

2024년 스마트해상물류 × ICT멘토링 프로젝트 결과보고서

2024. 10.

프로젝트명	번호	24_HP020
	국문	해상 물류 사이버 보안 관리 및 모니터링 구축
	영문	Establishment of maritime logistics cybersecurity management and monitoring
작 품 명	Seacurity	
팀 명	씨큐리티가디언즈	
멘 토		
팀 장	성신여자대학교, 유예지	
팀 원	성신여자대학교, 이정연, 이지연, 양소윤	

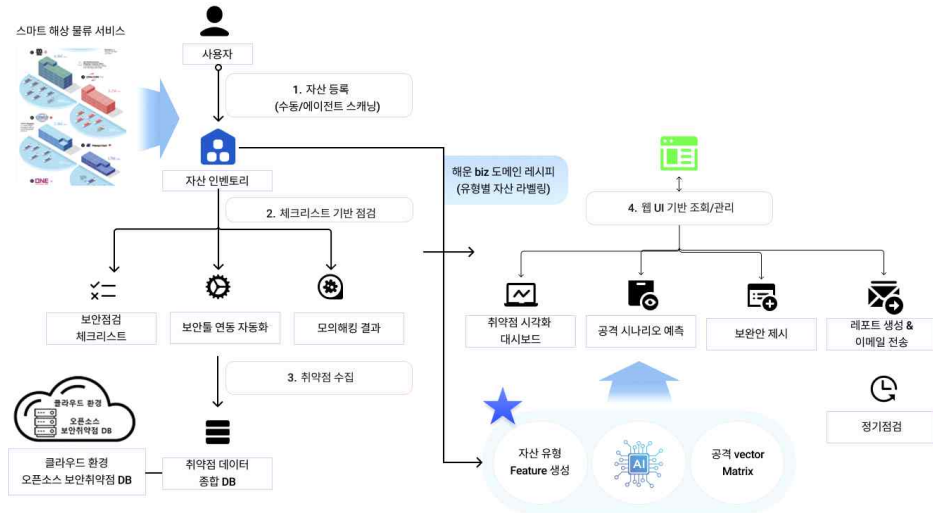
요 약 본

프로젝트 정보				
프로젝트명	해상 물류 사이버 보안 관리 및 모니터링 플랫폼 구축			
주제영역	<input type="checkbox"/>	컨테이너 화물 실시간 위치 및 상태 추적	<input type="checkbox"/>	항만 안전 IoT 개발
	<input type="checkbox"/>	유해 화학물질 가스 누출 감지	<input type="checkbox"/>	항만 원격조정 훈련 콘텐츠 제작
	<input type="checkbox"/>	물류 데이터 융복합 플랫폼	<input type="checkbox"/>	지속가능한 신재생에너지 활용
	<input checked="" type="checkbox"/>	실시간 항만 시설물 모니터링 및 예지 정비	<input type="checkbox"/>	액체 물류 스마트 모니터링 및 통제 기술
	<input type="checkbox"/>	사람-항만-선박 간 통신 교통 관제	<input checked="" type="checkbox"/>	해양/물류/항만의 적용 가능한 사업 아이템
	<input type="checkbox"/>	기타(<i>기타사항 기재</i>)		
달성성과	(스마트해상물류 경진대회) <input checked="" type="checkbox"/> 1차통과 <input type="checkbox"/> 2차통과 <input type="checkbox"/> 특허 <input checked="" type="checkbox"/> 학술(논문게재)			
	<input type="checkbox"/> 창업연계 <input type="checkbox"/> 프로그램등록 <input type="checkbox"/> 앱등록 <input type="checkbox"/> 기술이전			
수행기간	(예시) 2024. 4. 1. ~ 2024. 10. 31. (본인 팀에 맞는 수행기간으로 작성)			
프로젝트소개 및 제안배경	Seacurity는 해상 물류 분야의 사이버 보안을 강화하기 위해 개발된 지능형 보안 관리 플랫폼이다. 해상 물류의 디지털화로 인해 사이버 보안 위협이 급증하고 있으나, 기존의 보안 솔루션은 해양 산업의 특수성을 고려하지 못하는 한계가 있다. 이에 따라 선박과 항만에 사용되는 운영기술(OT)과 사물인터넷(IoT) 기기 등 사각지대에 놓인 자산들이 사이버 공격의 주요 타겟이 되고 있다. 이러한 상황에서 국제표준화기구(ISO)의 선박 사이버 보안 인증 요구사항을 기반으로 한 자동화된 점검과 모니터링을 통해 해상 물류 비즈니스의 안정성과 신뢰성을 향상시키고, 국가 물류 산업의 경쟁력을 높이며, 사이버 공격으로 인한 물류 시스템 마비를 방지함으로써 국가 안보 역량을 증진시킬 수 있을 것으로 기대된다.			
주요기능	1. 해양 비즈니스 특화 자산 인벤토리(자산 유형 분석 자동화) 2. 유형별 보안점검 체크리스트 3. 자동화 툴 및 모의해킹 점검기반 취약점 수집 4. 웹 인터페이스 기반 인벤토리 관리 5. 대시보드를 활용한 취약점 시각화 6. 취약점별 예상 공격 시나리오 경고 7. LLM 인공지능을 활용한 취약점 보완 안내 8. 자동 레포트 생성 및 이메일 전송 9. 자동화된 보고 및 정기점검			
적용기술	클라우드 컴퓨팅(AWS, Docker), 마이크로서비스 아키텍처(Spring boot, RESTful API), 인공지능(LLM, Transfer learning), 웹 기술(React, NEXT JS), 데이터베이스(Mysql), 자동화 및 스크립팅, 데이터 시각화			
기대효과 및 활용분야	1. 자율운항선박의 사이버보안 강화로 해양 안전성 제고 2. 효율적인 자산 관리 및 취약점 대응으로 운영 비용 절감 3. AI 기반 예측 및 분석으로 선제적 보안 대응 가능 4. 자동화된 보안 관리로 인적 오류 최소화 5. 해운, 조선, 해양 플랜트 등 다양한 해양 산업 분야에 활용 가능 6. 국제 해사 사이버보안 규정 준수 지원으로 글로벌 경쟁력 강화			

