 위해 의심하고 고민했습니다.
고민의 결과가 맞았는지는 모르겠습니다만,
아무튼 팀원 잘 만나서 다행입니다.

이우진(부팀장)

아랫집 분이 웹페이지 구현을 깔끔하게 잘
해주셔서, 덕분에 저는 CVE 기반 취약점
분석과 데이터 작업 등 저는 다른 파트에
도 숟가락을 얹을 수 있었습니다.

조수민(팀원)

스캐너를 개발하면서 네트워크에
대한 지식도 공부하게 되었고,
취약점 관련 API를 만져볼 수 있는
경험이 좋았습니다.

이순우(팀원)

웹 사이트 개발을 한지 오래되어
어려움이 있었지만 여러 기술을
새로 배우는 계기가 된 것 같아
재미있었습니다.

09 질문과 답변

감사합니다