

해상 물류 사이버 보안 및 모니터링 플랫폼

2024 . 10. 12

Contents

01 서론

1. 프로젝트 추진 배경
2. 프로젝트 개발 배경
3. 작품 소개

02 프로젝트 구조 및 기능 소개

- | | |
|------------------|--------------------|
| 4. 프로젝트 소개 | 7. 주요 적용 기술과 개발 환경 |
| 5. 인벤토리 시스템 프로세스 | 8. 기술적 차별화 |
| 6. SW 구성도 | |

04 프로젝트 가치와 작품의 기대 효과

9. 프로젝트의 차별성
10. 프로젝트의 특징 및 장점
11. 프로젝트의 가치와 노력
12. 작품의 활용 분야와 기대 효과
13. 시연

해운업계에서 사이버 보안 공격이 잇달아 발생·증가하고 있다.

그러나 해양 보안은 **IT시스템**과 **운영기술 시스템**이 융합된 특수한 환경 때문에,
기존 보안 관리 프로세스와 다른 새로운 형태의 보안 관리 모델이 요구된다.

조선 1위, 선박 사이버 보안 기술 큰 구멍

선박 스마트·디지털화, 자체 보안 솔루션 개발에 힘 써야

디에스랩컴퍼니, 해외 조선·해양 사이버 사고사례 분석

기사입력 2024.06.10 06:49 | 최종수정 2024.06.21 05

조선소, 선주사, 선박 기자재 기업의 사이버보안 주의 필요

해사 사이버 보안만의 특징이 있다. 선사 사이버 보안업계 관계자는 “통상 정보기술 (IT, Information Technology) 시스템 보안에 집중하는 타 산업과 달리 선박은 IT 시스템과 운영기술(OT, Operational Technology) 시스템이 융합된 환경인 점이 큰 차이다”라고 설명했다. IT 시스템은 컴퓨터, 소프트웨어, 데이터베이스, 통신, 서버 등을 관리하고 처리하는 것이라면 OT 시스템은 하드웨어 및 소프트웨어를 사용해 산업용 장비를 제어하는 방식이다. 최근 인도 선박의 경우 엔진, 발전기 등 주요 장비들이 사물인터넷(IoT)과 접목돼 OT 시스템 영역으로 분류된다.

선박 ICT 공급망 사이버 공격 위협 증가

● 김민권 기자 | ○ 승인 2023.01.16 16:39

점점 커지는 선박 해킹 위협... 공격 표면에 노출된 1,600개 이상 장치 발견

해사업계 주요 사이버 공격 사례

| 시기 | 대상 | 시스템 | 공격유형 | 영향 |
|------|--------------------------|------------|-----------|------------------------|
| 2017 | 컨테이너선 | 선박 항해 시스템 | 멀웨어 | 10시간 동안 통제권 상실 |
| 2017 | 마스크 | 터미널 IT 시스템 | 랜섬웨어 | 3주간 시스템 마비, 3,000억 손실 |
| 2018 | 해운선사 | 회사 이메일 | 스피어피싱 | 연간 100억 규모 손실 추정 |
| 2018 | COSCO 쉬펑 | IT 시스템 | 랜섬웨어 | 화물 운송 지연 |
| 2018 | 바르셀로나 항만 | 항만 IT 시스템 | 랜섬웨어 | 시스템 폐쇄 및 포렌식 의뢰 |
| 2018 | 샌디에고 항만 | 항만 IT 시스템 | 랜섬웨어 | 시스템 폐쇄 및 포렌식 의뢰 |
| 2019 | 자동차 운반선 | 선박 IT 시스템 | 랜섬웨어 | 대상 시스템 포맷 |
| 2019 | 유조선 | 선박 항해 시스템 | - | 이란혁명수비대에 이포 |
| 2019 | 영국 해양업체 | 회사 IT 시스템 | 랜섬웨어 | 주가 하락, 포렌식 의뢰 |
| 2020 | CMA CGM | 회사 IT 시스템 | 랜섬웨어 | 2주간 네트워크 시스템 다운 |
| 2020 | Hurghada Line | 회사 IT 시스템 | 랜섬웨어 | 여객번호 등 개인정보 유출 |
| 2021 | 트랜스넷 SOC | 항만 IT 시스템 | 랜섬웨어 | 모든 항만 터미널 운영 중단 |
| 2022 | Hapag-Lloyd | 회사 IT 시스템 | 스피어피싱 | 이메일 계정 통해 이메일 재전송 |
| 2022 | Port of London Authority | 회사 IT 시스템 | 분산서비스거부공격 | 온라인 인프라가 중단돼 오프라인으로 변환 |
| 2022 | Sembcorp Marine | 회사 IT 시스템 | - | 근로자 운행정보에 접근 |

<출처: '해상 사이버 보안 동향 및 선박 사이버 안전체계 구축 방안'(한국선급, 기술정책제어연구회 2020), 해사 사이버 보안 관리실무(한국선급 미카데미, 2023)>

해운업계 주요 사이버 공격 사례

따라서, 해양 산업의 특수성을 고려한 해양물류 보안 서비스의 필요성을 알 수 있었다.