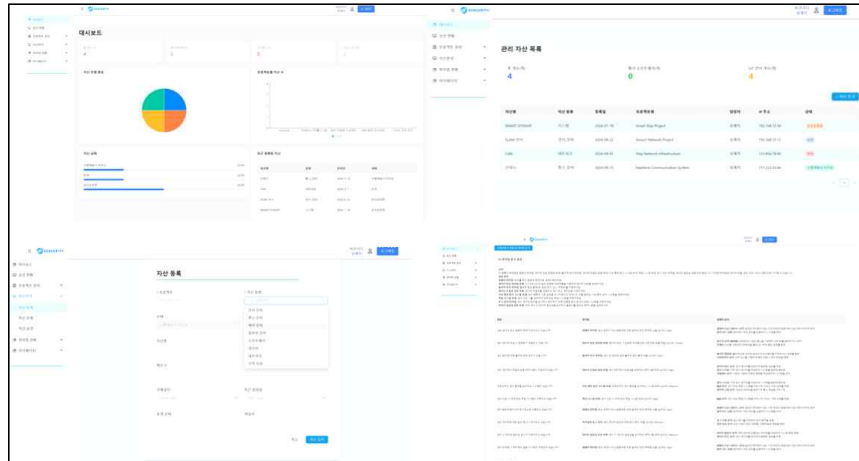
작품 구성도

작품 정보

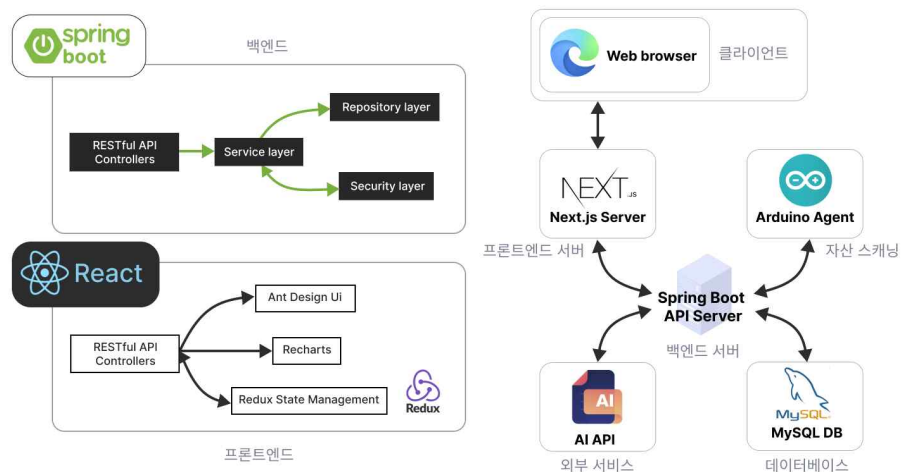
<시큐어 인벤토리 시스템 프로세스>



<웹 Ui 화면 >



<SW 구성도>



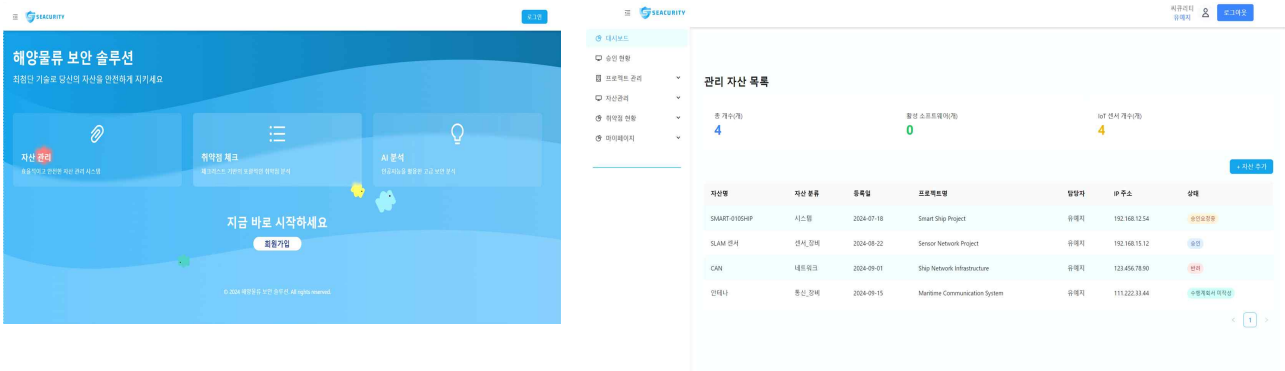
프로젝트 결과보고서

I. 프로젝트 개요

가. 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



□작품 내용

- Seacurity는 자율운항 선박의 해양 비즈니스 환경에 특화된 사이버보안 자산 인벤토리 관리 시스템임
- 자동화된 보안 취약점 스캔 및 분석
- AI 기반 공격 시나리오 및 대응 방안 도출
- 종합 보안 리포트 생성 및 자동 전송 기능
- 직관적인 웹 기반 관리 인터페이스 및 대시보드 제공

□정의

- 해상 물류 분야의 사이버보안을 종합적으로 관리하고 모니터링하는 지능형 플랫폼으로서 IT, OT, IoT를 아우르는 통합 자산 관리 및 보안 취약점 분석 솔루션을 제공함.
- 해상 및 해양 도메인 전문성을 갖춘 차세대 보안 관리 도구임.

나. 작품의 개발 배경 및 필요성

□개발 배경

- 해상 물류 산업의 디지털화에 따른 사이버보안 위협 증가

: 공격자들은 침입 탐지 및 방지 시스템 (IDS/IPS) 침투, 취약점 악용, 데이터 암호화 공격 등 다양한 공격 수법을 사용하여 해양 물류 시스템을 공격하고 있다. 이러한 공격은 물류 시스템 마비, 경제적 손실, 데이터 유출, 국가 안보 위협 등 심각한 피해를 야기할 수 있다.

