

한양여자대학교 스마트 IT

Seculot

IoT 기기 보안 강화를 위한 위험도 예측과
보안 오픈 소스 소프트웨어 제공 웹 플랫폼

목차

01

프로젝트 개요

- 팀 소개
- 프로젝트 소개 및 목표
- 문제 정의 및 개발 이유

02

분석 및 전략

- 벤치마킹 및 차별성
- SWOT 분석
- 페르소나

03

디자인 및 아키텍쳐

- 디자인 개요
- 프로토타입
- 워크플로우
- 진행현황

04

개발 환경 및 기술

- 개발 환경 및 언어
- 데이터베이스 설계
- E-R 다이어그램, 테이블 정의서, 모듈 목록

05

인공지능

- AI 모델 설명
 - 모델 개요, 데이터 수집, 데이터셋 설명, 모델 선택
- 점수 예측 알고리즘
 - 위험도 구간, 알고리즘 구현, 모델 성능 개선

06

주요 기능 개요

- 보안 오픈 소스 제공
- 즐겨찾기
- IoT 기기 위험도 평가
- 마이페이지
- 커뮤니티
- 챗봇

07

프로젝트의 기대효과 및 발전 가능성

- 기대효과
- 발전 가능성

08

기타

- TC
- 시연영상
- 부록
- 소감

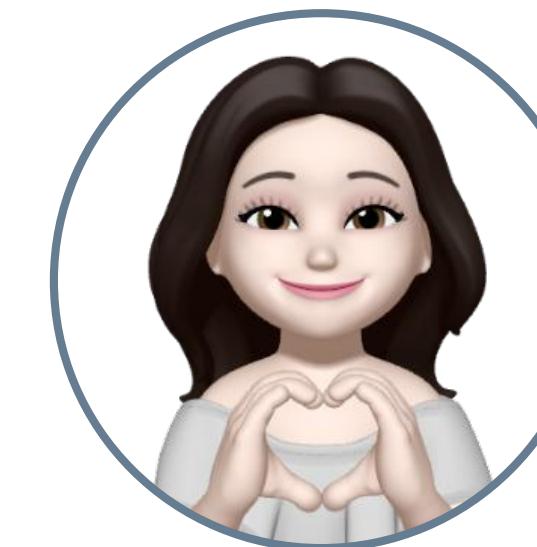
프로젝트 개요

S e c u l o T - D U C K

1.1. 팀 소개

1.2. 프로젝트 소개 및 목표

1.3. 문제 정의 및 개발 이유



2201636 임예빈 (팀장)

- 디자인
- 프론트엔드
- 백엔드
- PPT



2201614 서윤지 (팀원)

- 디자인
- 프론트엔드



2201637 임유빈 (팀원)

- 서브 디자인
- 프론트엔드

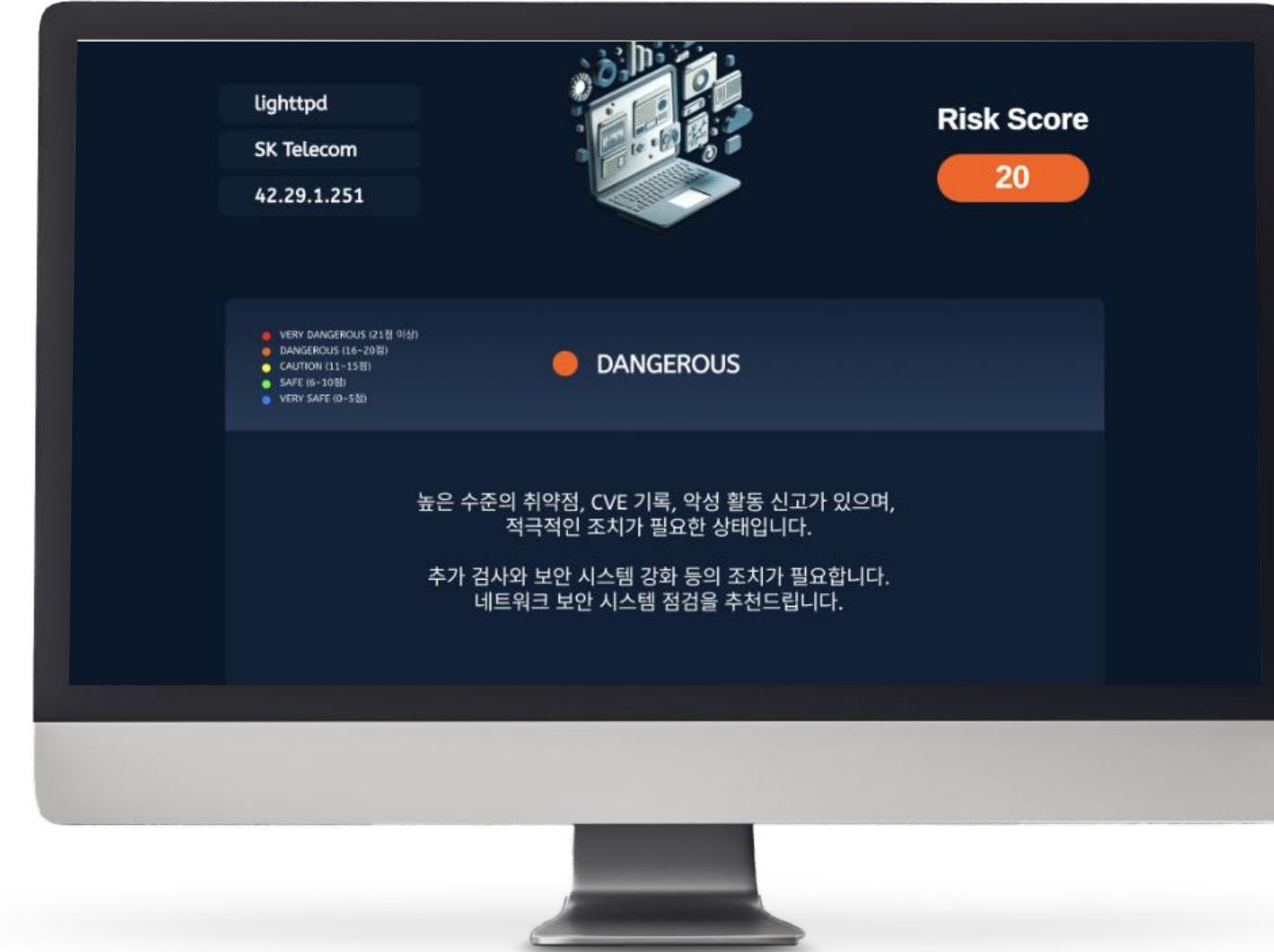
프로젝트 개요

S e c u l o T - D U C K

1.1. 팀 소개

1.2. 프로젝트 소개 및 목표

1.3. 문제 정의 및 개발 이유



SeculoT

Security + IoT

"IoT 기기의 보안 위험을 예측하고, 보안 오픈
소스 소프트웨어를 제공하여 사용자들이 보안
정보를 쉽게 찾고 활용할 수 있도록 돋는 웹 플랫폼"

- 1.1. 팀 소개
- 1.2. 프로젝트 소개 및 목표
- 1.3. 문제 정의 및 개발 이유

프로젝트 필요성

01

보안 위협 증가

IoT 기기의 사용이 증가함에 따라 보안 위협도 급증하고 있다. 많은 사용자가 보안에 취약한 기기를 사용하고 있지만, 적절한 대책을 모르거나 미비한 상태다.