해양 산업에서 고려해야 할 요소는?

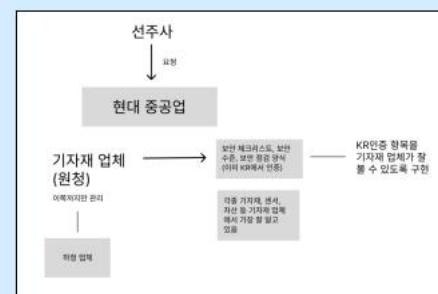
As Is



- 1 자산 관리는 누가 주체인가?
- 2 해양물류에는 어떤 자산이 있는가?
- 3 어떤 방식으로 자산을 등록하거나 보고하는가?
- 4 해양물류 산업에 어떤 취약점이 치명적인가?

To Be

- 1 팀별 조사
- 2 멘토님과의 회의 진행
- 3 실제 해양물류 분야의 프로세스를 알아보기 위해 선박 운행 회사의 현업자 분과 인터뷰 진행



복잡한 이해관계자 구조로 인한 체계적 관리의 어려움, ISM Code에 의한 자산 관리 의무화, 해양물류 특성 반영한 전문적 자산관리 시스템

개발 필요성 확인

프로젝트 개발 배경



해양 물류 디지털화로 인한
사이버 보안 위협 급증



해양 산업의
특수성을 고려하는
보안 솔루션 필요



해양 물류 비즈니스의
안정성과 신뢰성
향상 필요



해양물류 특화 보안 플랫폼 SEACURITY 구상

작품 소개

기획 의도

해상 물류 분야의
사이버 보안 강화

IoT 자산 관리 및
취약점 분석 자동화

인공지능 기반
보안 위협 대응 체계 구축

기존 보안 솔루션의
한계 극복 및 신규 보안 위협에
선제적 대응



정의

- 해상 물류 사이버보안을
종합적으로 관리하고
모니터링하는 **지능형 플랫폼**

- IT, OT, IoT를 아우르는 통
합 자산 관리 및 **보안 취약점**
분석 솔루션을 제공

- 해양 도메인 전문성을 갖춘
차세대 보안 관리 도구

프로젝트 구조 및 기능 소개

프로젝트 정의



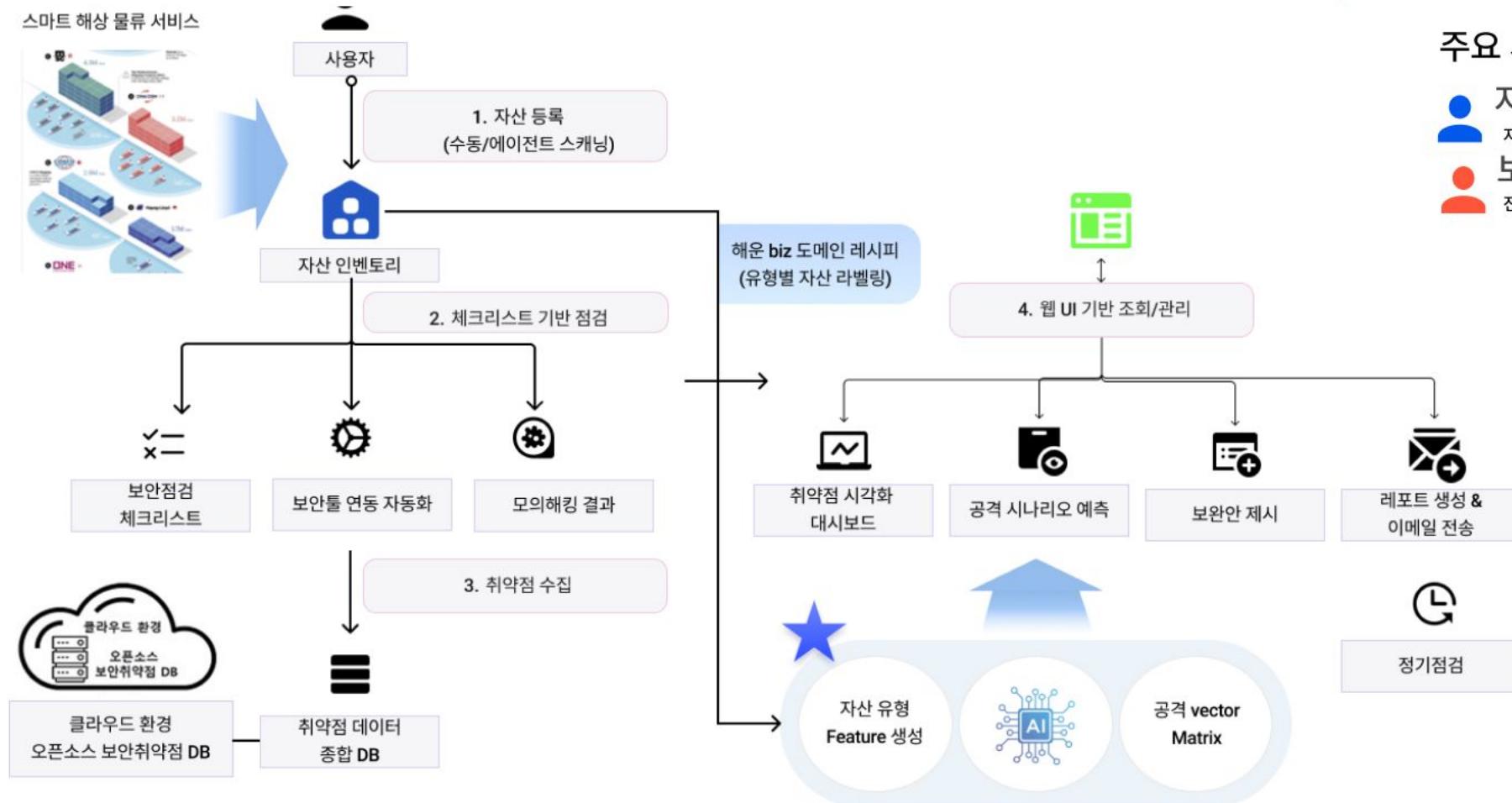
“해양 물류 특화 자산을 등록하고, 맞춤형 보안 체크리스트를 통해 보안 계획을 수립하며, 역할 기반 접근 제어(RBAC)로 효율적인 보안 관리 및 승인 프로세스를 제공하는 통합 자산관리 플랫폼”