- 복잡한 IoT 환경에서의 자산 관리 어려움

- 수동적이고 비효율적인 기존 보안 관리 방식의 한계

: 해상과 해양 산업은 여러 특수성을 지니고 있음에도 불구하고, 현재 대부분의 보안 솔루션은 이러한 점을 충분히 고려하지 않은 채 범용적인 접근을 하고 있다. 육상의 IT 환경에 최적화된 보안 솔루션들은 선박이나 항만 같은 곳에서 쓰이는 운영기술(OT)이나 사물인터넷(IoT) 기기들의 보안 요구사항을 제대로 반영하지 못하기 때문이다. 게다가 기존 솔루션들은 주로 IT 자산 관리에만 초점을 맞추다 보니, 선박이나 항만에 설치된 각종 센서, 제어시스템 등 OT/IoT 자산에 대한 가시성이 많이 부족하다. 이런 사각지대에 있는 자산들이 바로 사이버 공격의 주요 타겟이 되고 있다. 여기에 숙련된 해양 보안 전문 인력이 부족한 상황에서, 수동적이고 사후 대응 위주의 보안 운영으로는 한계가 있을 수밖에 없다.

□필요성

- 해상 물류 분야의 사이버 보안 수준 향상

: 해상 물류 산업의 사이버 보안 취약점을 국제표준화기구(ISO)의 선박 사이버보안 인증 요구사항을 기반으로 한 자동화 점검을 통해 효율적으로 관리하고 이력을 정기적으로 모니터링함으로써 해상 물류 비즈니스의 안정성과 신뢰성을 향상시키고자 한다. 이는 국가의 물류 산업 경쟁력을 향상시키고 사이버 공격으로 인한 물류 시스템의 마비를 방지함으로써 국가의 안보의 역량을 증진시킬 것으로 예상된다.