02

보안 도구 접근성 부족

사용자가 실질적인 보안 대책을 찾기 어렵고, 적절한 오픈 소스 소프트웨어에 대한 접근이 제한적이다. 이 프로젝트는 이러한 문제를 해결하기 위해 다양한 보안 도구를 모아서 제공한다.

03

보안 인식 부족

많은 사용자가 자신의 IoT 기기가 보안 위협에 노출될 수 있다는 점을 인지하지 못하고 있다. 이 프로젝트는 보안 인식을 높이고, 관심을 가지게 하며, 적극적으로 보안 상태를 점검할 수 있도록 돋는다.

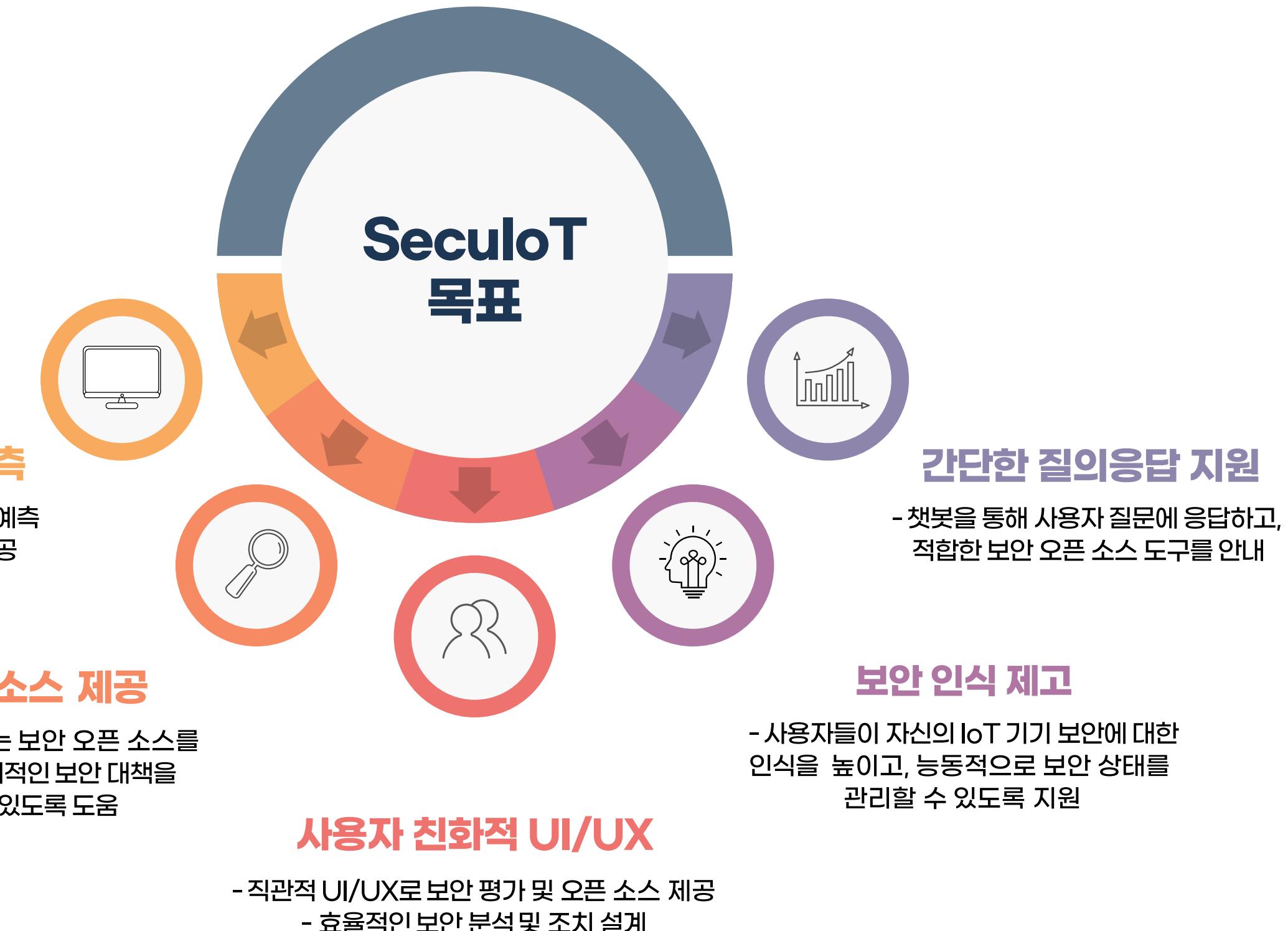
프로젝트 개요

S e c u l o T - D U C K

1.1. 팀 소개

1.2. 프로젝트 소개 및 목표

1.3. 문제 정의 및 개발 이유



프로젝트 개요

S e c u l o T - D U C K

1.1. 팀 소개

1.2. 프로젝트 소개 및 목표

1.3. 문제 정의 및 개발 이유

기존 문제점

문제 근거

보안 소프트웨어 정보의 분산

- 다양한 플랫폼에 보안 오픈소스가 흩어져 있어, 필요한 소스를 바로 찾기 어렵다.
- 보안 소프트웨어에 대한 통합된 정보 제공이 부족하다.



오픈소스 소프트웨어의 분산

보안 관련 오픈 소스 소프트웨어는 다양한 개발자 및 커뮤니티에 서제공되지만, 이를 한 곳에서 접근하기는 어렵다.

IoT 기기 보안의 취약성

- 많은 사용자가 자신이 사용하는 IoT 기기의 보안 상태를 정확히 모른다.
- 기본 보안 설정이 부족하거나 업데이트되지 않은 IoT 기기가 공격에 취약하다.



IoT 기기의 보안 취약점 증가

IoT 기기의 보안 취약점은 매년 증가하고 있으며, 이는 개인정보 유출 및 사이버 공격의 주요 원인이 되고 있다.

복잡한 보안 설정/평가

- 일반 사용자가 IoT 기기의 보안 위험을 평가하고 이해하는 것은 어렵다.
- 보안 설정이 복잡하여 일반 사용자가 이해하기 어렵다.



사용자의 보안 인식 부족

많은 사용자가 자신의 IoT 기기가 보안 위험에 처할 수 있음을 인식하지 못하고 있으며, 이에 따른 예방적 조치가 부족하다.