해양 물류 특화 자산
등록 및 관리

맞춤형 보안 체크리스트

승인 프로세스 관리

인벤토리 시스템 프로세스



자산 등록 → 보안 체크리스트 → 계획 수립 → 승인 프로세스

사용자 화면

```
[ubuntu:~]$ ./sendInfo.sh
{
  "os_info": "Ubuntu 20.04.6 LTS",
  "hostname": "ubuntu",
  "kernel_version": "5.15.0-117-generic",
  "uptime": "up 2 weeks, 2 days, 7 hours, 12 minutes",
  "cpu_info": "Intel(R) Core(TM) i9-10850K CPU @ 3.60GHz",
  "cpu_usage": "77.3%",
  "mem_total": "7.7G",
  "mem_usage": "25.76GB",
  "disk_usage": "92%",
  "disk_info": "99G / 34G",
  "package_count": "1534",
  "last_boot": "2024-08-07 04:13",
  "active_users": "1",
  "last_login": "ultimoFri Aug 9 21:22
2024Med Aug 7 04:34
2024Med Jul 31 20:01
11
vtmp:Thu:Jul 4 01:42:41 2024",
  "network_info": "lo:127.0.0.1/8
ens3:192.168.149.132/24
```

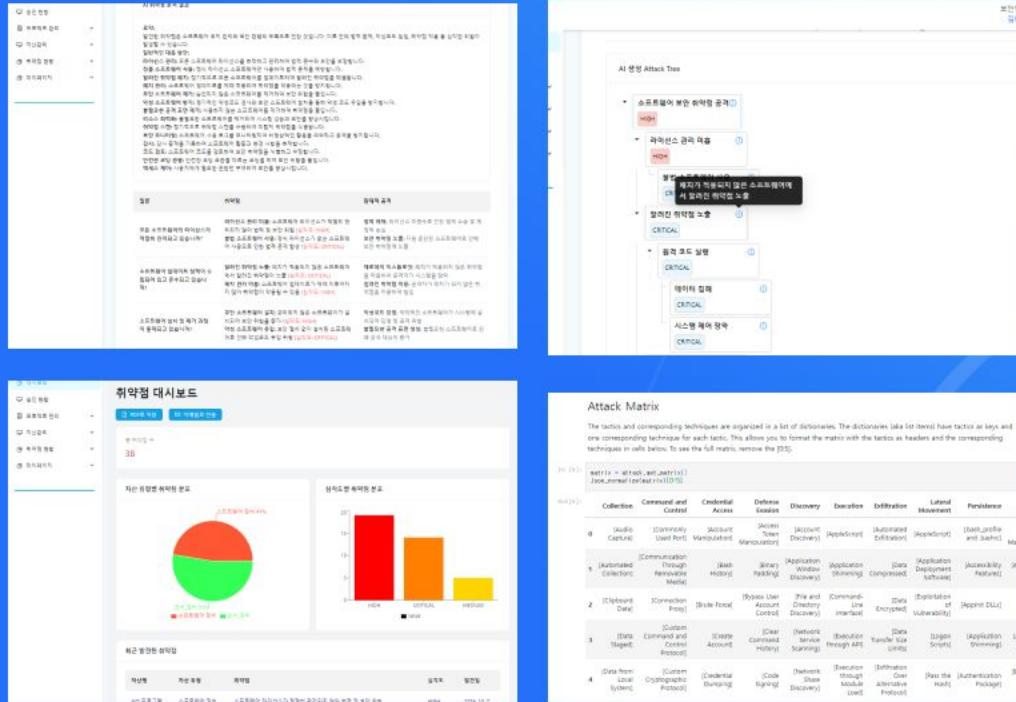


해양 물류 특화 자산 등록 및 관리

- IoT 센서 자동 등록 기능
 - 프로젝트별 자산 분류
 - 자산 유형별 맞춤 정보 입력
 - 자산 현황 대시보드 제공

맞춤형 보안 체크리스트

사용자 화면



- MITRE ATT&CK, CVE 기반 체크리스트
- 해양 물류 도메인 특화 항목 포함
- 자산 유형별 최적화된 체크리스트 제공
- 사용자 친화적 인터페이스로 쉬운 작성
- LLM 활용 실시간 취약점 분석
- Attack Tree를 활용한 공격 시나리오 시각화
- 대시보드를 통한 취약점 시각화