- 자동화된 취약점 관리로 보안 담당자의 업무 효율성 증대

- AI 기반 분석으로 보다 정확하고 신속한 보안 위협 대응 체계 구축

- 정기적인 보안점검 및 보고 프로세스의 자동화

다. 작품의 특징 및 장점 / 국내 · 외 기술 현황 및 본 프로젝트의 차별성

□국내 · 외 기술 현황

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

- AI 기반 위협 분석 기술은 발전 중이나, 산업 특화된 솔루션은 부족한 실정
- 자산 관리와 취약점 분석, 대응 방안 도출을 통합적으로 제공하는 솔루션은 제한적

□작품의 특징 및 장점

- IoT 자산 자동 스캔 및 분류 기능
- 다양한 보안 툴과의 연동을 통한 종합적인 취약점 분석
- MITER ATT&CK 프레임워크 기반의 AI 모델 활용
- 사용자 친화적인 웹 인터페이스 및 대시보드
- 자동화된 보고서 생성 및 전송 시스템

□기능적/기술적 차별성

- 해상 물류 특화 보안 솔루션으로, 산업 특성에 맞는 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
- 자동화된 보고 체계로 지속적이고 효율적인 보안 관리 지원
- 사용자 편의성을 고려한 직관적인 인터페이스로 접근성 향상

II. 프로젝트 수행결과

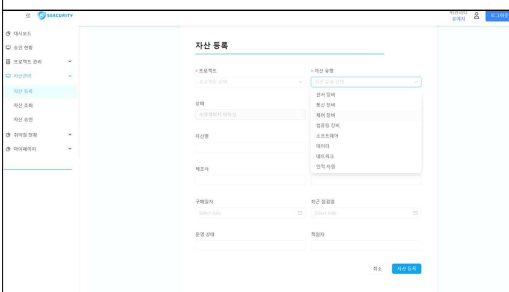
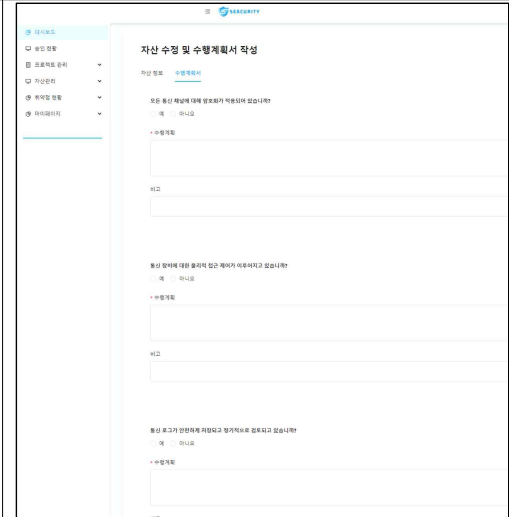
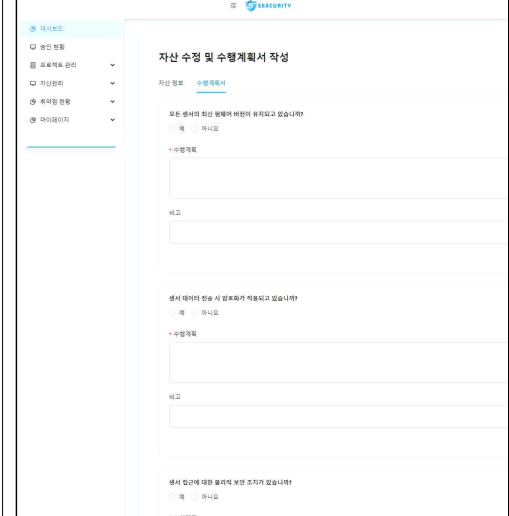
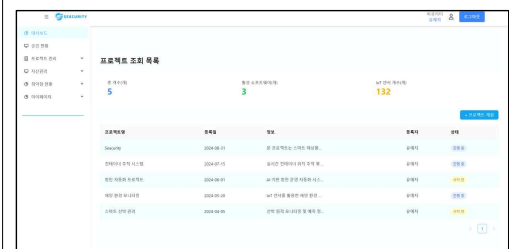
가. 프로젝트 개발환경


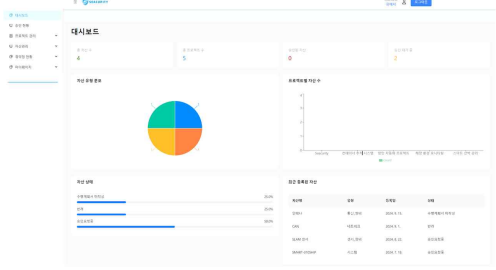
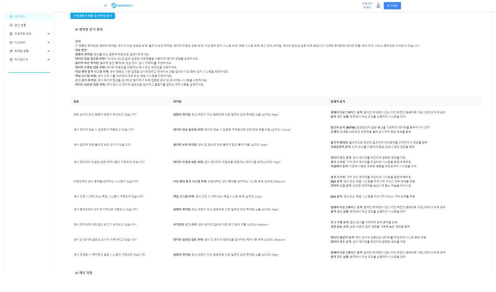