프로젝트 개요

S e c u l o T - D U C K

1.1. 팀 소개

1.2. 프로젝트 소개 및 목표

1.3. 문제 정의 및 개발 이유

근거 기사 자료 - IoT 보안

<1조 달러 돌파 눈앞에 둔 IoT 시장 규모 - CCTV뉴스 - 석주원 기자 (cctvnews.co.kr)>

전세계 IoT 시장 규모가 2023년까지 연평균 12.6%의 성장세를 유지해 2022년 1조 달러(약 1126조 원)를 돌파하고, 2023년에는 1조 1천억 달러(약 1234조 원)에 이를 것으로 전망했다. 스마트팩토리와 운송분야가 가장 큰 시장을 형성할 것으로 봤고, 가정용 시장에서는 스마트홈과 커넥티드카가 IoT 시장의 성장을 주도할 것으로 내다봤다. 코로나19의 장기화로 실내에서 생활하는 시간이 증가한 것도 스마트홈 시장 성장에 영향을 미칠 것으로 보인다. 스마트홈 IoT를 활용하는 가구 수는 매년 20% 이상씩 증가해 2023년에는 3억 가구가 넘어설 것으로 내다봤다.

<냉장고에 설치된 카메라, 해커가 노린다…삼성도 강조한 'IoT 보안' 뭐길래 - 조선비즈 (chosun.com)>

스마트폰과 스마트TV를 매개로 냉장고, 로봇청소기, 세탁기, 식기세척기, 조리기, 조명 등 다양한 가전제품이 연결되며 상호작용하는 시대가 열렸다. 여러 기기를 종합적으로 컨트롤 할 수 있다는 편리함을 가졌지만 보안에 취약한 구조를 가진다. 한 기기만 해킹해도 나머지 기기는 무방비로 열리기 때문에 IoT 보안이 중요하다고 강조하는 이유이다. 아파트 월패드 해킹으로 카메라에 담긴 사생활 영상이 다크웹에서 거래되기도 했다. 보안업계 관계자는 "집 안에 있는 기기가 모두 인터넷 공유기를 통해 서로 연결되는데, 스마트폰이 해킹당하거나 아파트 관리소 서버가 해킹당하면 월패드부터 모든 집안의 전자기기가 해커에 노출될 수 있어 위험하다"라고 했다.

<늘어나는 IoT 기기, "해킹 공포 여전해" - CCTV뉴스 - 전유진 기자 (cctvnews.co.kr)>

AIスピ커와 IoT 기기 등 이용자의 개인 데이터를 수집하는 제품들이 생활 속으로 빠르게 침투하면서 개인정보 유출에 관해 우려되고 있다. 일상생활에서 사용하는 각종 통신 기기들이 IoT·휴대용 통신 수단 그리고 이와 결합한 다양한 형태의 서비스로 퍼지면서 많은 사람이 사이버 보안 위협의 표적이 되고 있다. 가정용 IP 카메라가 해킹되면 사생활이 그대로 노출되고 자동차와 진료 기기가 해킹되면 교통사고나 의료사고로 연결되어 생명이 위험해질 수 있다. 우리나라에서도 IP 카메라나 스마트홈 기기를 해킹해 사생활을 침해하는 등의 여러 사건이 발생하고 있다. IP 카메라 1800여 대를 해킹하고 1만 665 차례 접속해 남의 사생활을 훔쳐 본 40대 남성에게 징역 1년이 선고된 바 있다. IoT 보안 우려가 커지고 있는 반면 해킹 범죄 사범 검거율은 감소하고 있다.

<'오징어게임'인 줄 알았는데 스파이웨어…악성코드급증 (hani.co.kr)>

피씨(PC), 스마트폰뿐만 아니라 가정용 공유기, 월패드 등 사물인터넷(IoT) 기기들도 공격 대상이 되면서 악성코드 적발 사례도 빠르게 늘고 있다. 정상적인 프로그램이나 인기 콘텐츠 등으로 위장된 스파이웨어들도 많이 발견되고 있다. 사물인터넷 대상 악성코드인 모지(moji) 유포지의 적발 건수가 이 기간 30% 늘었다. 모지는 가정용 공유기·월패드·폐회로 티비(CCTV) 등을 감염시켜 다른 서버나 피시로 악성코드를 퍼뜨리는데 '경유지'로 삼는다. 가정용 공유기부터 스마트홈 월패드까지 생활의 모든 것이 인터넷으로 연결되면서 이를 노리는 사이버 공격이 크게 증가하고 있다. 기기 사용자는 기본 제공 비밀번호 변경, 소프트웨어 최신 버전 업데이트 등의 보안 수칙을 준수해 감염 피해를 예방할 수 있다고 한다.

프로젝트 개요

S e c u l o T - D U C K

1.1. 팀 소개

1.2. 프로젝트 소개 및 목표

1.3. 문제 정의 및 개발 이유

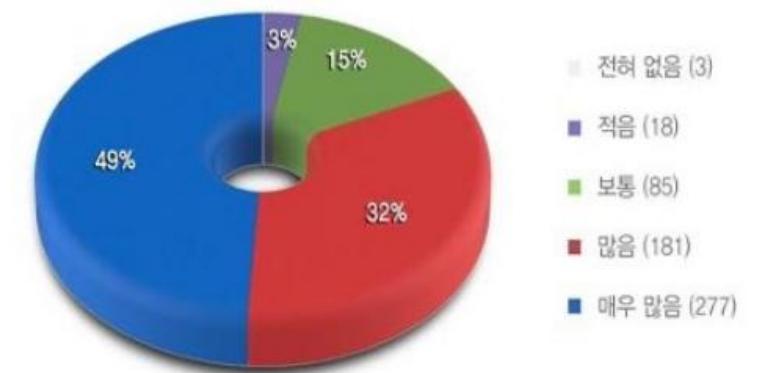
근거 기사 자료 - 보안 분야 관심도

<상위 30위권 대학 '사이버보안학과' 학종 경쟁률 및 등급컷 순위 - 에듀진 (edujin.co.kr)>

2024학년도 경쟁률이 가장 높은 대학은 가천대 글로벌 스마트보안학과로 43.17대1을 기록했으며, 숭실대 정보보호학과 19.25대1, 중앙대 CAU 탐구형 인재 산업보안학과 17.17대1등 순으로 경쟁률이 높았다. 전년대비 경쟁률이 상승한 대학은 가천대 스마트보안학과로 2023 경쟁률 21대1에서 2024 경쟁률 43.17대1로 22.17p 큰 폭 상승했다.

<보안 관심 일반인 92% "사용중인 IoT기기 보안우려" - ZDNet Korea>

보안에 관심 있는 일반인 가운데 92%는 사용하고 있는 사물인터넷 기기에서 언젠가 보안 문제가 생길 것으로 예상한다는 조사 결과가 나왔다. 한국 인터넷 진흥원(KISA)이 일반인 564명 대상으로 진행한 IoT 기기 보안 위협 인식도 설문조사 분석 내용 일부다. 실생활에서 개인이 IoT 기기 보안에 얼마나 관심을 갖고 위협에 대처하는지 알아보고 대처하기 위한 의견을 수렴한다는 취지였다. 설문은 IoT 기기 사용 현황 및 IoT 보안 인식도, 안전한 IoT 기기 사용을 위한 활동 현황과 보안 위협 체감 정도, 안전한 IoT 기기 사용을 위한 활동 현황과 보안 위협 체감도, 3개 범주 9개 항목으로 구성됐고 564명이 응답했다.