승인 프로세스 관리

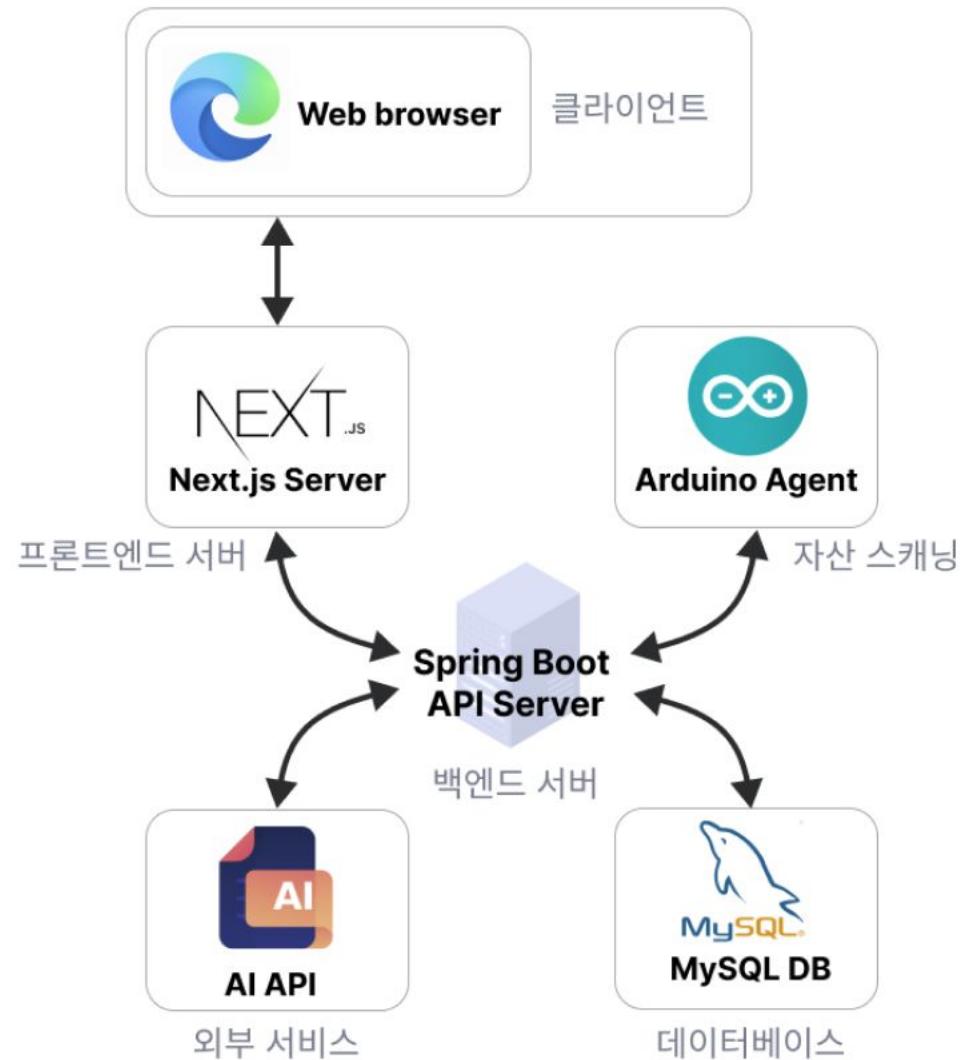
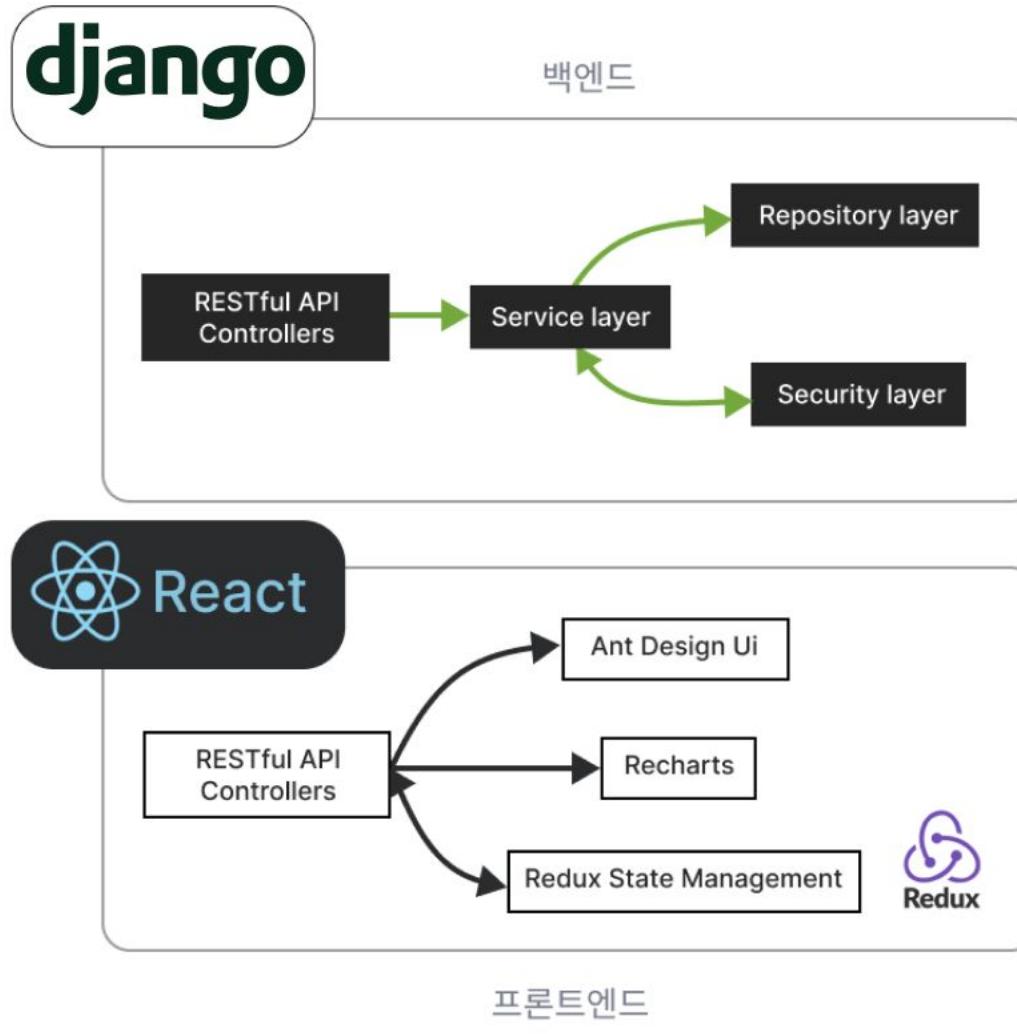
사용자 화면