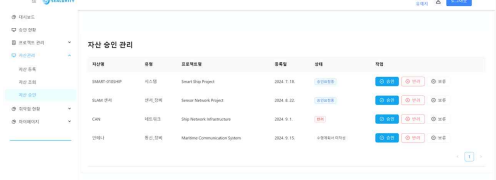
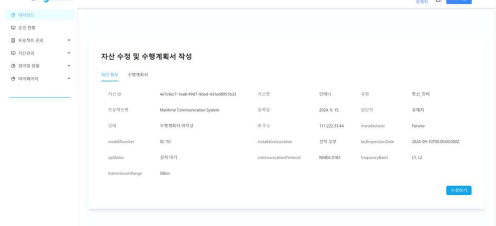
구분		상세내용
S/W 개발환경	OS	Windows 11, ubuntu 22.04
	개발환경(IDE)	Visual Studio Code
	개발도구	Git, npm, Maven
	개발언어	JavaScript, TypeScript, Java
	기타사항	Docker for containerization, MySQL, 클라우드 서버 (AWS EC2)
H/W 구성장비	디바이스	해당 없음
	센서	해당 없음
	통신	해당 없음
	언어	해당 없음
	기타사항	IoT 테스트베드용 라즈베리파이 4
프로젝트 관리환경	형상관리	GitHub
	의사소통 관리	Slack,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

나. 환경장비(기자재/재료) 활용

번호	품명	작품에서의 주요기능
1	아두이노 우노	- 센서 정보 자동 전송 및 확인을 위한 테스트베드
2	라즈베리파이	- 센서 정보 자동 전송 및 확인을 위한 테스트베드 라즈베리파이 및 각종 센서 통해서 구축
3		-
4		-
5		
6		

다. 주요 기능 목록

자산 인벤토리	<ul style="list-style-type: none"> - 사용자는 목록을 스캔하여 필요한 자산을 프로젝트에 추가하여 손쉽게 관리 가능 - 자산 유형별로 다른 속성의 정보를 등록할 수 있도록, 자산 유형 이름을 파싱하여 다른 자산 입력 폼 제공 	
유형별 보안점검 체크리스트	<ul style="list-style-type: none"> - MITER ATTACK 네비게이터와 CSV 취약점, 해양물류 도메인 논문에 언급된 각 자산별 취약점과 공격을 매핑하여, 체크리스트 형태의 질문지에 매핑 - 자산의 수행계획서 작성 시, 해당하는자산의 취약점에 대비할 수 있는 체크리스트 출력 및 계획수립 가능 	
자동화 툴 및 모의해킹 점검기반 취약점 수집	<ul style="list-style-type: none"> - 블랙덕, 소나큐브 등 모의해킹 툴을 사용하여 수집한 취약점을 별도의 [비고]칸과 첨부파일 칸에 수기로 작성 및 첨부 가능 - 보안담당자는 해당 파일과 비고란을 확인하여 모의해킹 결과를 열람하고 후속대응 가능 	
웹 인터페이스 기반 인벤토리 관리	<ul style="list-style-type: none"> - 각 인벤토리는 프로젝트 단위로 쪼개어져 프로젝트 단위로 관리 가능하게끔 인터페이스 설계 - 일목요연하게 볼 수 있도록 테이블 형태의 표 위주의 구성 - 표 내부의 데이터 및 버튼을 클릭 	


	<p>및 상호작용하여 세부 정보 확인 및 해당 자산 관련 페이지 이동 추가</p>	
<p>대시보드를 활용한 취약점 시각화</p>	<ul style="list-style-type: none"> - 관리 자산별 취약점 목록과 자산 목록을 React 차트 라이브러리를 이용하여 구현 - 본인이 담당하는 자산의 승인/비승인 여부와 업데이트 및 취약점 내역 한 눈에 확인 가능 	
<p>취약점별 예상 공격 시나리오 경고</p>	<ul style="list-style-type: none"> - 체크리스트에 매핑된 취약점과 예상 공격을 통해, DB Join을 통하여 해당 취약점이 가질 수 있는 공격 루트와 예상 시나리오 출력 - 보다 자세한 취약점 및 후속 공격 설명 항목을 표로 시각화 	
<p>LLM 인공지능을 활용한 취약점 보완 안내</p>	<ul style="list-style-type: none"> - LLM 채팅을 통해 취약점 설명을 전생하여 확인 가능하며, 이후 자유로운 후속 질의를 통해 최우선 조치 식별 	
<p>자동 레포트 생성 및 이메일 전송</p>	<ul style="list-style-type: none"> - 취약점 결과 및 대시보드 화면을 pdf로 저장하여 지정된 사용자에게 메일 전송 	
<p>자동 정기점검</p>	<ul style="list-style-type: none"> - 주기적으로 체크리스트 및 자산 담당자에게 알림을 보내어 자산 상태 재확인하고 체크리스트 재작성 요구 	