일반적인 사이버보안 관심도를 '전혀없음, 적음, 보통, 많음, 매우많음'으로 묻는 항목에 '많음'과 '매우많음'이라 답한 응답자가 458명(81%)이었다. '전혀없음' 응답자는 3명(0%)이었다. 이 조사 응답은 주로 "사이버보안에 최소한의 관심이 있는 사람" 기준이라 보는 게 적절하다는 얘기다.



응답자 86%는 실생활에 1~5개 IoT 기기를 사용 중이었다. 응답자의 IoT 기기 활용도는 유형별 편차가 커다. 최다 활용 품목은 403명(71%)이 쓰는 '가정용 인터넷 공유기'였다. 그리고 '도어락(출입문)' 314명(55%), '스마트 가전(에어컨, 세탁기, 냉장고)' 192명(34%), '인공지능 스피커' 158명(28%), '스마트 밴드' 128명(22%) 순으로 사용 중이라고 답했다.

프로젝트 개요

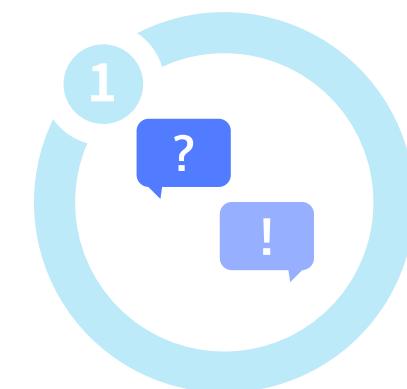
S e c u l o T - D U C K

1.1. 팀 소개

1.2. 프로젝트 소개 및 목표

1.3. 문제 정의 및 개발 이유

개발 이유



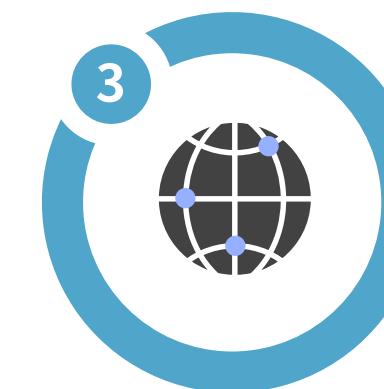
보안 위협에 대한 실질적인 대응

AI 기반의 위협도 예측 및
보안 소프트웨어 추천



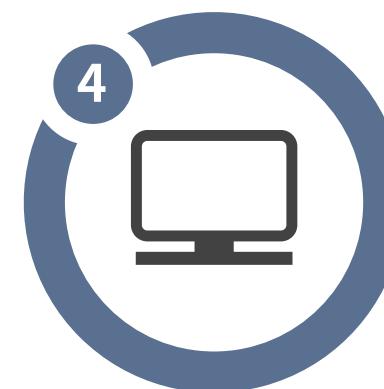
보안 솔루션의 접근성 향상

사용자 친화적 인터페이스와
챗봇 기능을 통한 손쉬운 사용



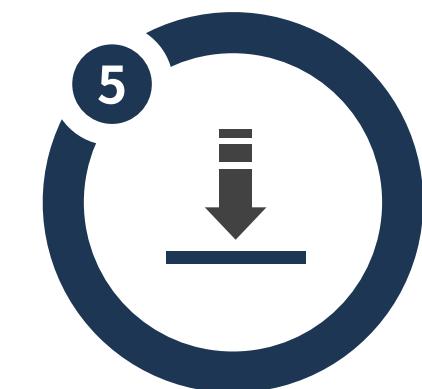
보안 인식 제고

보안 인식 교육 및 정보 제공



데이터 기반의 맞춤형 보안

데이터 기반의 정확한
보안 분석 및 추천



시장 경쟁력 확보

차별화된 보안 솔루션 모음
제공으로 시장 경쟁력 강화

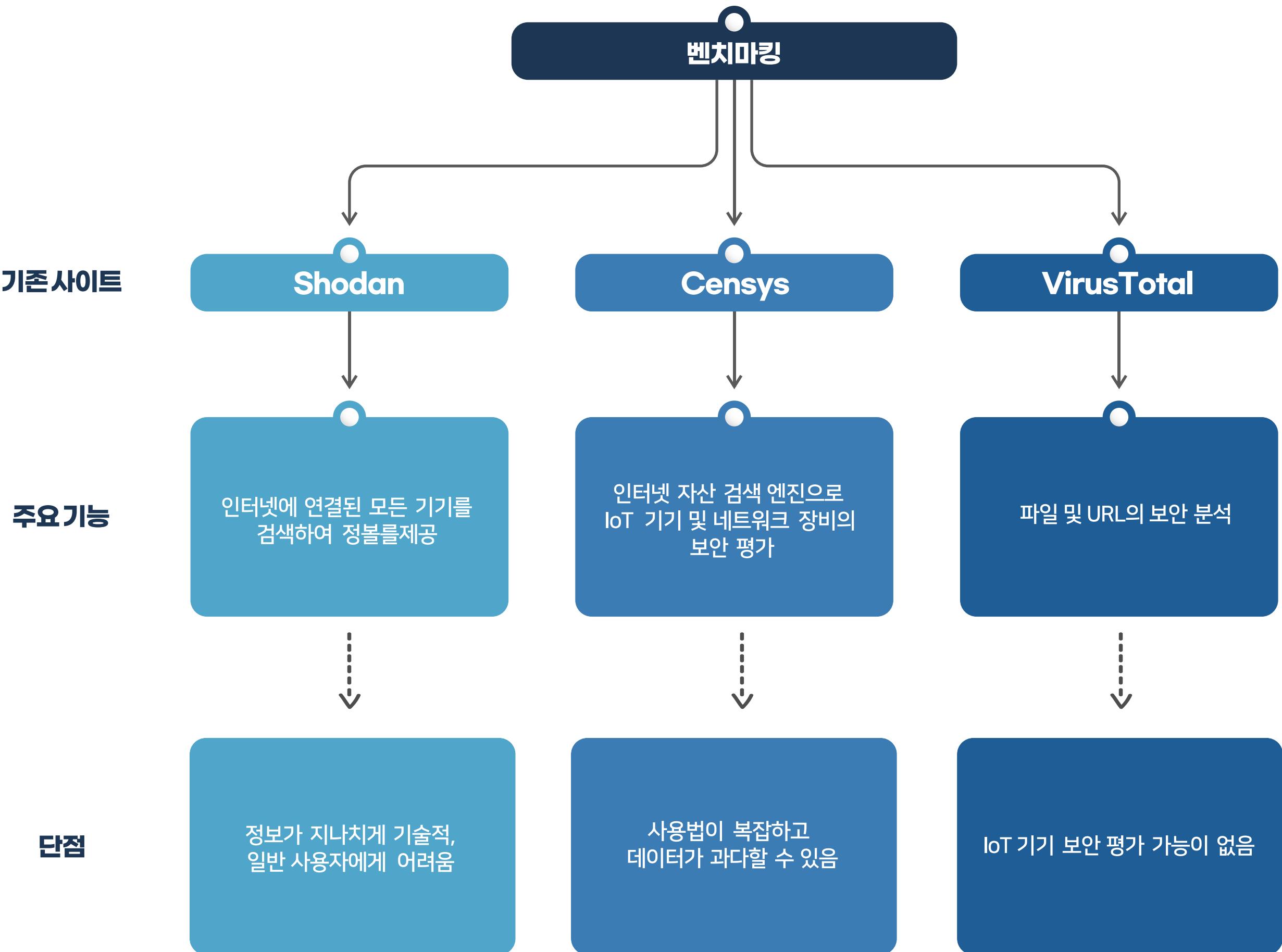
분석 및 전략

S e c u l o t - D U C K

2.1. 벤치마킹 및 차별성

2.2. SWOT 분석

2.3. 페르소나



분석 및 전략