The figure displays four screenshots of the Seacurity application's user interface:

- Top Left:** Asset Management (자산 관리) screen showing a list of assets with columns for Asset ID, Name, Type, Status, and Action.
- Top Right:** Approval Process Management (승인 프로세스 관리) screen showing a form for creating an asset configuration and assignment task.
- Bottom Left:** Audit Log Analysis (회약점 대시보드) screen showing a pie chart of audit types and a bar chart of audit counts.
- Bottom Right:** Risk Analysis (위험 분석) screen showing a detailed table of risk assessments across various categories.

- 자산등록자의 보안 계획 수립
- 보안담당자의 검토 및 승인 기능
- 승인 상태 실시간 모니터링
- 이력 관리 및 감사 추적 기능
- 자동 보고서 생성 및 이메일 발송
- 정기적인 보안 점검 알림 기능

SW 구성도



주요 적용 기술과 개발 환경



1 웹 아키텍쳐 - 마이크로서비스 아키텍쳐



- 백엔드 : Django, RESTful API
- 프론트엔드 : React, Next.js
- 도커 컨테이너 기반 배포/AWS 클라우드 환경/MySQL 데이터베이스 연동

2 IoT 테스트베드



- 라즈베리파이, 쉘코드 활용
- 실제 IoT 환경 모의
- agent를 활용하여 구축된 인벤토리 내로 OS 정보 등 인벤토리 자산 입력 자동

3 LLM 인공지능



- LLM 인공지능과 취약점 데이터베이스 연동
- MITER ATTACK 매트릭스 활용
- 공개 보안 문서 및 기술 자료 활용

| 구분 | | 상세내용 |
|--------------|-----------|---|
| S/W 개발환경 | OS | Windows 11, ubuntu 22.04 |
| | 개발환경(IDE) | Visual Studio Code |
| | 개발도구 | Git, npm, |
| | 개발언어 | JavaScript, TypeScript, |
| | 기타사항 | Docker for containerization, MySQL, 클라우드 서버 (AWS EC2) |
| H/W 구성장비 | 디바이스 | 해당 없음 |
| | 센서 | 해당 없음 |
| | 통신 | 해당 없음 |
| | 언어 | 해당 없음 |
| | 기타사항 | IoT 테스트 베드용 라즈베리파이 4 |
| 프로젝트 관리환경 | 형상관리 | GitHub |
| | 의사소통관리 | Slack, Zoom, Kakaotalk |
| | 기타사항 | Notion, Jira for project tracking |