--	--	--

- S/W 주요 목표대비 현재 개발결과 상세 설명

모두 개발 완료

2) H/W 개발 기능 상세내용

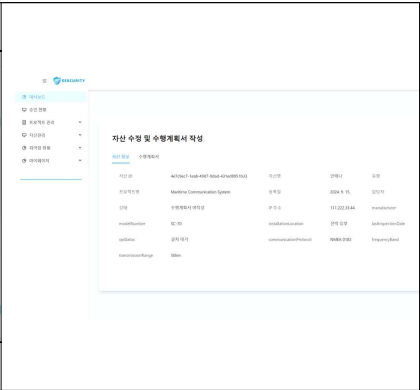
기능/부품	설명	작품실물사진
IoT 테스트베드용 라즈베리파이 4	센서 정보 자동 전송 및 확인을 위한 테스트베드 라즈베리파이 및 각종 센 서 통해서 구축	

- H/W 주요 목표대비 현재 개발결과 상세 설명

라. 프로그램 작동 동영상

- <https://youtu.be/kDp7NmD8Ukw>
- <https://youtu.be/pvz8RQevrkk>

마. 결과물 상세 이미지

		
---	--	---

(이미지 첨부)

바. 달성성과

<input checked="" type="checkbox"/> 논문게재 및 포스터발표	게재(발표)자명	논문(포스터)명	게재(발표)처	게재(발표)일자
	유예지	산학 사이버 보안 위협 모델링 VSAT 및 위성 통신 취약점 분석과 대응 전략	ACK 2024	2024. 11.01.
<input type="checkbox"/> 앱(APP) 등록	등록자명	앱(APP)명	등록처	등록일자
				2024. 00. 00.
<input type="checkbox"/> 프로그램 등록	등록자명	프로그램명	등록처	등록일자
				2024. 00. 00.
<input type="checkbox"/> 특허출원	출원자명	특허명	출원번호	출원일자
				2024. 00. 00.
<input checked="" type="checkbox"/> 공모전	구분(교내/대외)	공모전명	수상여부(출품/수상)	상격
	대외	제회 해양기업 디지털 전환 우수사례 아이디어 공모전	출품	
<input type="checkbox"/> 실용화	#실용화한 내용에 대한 구체적 작품설명			
<input type="checkbox"/> 기타				

Ⅲ. 프로젝트 수행방법

가. 업무분장

번호	성명	역할	담당업무
1	신승훈	멘 토	작품 가이드라인 제시 및 문서 검토
2	최현우	지도교수	논문 첨삭
3	유예지	팀 장	- 프론트엔드&백엔드 개발
4	이정연	팀 원2	- 보안 체크리스트 모델링 및 데이터베이스 구축
5	이지연	팀 원3	- UI 디자인 및 문서 작성
6	양소윤	팀 원4	- 프론트엔드 개발 및 데이터베이스 모델링

나. 프로젝트 수행일정

프로젝트 기간 (ICT멘토링 사이트 기준)			2024. 4. 1. ~ 2024. 10. 31.						
구분	추진내용	구분	프로젝트 기간						
			4월	5월	6월	7월	8월	9월	10월
계획	프로젝트 제반사항 정립 및 계획 구체화	계획	4	5					
		진행	4	5	6				
분석	취약점 기반 MITER ATT&CK 보안 공격 시나리오 분석	계획			6	7			
		진행			6	7			
설계	시스템 아키텍처 설계 및 데이터 모델링	계획				7	8		
		진행				7	8		
	사용자 인터페이스 설계	계획				7	8		
		진행				7	8		
개발	IoT 센서 데이터 자동전송 데몬 및 서버 구축	계획						9	10
		진행						9	
	백엔드 서비스 및 데이터베이스 구현	계획					8	9	
		진행					8	9	
	보안 인공지능 모델 구현	계획						9	10
		진행						9	
	프론트엔드 인터페이스 개발	계획					8	9	
		진행					8	9	
테스트	데모 제작 및 피드백 반영	계획					8	9	10
		진행					8		
종료	개발 종료 및 공모전 발표 준비	계획						9	10
		진행							10

다. 프로젝트 수행(협업) 방안

- 페어 프로그래밍을 위해 8월 한 달간 매일 오후 3시부터 10시까지 대면으로 모여 코딩 진행
- 같은 학교 학생들로 구성되어 있어 학교 내부 회의실을 활용하여 지속적인 협업 환경

구성

- 대면 작업을 통해 실시간 소통 및 문제 해결이 가능해져 개발 효율성 증대
- GitHub를 이용한 코드 버전 관리 및 코드 리뷰 진행
- 주간 스프린트 계획 수립 및 회고를 통한 지속적인 프로세스 개선
- 협업툴(notion)을 이용하여 회의 내용 및 프로젝트 수행 내역 공유