S E C U L O T - D U C K

2.1. 벤치마킹 및 차별성

2.2. SWOT 분석

2.3. 페르소나



1. 중앙 집중형 보안 소프트웨어 제공

다양한 보안 오픈 소스를 한 곳에서 쉽게
검색하고 접근 가능할 수 있도록 한다.



2. 간단한 IoT 기기 위험도 평가

인공지능 기반의 IoT 기기 위험도 평가 기능을 제공한다.
비전문가도 쉽게 이해할 수 있는 점수, 구간을 제공한다.



3. 사용자 친화적 인터페이스

복잡한 기술 용어 대신 사용자가 쉽게 이해할 수
있는 용어와 평가 기준을 제공한다.



분석 및 전략

S e c u l o T - D U C K

2.1. 벤치마킹 및 차별성

2.2. SWOT 분석

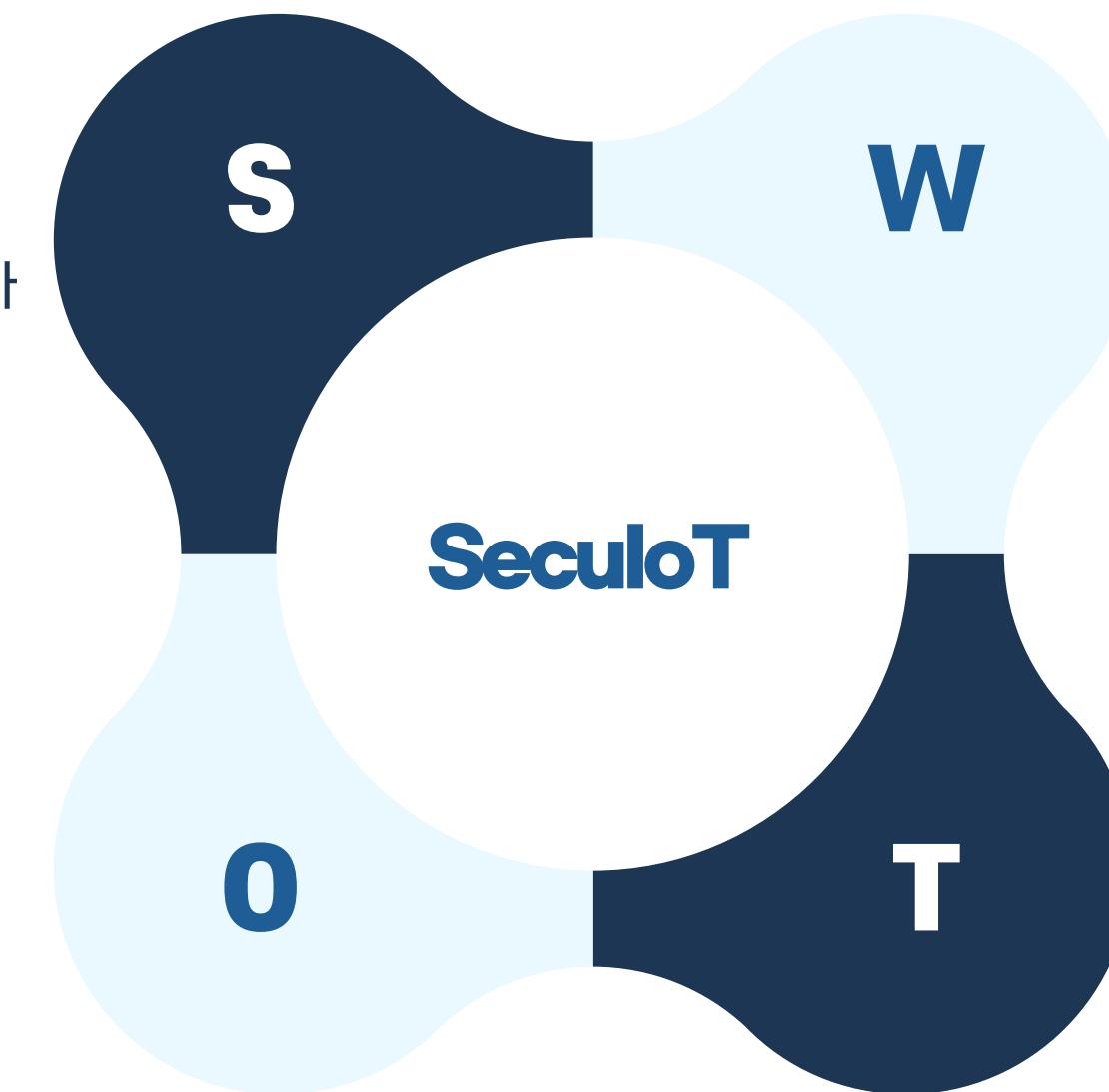
2.3. 페르소나

강점

- 다양한 보안 오픈 소스 제공
- 직관적인 IoT 기기 위험도 평가
- 사용자 친화적 인터페이스

기회

- IoT 기기의 보급 확산
- 보안 인식의 증가
- 사용자 데이터 기반 서비스 확장 가능



약점

- 초기 사용자 기반 부족
- 인공지능 모델의 학습 데이터 제한
- 기술적 지원 필요

위협

- 기존 대형 보안 플랫폼
- 신종 보안 위협의 출현
- 법적 규제 강화

분석 및 전략

S e c u l o T - D U C K

2.1. 벤치마킹 및 차별성

2.2. SWOT 분석

2.3. 페르소나



이름: 김안심

나이: 32세

직업: 마케팅 기획자

배경: 스마트홈 IoT 기기(스마트 조명, 보안 카메라 등)를 자주 사용하는 일반 사용자로, 보안에 대한 지식이나 인식이 높지 않음

목표: 자신이 사용하는 IoT 기기가 안전하게 보호되는지 알고 싶고, 보안에 관심이 생겨 여러 가지를 찾고 공부해보고 싶음, 필요할 경우 간단히 조치할 수 있는 방법을 찾고자 함

고민: 보안이 중요하다는 건 알지만, 구체적으로 어떤 점이 위험한지 모르고, 업데이트나 설정이 어렵다고 느껴 보안 관련 작업을 미루는 경향이 있음.