<작품 개발 환경>

기술적 차별화



1. MITRE ATT&CK 매트릭스 DB화

- 체계적인 위협 모델링 및 보안 평가
- 실시간 업데이트로 최신 위협 대응

2. Django 기반 강력한 권한 관리 시스템

- 세분화된 역할 기반 접근 제어(RBAC) 구현
- 자산 등록자와 보안 담당자로 역할 명확화

3. 반자동화된 IoT 자산 모니터링 시스템

- 사용자 설정 쉘 스크립트를 통한 자산 정보 수집

4. AI 기반 맞춤형 취약점 분석

- LLM을 활용한 취약점 분석
- Attack Tree를 통한 공격 시나리오 시각화

5. 해양 물류 도메인 특화 데이터 모델

- 해양물류 특화 자산 모델 구현
- 해양물류 도메인 특화 보안 체크리스트 설계

프로젝트 가치와 작품의 기대효과



프로젝트 특징 및 장점



문제 정의

대부분의 기존 솔루션들은 특정 영역(네트워크, 앤드포인트 등)에 국한된 보안 관리 기능을 제공한다는 문제가 있었다. AI 기반 위협 분석 기술은 발전 중이나, 산업 특화된 솔루션은 부족한 실정이며, 자산 관리와 취약점 분석, 대응 방안 도출을 통합적으로 제공하는 솔루션은 제한적으로 존재한다.

1

IoT 자산 자동 스캔 및 분류 기능

2

사용자 친화적인 웹 인터페이스 및 대시보드

3

다양한 보안 툴과의 연동을 통한 종합적인 취약점 분석

4

MITRE ATT&CK 프레임워크
기반의 AI 모델 활용

5

자동화된 보고서 생성 및 전송 시스템

프로젝트의 차별성



◆ 국내·외 기술 현황

대부분의 기존 솔루션들은 특정 영역
(네트워크, 엔드포인트 등)에 국한된 보안 관리

AI 기반 위협 분석 기술은 발전 중이나, 산업 특화
된 솔루션은 부족한 실정

자산 관리와 취약점 분석, 대응 방안 도출을 통합
적으로 제공하는 솔루션은 제한적

◆ 기능적·기술적 차별성

해상 물류 특화 보안 솔루션으로, 산업 특성에 맞
는 맞춤형 보안 관리 제공

IoT 자산부터 소프트웨어 취약점까지 포괄하는
통합 보안 관리 플랫폼



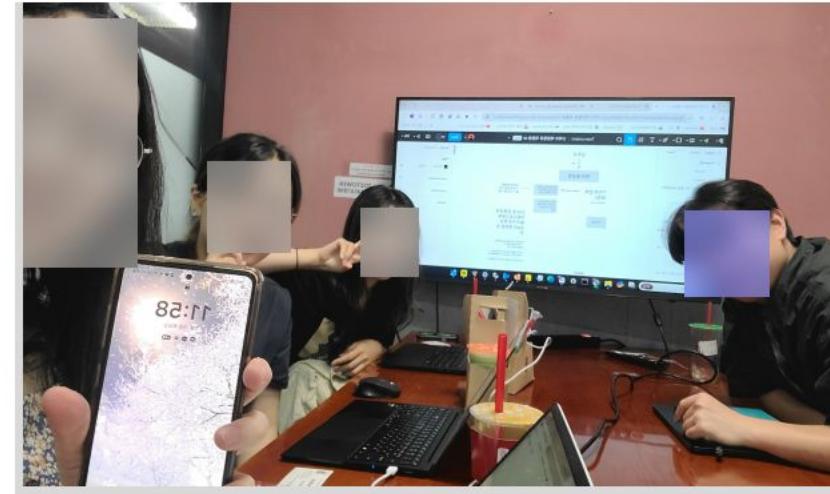
AI 기반 공격 시나리오 및 대응 방안 도출로
선제적 보안 대응 가능

프로젝트의 가치와 노력(1)

전문가의 조언을 통한 실제 해양물류 보안 프로세스 적용

| | | |
|-------|------------|---|
| 주간 회의 | 2024/03/19 | ▣ 오프라인 회의 - task 공유 |
| | | ↳ 편집 필요한 자료 |
| 코멘트 | | ↳ 교수님 논문 코멘트를 |
| | | ↳ 해상물류 OT 내용 |
| 주간 회의 | 2024/04/11 | 🕒 프로젝트 계획 설정 회의 |
| | | ↳ 오프라인 회의록 |
| | 2024/04/20 | ₩ 해양물류 킥오프 회의 |
| | 2024/05/02 | 🕒 정규 회의 |
| | 2024/05/02 | 🕒 정기 회의 |
| 주간 회의 | 2024/05/09 | ✍ 정기 회의 - 해상물류, 이미지 라벨링 진행 (labelimage) |
| 주간 회의 | 2024/05/18 | ✍ 0518 해상물류 회의 |
| 주간 회의 | 2024/05/30 | 🕒 0530 정기 회의 |
| | 2024/06/24 | ✍ 기획서 작성 |
| | 2024/06/25 | 🕒 해양물류 멘토님 회의록 미팅 |
| | | 🕒 해양물류 해야 할 것(작성) |
| 주간 회의 | 2024/06/27 | ▣ 발표 후 논의사항 |