라. 문제점 및 해결방안

○ 프로젝트 관리 측면

- 문제점

팀원들의 기술 스택 차이로 인한 작업 속도 불균형

- 해결 경험

페어 프로그래밍 도입 및 정기적인 기술 공유 세션을 통해 팀원 간 지식 격차 해소

- 문제점

장시간 대면 작업으로 인한 피로도 증가

- 해결 경험

적절한 휴식 시간 배정 및 작업 환경 개선(편안한 의자, 조명 조절 등)

○ 작품 개발 측면

- 문제점

Spring Security의 복잡한 권한 설정으로 인한 개발 지연 및 디버깅 어려움

- 해결 경험

초기에는 모든 제한을 해제하고 super admin 권한으로 개발을 진행한 후, 기능이 정상 작동하는 것을 확인한 뒤 점진적으로 권한을 세분화하는 방식을 채택. 이를 통해 개발 속도를 높이고 문제 해결을 용이하게 함.

- 문제점

서버 로깅 시 403 Forbidden 오류로 인한 디버깅 어려움

- 해결 경험

권한 설정을 일시적으로 완화하여 로깅을 가능하게 한후, 문제 해결 후 점진적으로 보안 수준을 높임.

- 문제점

자산 관리에 있어서 체크리스트를 어떻게 뽑아야하는지, 해상물류에 특화된 도메인을 어떻게 잡아야하는지에 대한 막막함과 어려움

- 해결 경험

실제 해양물류 정보보안팀 소속 멘토님과 강남역 토즈타워 회의실을 빌려 대략 두 시간 동안 선박에 대한 자산 관리 회의 진행. 선박을 위주로 자산 관리, 취약점 점검 등

피드백을 받고 방향성을 잡기 시작함.

IV. 기대효과 및 활용분야

가. 작품의 활용(적용)분야

- 해운 산업의 경우 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 등 적용할 수 있다.
- 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 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 강화를 적용할 수 있다.
- 이 외에도 해양 플랜트, 해양 보안 기관 등 다양한 활용 및 사용자들에게 적용할 수 있다.

나. 작품의 활용에 의한 기대효과(사용자)

- 사이버 보안 위협에 대한 신속한 탐지 및 대응 능력 향상
- IoT 자산 관리의 효율성 증대로 인한 운영 비용 절감
- 자동화된 취약점 분석으로 인한 보안 담당자의 업무 부담 감소
- AI 기반 공격 시나리오 예측을 통한 선제적 보안 대책 수립 가능
- 정기적인 보안 점검 및 보고서 자동 생성으로 규제 준수 용이성 증대
- 통합 보안 관리 시스템으로 인한 전반적인 보안 수준 향상
- 실시간 모니터링을 통한 보안 사고 대응 시간 단축
- 맞춤형 보안 솔루션으로 해양 산업 특성에 최적화된 보안 관리 기능

다. 작품의 기대가치

□차별성 및 시장성

- 해양 산업 특화 솔루션으로, 기존의 범용 보안 솔루션과 차별화
- IoT 자산 관리부터 AI기반 위협 분석까지 통합된 원스톱 보안 관리 플랫폼 제공

- MITER ATT&CK 프레임워크와 실제 취약점 데이터 기반의 고도화된 AI 모델
- 해양 산업의 디지털화 가속에 따른 사이버 보안 시장 확대 전망
- 통합 솔루션으로 개별 보안 도구 구매 대비 비용 효율성 제공
- 자동화된 프로세스로 인한 인건비 절감 효과로 장기적 비용 절감 가능

□사회적, 경제적 가치

- 해양 물류 인프라의 안전성 강화로 국가 경제 안보에 기여
- 사이버 보안 사고 예방을 통한 해양 환경 보호 및 안전 운항 지원
- 국제 해사 기구(IMO)의 사이버 보안 규정 준수 지원으로 국제 경쟁력 강화
- 사이버 보안 사고로 인한 경제적 손실 예방
- 효율적인 보안 관리로 인한 운영 비용 절감 및 생산성 향상
- 국내 해양 사이버 보안 기술의 고도화로 관련 산업 육성 및 수출 증대 기대
- 안전한 해상 물류 환경 조성으로 국제 무역 및 물류 산업 발전에 기여

V. 참고자료

가. 참고 및 인용자료

- 조용현 and 차영균. “위협 모델링을 이용한 선박 사이버보안 요구사항 연구“
정보보호학회논문지 29, no.3 (2019) : 657-673.doi:
<https://doi.org/10.13089/JKIISC.2019.29.3.657>
-