행동 패턴: 모바일을 통해 간단히 보안 위험 상태를 확인하고 해결 방법을 찾는 데에 관심이 많음.

니즈: 직관적이고 이해하기 쉬운 UI/UX, 보안 상태를 시각적으로 보여주는 위험도 점수, 필요한 경우 바로 관련있는 보안 소프트웨어를 찾을 수 있기 원함



이름: 윤성재

나이: 40세

직업: 중소기업 IT 관리자

배경: 중소기업에서 네트워크 및 장비 보안을 담당하고 있으며, 회사 내 여러 IoT 장비의 보안 위험 관리가 주요 업무 중 하나임

목표: 각 IoT 기기의 보안 상태를 쉽게 모니터링하고, 발견된 위험 요소에 대해 적절한 대처 방안을 신속히 적용하는 것

고민: 보안 도구와 관련 정보를 얻기 위해 많은 시간을 할애하며, 일부 보안 소프트웨어가 비싸고 설치 과정이 복잡하여 작업에 부담이 되고, 매번 여러 사이트를 검색해 들어가기 힘듦

행동 패턴: 실시간으로 위험도를 모니터링할 수 있는 기능과 보안 대책을 쉽게 찾아 적용할 수 있는 접근성을 중시함

니즈: 통합 대시보드에서 보안 위험도 점수를 확인하고, 적절한 오픈 소스 보안 소프트웨어를 추천 받는 기능, 챗봇을 통해 보안 관련 질의에 대한 즉각적 답변을 받길 원함

분석 및 전략

S e c u l o T - D U C K

2.1. 벤치마킹 및 차별성

2.2. SWOT 분석

2.3. 페르소나



이름: 한미래

나이: 28세

직업: 보안 전공 대학생

배경: IoT 보안과 관련한 학문적 연구를 진행 중이며, 최신 보안 위협과 오픈 소스 보안 소프트웨어에 관심이 많음

목표: 연구에 필요한 보안 오픈 소스를 얻고, IoT 기기의 최신 보안 위험과 취약점을 학습하여 연구에 활용

고민: 여러 보안 소스와 위험 데이터를 수집하기 어렵고, 최신 보안 트렌드에 대한 정보를 항상 추적하는 데 어려움이 있음

행동 패턴: 다양한 오픈 소스 보안 소프트웨어를 실험해 보고, 보안 취약점 데이터 등을 활용하려 함

니즈: 보안 연구에 도움이 되는 상세 데이터 제공, 고급 사용자를 위한 보안 위험도 세부 정보, 최신 오픈 소스 보안 소프트웨어 접근성

디자인 및 아키텍쳐

S e c u r i o T - D U C K

3.1. 디자인 개요

3.2. 프로토타입

3.3. 워크플로우

3.4. 진행 현황

메인 색상



06192B

서브 색상

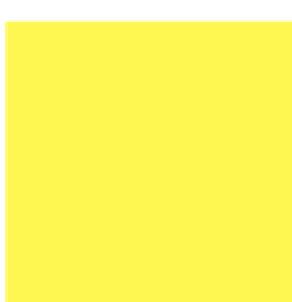


5A7093

위험도 평가 단계 색상



FF0000



FFF500



1D3653



7CACF8



FFFFFFFF



DDE1E9



0085FF

03

디자인 및 아키텍쳐

S e c u l o T - D U C K

3.1. 디자인 개요

3.2. 프로토타입

3.3. 워크플로우

3.4. 진행 현황



<메인 페이지>

DUCK

Safety Assessment Dash Board Security Toolkit Chatbot Community Sign Login

IP Risk Assessment

IP 위험도 측정

제공되는 IoT 기기와 서비스를 평가하고, 보안 강화를 위한 조치를 제시합니다.

IP 위험도 측정하기 가기

사용하는 IoT 장치의 안전을 증명하기 위한 시스템입니다.

사용 중인 IoT 장치의 기기과 통신서를 통해, 현재 장치의 IP 주소가 인터넷에 연결되었는지 여부를 확인합니다.

IP 위험도 측정하기 가기 IP 위험도 측정 목록보기

DUCK

IP 위험도를 측정하여 보안을 강화하는 오픈 키트

IP 위험도 측정, 위험 목록 파악, 차단 기록 분석

이러 오픈 소스를 한번에 간편하게

Chatbot 주선 시스템으로 쉽게

커뮤니티로 실시간으로 재밌게

address: Seoul, Korea City, Gyeonggi-do, Yongin-si, Gyeonggi-dong
e-mail: info@duck-project.org
Phone: 010-1234-5678

<Safety Assessment>

SeculoT

Safety Assessment Dash Board Security Toolkit Chatbot

인증된 장치의 안전성을 평가하는 시스템입니다.

Safety Assessment

기기 이름을 입력해주세요

통신사를 입력해주세요

미동록 장치일 경우 부정확한 점수가 예측될 수 있습니다.

완료

SeculoT

Safety Assessment Dash Board Security Toolkit Chatbot

IoT 기기 위험도 평가 - 기기 정보 입력창

lighttpd SK Telecom

Risk Score 4

매우 안전합니다.

IoT 기기 위험도 평가 - 위험도 평가 단계

03

디자인 및 아키텍쳐

S e c u l o T - D U C K

3.1. 디자인 개요

3.2. 프로토타입

3.3. 워크플로우

3.4. 진행 현황



<로그인>

SeculoT Safety Assessment Dash Board Security Toolkit Chatbot Sign Login

LOGIN

Email

Password

Login

Find Password | Sign Up

<회원가입>

SeculoT Safety Assessment Dash Board Security Toolkit Chatbot Sign Login

Sign UP

Welcome to Duck right now

Name

이름을 입력해주세요.

Password

비밀번호 입력해주세요.

Confirm Password

비밀번호를 한번더 입력 해주세요.

E-mail

이메일 입력해주세요.

By checking this box, you agree to our Terms & Conditions and Privacy Policy, which includes consenting to how we handle your information

Create Account

<비밀번호 찾기>

SeculoT Safety Assessment Dash Board Security Toolkit Chatbot Sign Login

Find Password

E-mail

이메일 입력해주세요.