| | | |
|-------|------------|-------------------------|
| 팀 회의 | 2024/08/08 | ▣ 구현해야 할 것 역할분담 |
| 임시 회의 | 2024/08/14 | 😊 진행상황리뷰 |
| | 2024/08/17 | ☒ To Do 리스트 |
| | 2024/08/20 | ☒ To Do 리스트 |
| 팀 회의 | 2024/08/22 | 🔥 회의 |
| | 2024/08/24 | 💙 광화문 해양물류 멘토님과 미팅 |
| | 2024/08/27 | 🕒 역할 분담(각자 할 일 하기) |
| 코멘트 | 2024/08/30 | 💜 💬 멘토님과 회의 |
| 팀 회의 | 2024/08/30 | ❗ 팀 회의 (역할분담) |
| | | ↳ 스해율 보고서 To write list |
| | 2024/09/07 | ↳ 논문 링크 |
| 팀 회의 | 2024/09/08 | 🌐 온라인 회의 |
| | 2024/09/10 | 📅 💬 논문회의 |
| | 2024/09/30 | 🔥 일정정리 |
| | 2024/10/01 | ❤️ 10/7 발표자료 회의록 |
| | 2024/10/02 | ✉️ 교수님 조언 |



꾸준한 팀별 회의와 피드백,
멘토님과의 미팅 진행

지속적인 프로젝트 개선과 팀 협업

선박 운행 회사 아비커스
보안 팀장님과의 인터뷰 진행

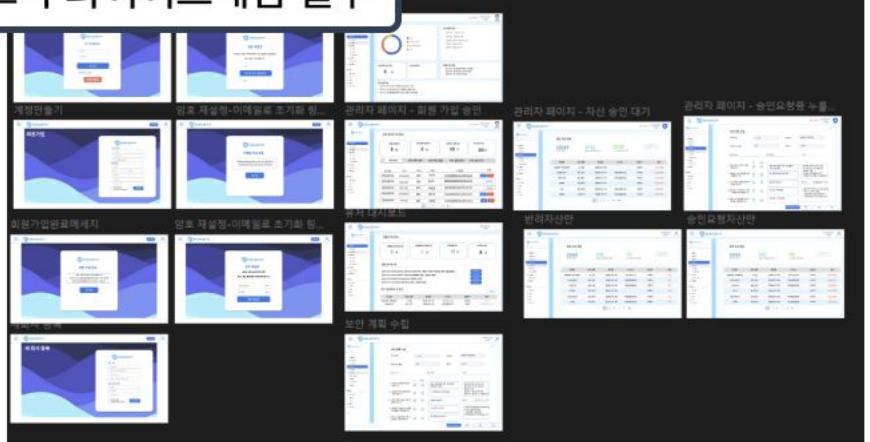
현업자 미팅을 통한 프로젝트 보완과
실효성 향상

프로젝트의 가치와 노력(2)