별첨

스마트해상물류 × ICT멘토링 프로젝트 산출물



전남대학교 광주캠퍼스

주최: kips 한국정보처리학회

주관: kips 한국정보처리학회 전남대학교

후원: GJTO 광주관광공사 전남대학교 소프트웨어융합대학사업단 KC-ST 한국과학기술단체총연합회

협찬: ETRI 한국전자기술연구원 CQZ TECHNOLOGY LG U+ kt KT경제정보통신사업부 DESILO

SNPLAB SK telecom MarkAny* 비온씨 이투스교육 리얼리브 NEXlim 세림TSG KCC정보통신연구원

Soda (위소다)시스템 AhnLab opas UNIWIDE UNIC WITCHES SK broadband

모데인 NatureSYS JWATS COONTEC HEAAN KCC정보통신

HUAWEI GL associates DO+용인시스템 SECUEVER ATEC 에어텍 KNETZ 무순

19. AI를 활용한 유해조류 퇴치기 KIPS_C2024B0237
신기택*, 장혜리, 조수형, 홍예원(서울과학기술대학교)
20. ARM과 Cube AI를 이용한 저전력 AI 객체 인식 군사 경계 시스템 ARM-I KIPS_C2024B0243
김영환*, 문석영, 박진수, 신민재, 정민재(영지대학교)

S5. 메타버스 및 XR

01. 인공지능 유사도를 활용한 재료 기반 음식 추천 AR 서비스 개발 KIPS_C2024B0151
이소정(성신여자대학교), 김지훈(한양대학교), 김강현(한국방송통신대학교), 안정후(서울과학기술대학교), 함승원(성신여자대학교), 문재현(한국기술거래사회)

S7. 인간-컴퓨터 상호작용

01. 보행 해충 제거 및 처리 기기 개발에 관한 연구 KIPS_C2024B0042
이다혜*, 정가은, 장서우, 권소윤, 윤예지(이화여자대학교)

ICT엔도링(스마트해상물류)

C1. 컴퓨터시스템 및 이론

01. VR기반 항만 크레인 시뮬레이터의 현실성 향상법 KIPS_C2024B0129
민재영*, 최서현, 함경민(동양미래대학교)

C4. 차세대 통신 시스템 및 네트워크

01. 해안 대기환경 감시를 위한 드론 시스템 개발 KIPS_C2024B0158
이가윤*, 김주혁, 이병택(가톨릭대학교), 유진호(한국전교)

C5. 사물인터넷

01. 항만구역 안전사고 방지 위한 순찰 로봇 KIPS_C2024B0059
산승진, 안현아, 배가은, 홍민(한국공학대학교), 김인수(ECS텔레콤)
02. 항만-선박 내 실정지 환자 응급 처치를 위한 스마트 심폐소생기 KIPS_C2024B0081
신윤정*, 오민지, 이종규, 김승환, 김지환(한국공학대학교), 김인수(ECS텔레콤)

C6. 정보보안

01. 선박 사이버 보안 위험 모델링: VSAT 및 위성 통신 취약점 분석과 대응 전략 KIPS_C2024B0386
유예지*, 이정연, 이재연, 양소윤, 최현우(성신여자대학교)

C9. ICT융합

01. RE100/CF100 대응을 위한 스마트 항만 모니터링 시스템 구축 KIPS_C2024B0007
이상안(인하대학교), 강병현(경북대학교), 고준섭(연세대학교)
02. UWB를 이용한 스마트 물류 시스템 구축 KIPS_C2024B0021
김호재, 공다인, 김가은*, 김수민(울산대학교)
03. 항만 종사자의 사고 예방 및 대응을 위한 원격 항만 정찰 로봇 KIPS_C2024B0073
장원호*, 서지영, 방진보, 전창영(한국공학대학교)
04. 항만-선박내인명사고방지위한UWB기반스마트안전시스템 KIPS_C2024B0101
윤진혁, 양상진, 권동민*, 최동환, 정두희(한국공학대학교), 김인수(ECS텔레콤)
05. 자율운항선박을 위한 강화학습 에이전트 기술 연구 KIPS_C2024B0126
오유원(서울시립대학교), 양소희(동덕여자대학교), 이재훈(서울과학기술대학교), 황윤주(동덕여자대학교), 이규영(한국과학기술원)
06. AI 기반 자율 청소 로봇 구현을 통한 해변 통합 관리 시스템 제안 KIPS_C2024B0131
송예경, 유자혜*, 황예찬, 재유나, 박기영(경북대학교)
07. YOLO7 기반 해상 침적 쓰레기 감출 방법에 관한 연구 KIPS_C2024B0134
최영수(국립목포대학교), 김도연(해제대학교)
08. 디지털 트윈을 이용한 항만 컨테이너 적재 최적화에 관한 연구 KIPS_C2024B0142
김유경, 남정화*, 양정은, 유재현, 하재복, 권혁준(한국폴리텍대학)

S2. 데이터 과학

01. AIS 데이터 분석을 통한 선박 안전행로 데이터 모델 개발 KIPS_C2024B0505
김상우, 양연희(남서울대학교), 조현화(남서울대학교), 이강준(HD현대중공업)

26 ACK 2024