Send Reset Email

03

디자인 및 아키텍쳐

S e c u l o T - D U C K

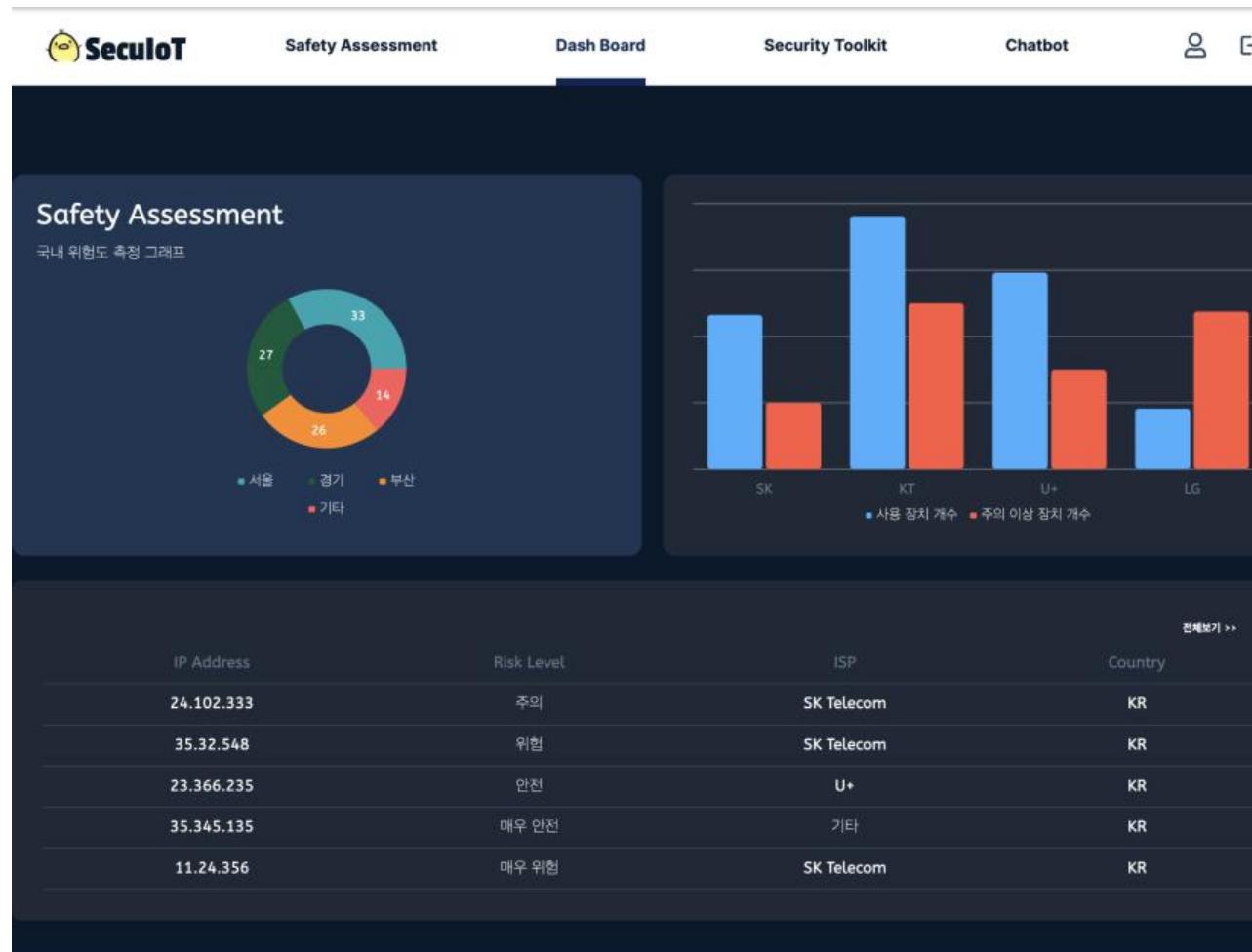
3.1. 디자인 개요

3.2. 프로토타입

3.3. 워크플로우

3.4. 진행 현황

<Dash Board>



<보안 키트 중 네트워크 분석 -> Wireshark>

The Security Toolkit interface shows the 'Wireshark' tool selected under '네트워크 분석'.

Wireshark
<https://www.wireshark.org>

네트워크 패킷을 캡처하고 분석하는 가장 인기 있는 도구입니다.
 다양한 프로토콜을 지원하며 사용자 친화적인 GUI를 제공합니다.
 다양한 상황에서 활용할 수 있습니다.

Wireshark

 WIRESHARK

Wireshark는 네트워크 트래픽을 분석하는 강력한 도구로서,
 일반 사용자들도 네트워크 문제 해결이나 보안 감시, 네트워크 성능 개선 등
 다양한 상황에서 활용할 수 있습니다.

<보안 도구 키트 메뉴창>

The menu bar includes: SeculoT, Safety Assessment, Dash Board, Security Toolkit (selected), Chatbot, and User/Logout.

The 'Security Toolkit' menu contains several sub-sections:

- 보안 분석 도구**
 - 네트워크 분석
 - Wireshark
 - TCPdump
 - Zeek
 - Suricata
 - Moloch
 - 시스템 분석
 - 웹 애플리케이션 분석
- 취약점 스캐닝 도구**
 - 정적 분석 도구
 - 동적 분석 도구
- 보안 강화 도구**
 - 방화벽 설정 도구
 - 암호화 도구
 - 악성 코드 분석 도구
- 시스템 모니터링 도구**
 - 로그 도구
 - 침입 탐지 시스템
 - 시스템 모니터링
- 교육 및 인식 증진 도구**
 - 보안 교육 플랫폼
 - 시스템
 - 웹분석

03

디자인 및 아키텍쳐

S e c u l o T - D U C K

3.1. 디자인 개요

3.2. 프로토타입

3.3. 워크플로우

3.4. 진행 현황



<마이페이지>

Device 1

Risk Score: 4 (VERY SAFE)

Lighttpd, SK Telecom, 2024. 10. 29.

즐겨찾기 목록

- 보안 분석 도구: TCPdump
- 취약점 스캔 도구: 즐겨찾기한 도구가 없습니다.
- 보안 강화 도구: Uncomplicated Firewall(UFW)
OpenSSL, VirusTotal
- 시스템 모니터링 도구: OSSEC
Snort
- 교육 및 인식 증진 도구: 즐겨찾기한 도구가 없습니다.

<장치 전체보기>

나의 디바이스

나의 기종을 관리할 수 있습니다.

Device 1

Device 2

Lighttpd, SK Telecom, Risk Score: 4 (VERY SAFE)

<챗봇>

DUKBOT

새로운 채팅

DUKBOT, 2024. 10. 29.
네트워크 관련 도구 있어?

DUKBOT, 2024. 10. 29.
네트워크 취약점 스캐너 추천해줘

DUKBOT, 2024. 10. 29.
네트워크 트래픽 관련 도구 추천해줘

DUKBOT, 2024. 10. 29.
네트워크 트래픽 도구 추천해줘~

사용자 : 네트워크 관련 도구 있어?

DUKBOT : Wireshark

네트워크 패킷을 캡처하고 분석하는 가장 인기 있는 도구입니다. 다양한 프로토콜을 지원하며 사용자 친화적인 GUI를 제공합니다. 네트워크 문제 해결 및 보안 분석에 유용합니다.