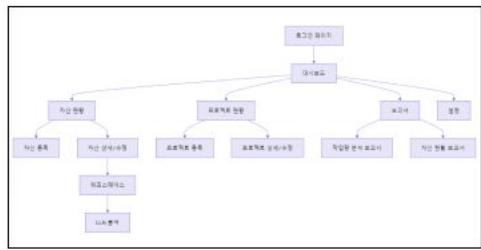


체계적인 프로젝트 설계와 개발 과정

피그마 와이어프레임 일부



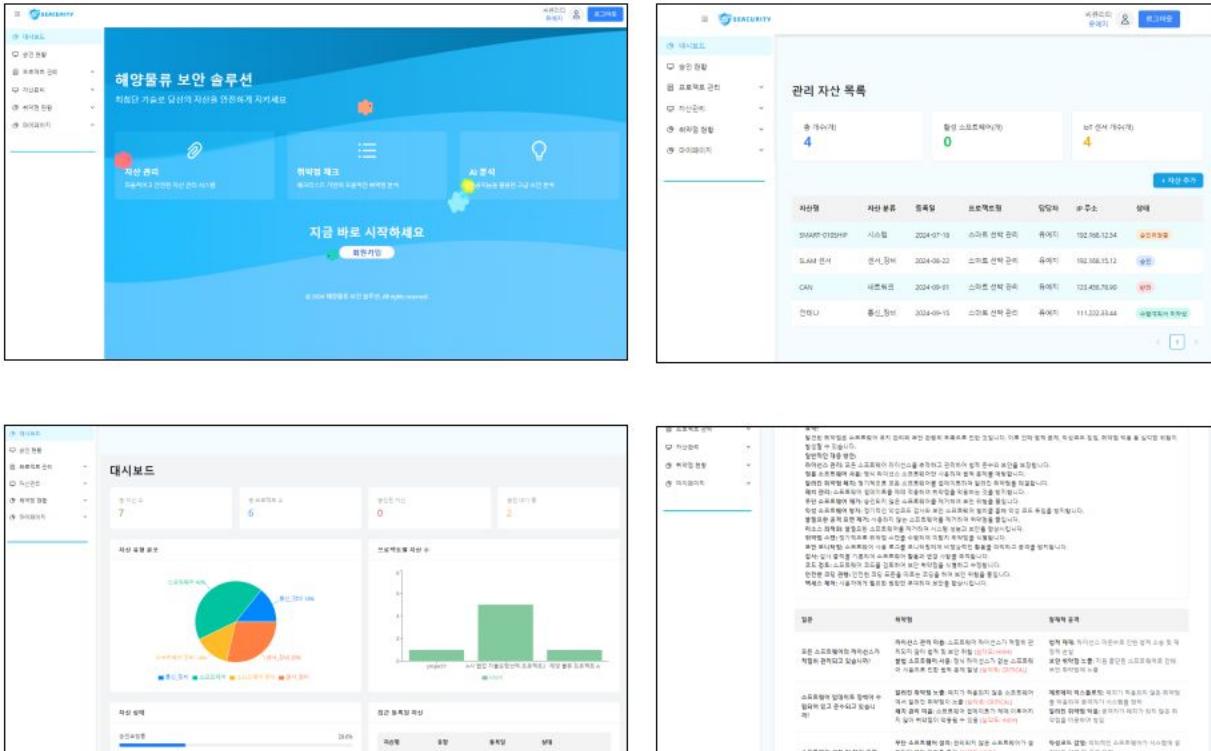
페이지 흐름도 구상



자산 조사

| 번호 | 자산이름 | 번호 | 자산이름 |
|----|------------------|----|-----------------------|
| 1 | 센서 장비 | 13 | 전세계 배상조난안전시스템 (GMDSS) |
| 2 | 통신 장비 | 14 | 품행죽성기 |
| 3 | 제어 장비 | 15 | 위성항법시스템 (GPS) |
| 4 | 컴퓨팅 장비 | 16 | 자이로 캠퍼스 |
| 5 | 소프트웨어 | 17 | 속도계 |
| 6 | 데이터 | 18 | 상황인식 시스템 |
| 7 | 네트워크 | 19 | 전자해도표시정보시스템 (ECDIS) |
| 8 | 인력 자원 | 20 | SCADA 서버 |
| 9 | 물리적 인프라 | 21 | 연진 자동화 시스템 |
| 10 | 항해 데이터 기록기 (VDR) | 22 | 경로 계획 시스템 |
| 11 | 고조주파(VHF) 라디오 | 23 | 항해 및 충돌 회피 시스템 |
| 12 | 자동식별시스템 (AIS) | 24 | 선수 추진 제어기 |
| | | 35 | 기상 정보 시스템 |
| | | 36 | 화물 관리 시스템 |

실제 구현



작품의 활용 분야와 기대효과

해운 산업



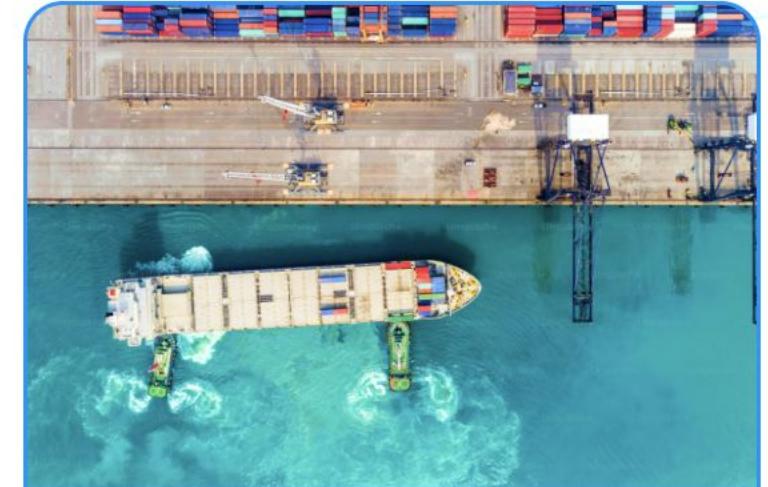
컨테이너선, 벌크선, 탱커선 등 다양한 유형의 상선 운영 회사가 있고 선박 내 IoT 장비 및 통신 시스템의 보안 관리나 선박-육상 간 데이터 통신 보안 강화 등을 적용할 수 있다.

조선 산업



조선 산업의 경우 대형 조선소 및 중소 조선 기업, 조선 기자재 제조 기업, 선박 설계 회사 등이 있다. 선박 설계 단계부터 보안을 고려한 시스템 구축, 스마트 조선소 내 네트워크 보안 강화를 적용할 수 있다.

항만 운영



항만 운영의 경우 컨테이너 터미널 운영 회사나 항만 공사 및 항만 관리 당국 등이 있고 항만 자동화 시스템 보안, 화물 추적 시스템 보호, 출입 통제 시스템 보안 강화 를 적용할 수 있다. 이 외에도 해양 플랜트, 해양 보안 기관 등 다양한 기관 및 사용자들에게 적용할 수 있다.

작품의 활용 분야와 기대효과



사이버 보안 위협에 대한
신속한 탐지 및 대응 능력 향상

정기적인 보안 점검 및 보고
서 자동 생성으로 규제 준수
용이성 증대

실시간 모니터링을 통한
보안 사고 대응 시간 단축

IoT 자산 관리의 효율성
증대로 인한 운영 비용 절감

맞춤형 보안 솔루션으로
해양 산업 특성에 최적화된
보안 관리 기능

AI 기반 공격 시나리오 예측
을 통한 선제적 보안 대책
수립 가능



사용자 입장에서의 기대효과

자동화된 취약점 분석으로
인한 보안 담당자의
업무 부담 감소

시연