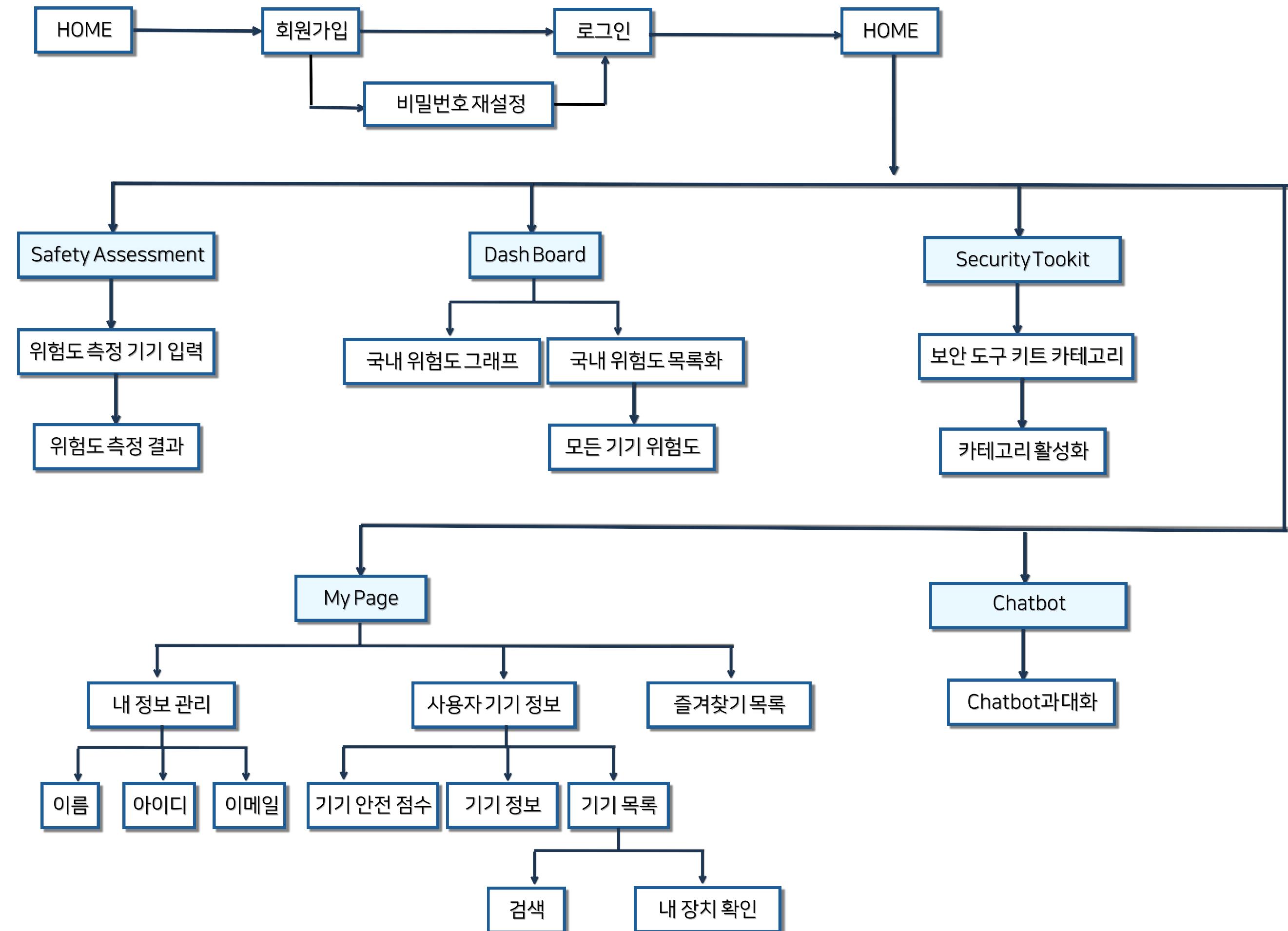
네트워크 관련 도구 있어?

3.1. 디자인 개요

3.2. 프로토타입

3.3. 워크플로우

3.4. 진행 현황



디자인 및 아키텍쳐

S e c u r i o T - D U C K

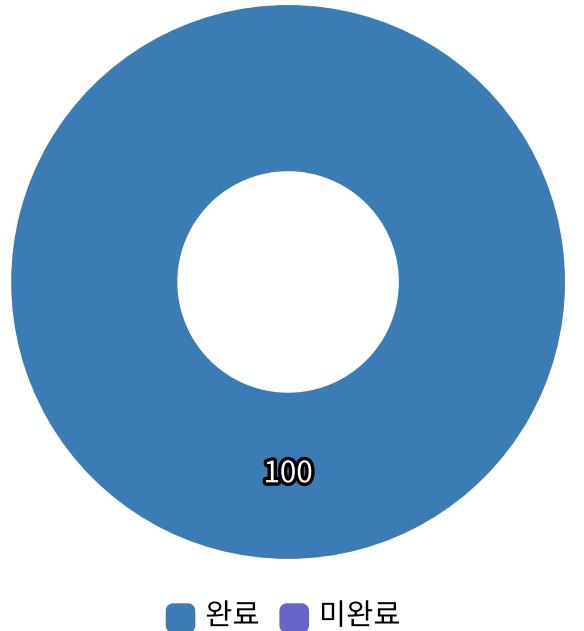
3.1. 디자인 개요

3.2. 프로토타입

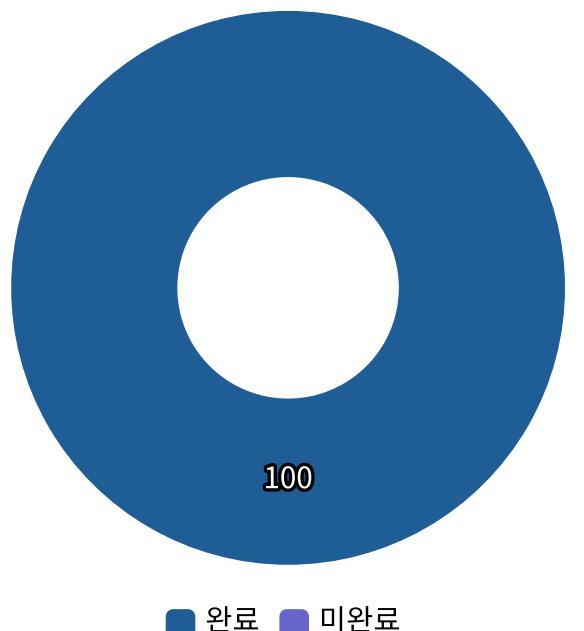
3.3. 워크플로우

3.4. 진행 현황

디자인



개발



기능	현황
회원가입	100%
로그인	100%
비밀번호 찾기	100%
메인 페이지	100%
메뉴바	100%
대시보드	100%
보안 도구 상태창	100%
보안 도구 페이지(들)	100%
즐겨찾기 관리 및 조회	100%
내 장치 기록 관리 및 조회	100%
чат봇	100%

4.1. 개발 환경 및 언어

4.2. 데이터베이스 설계

4.2.1. E-R 다이어그램

4.2.2. 테이블 정의서

4.2.3. 모듈 현황



개발 환경 및 기술

S e c u r i o T - D U C K

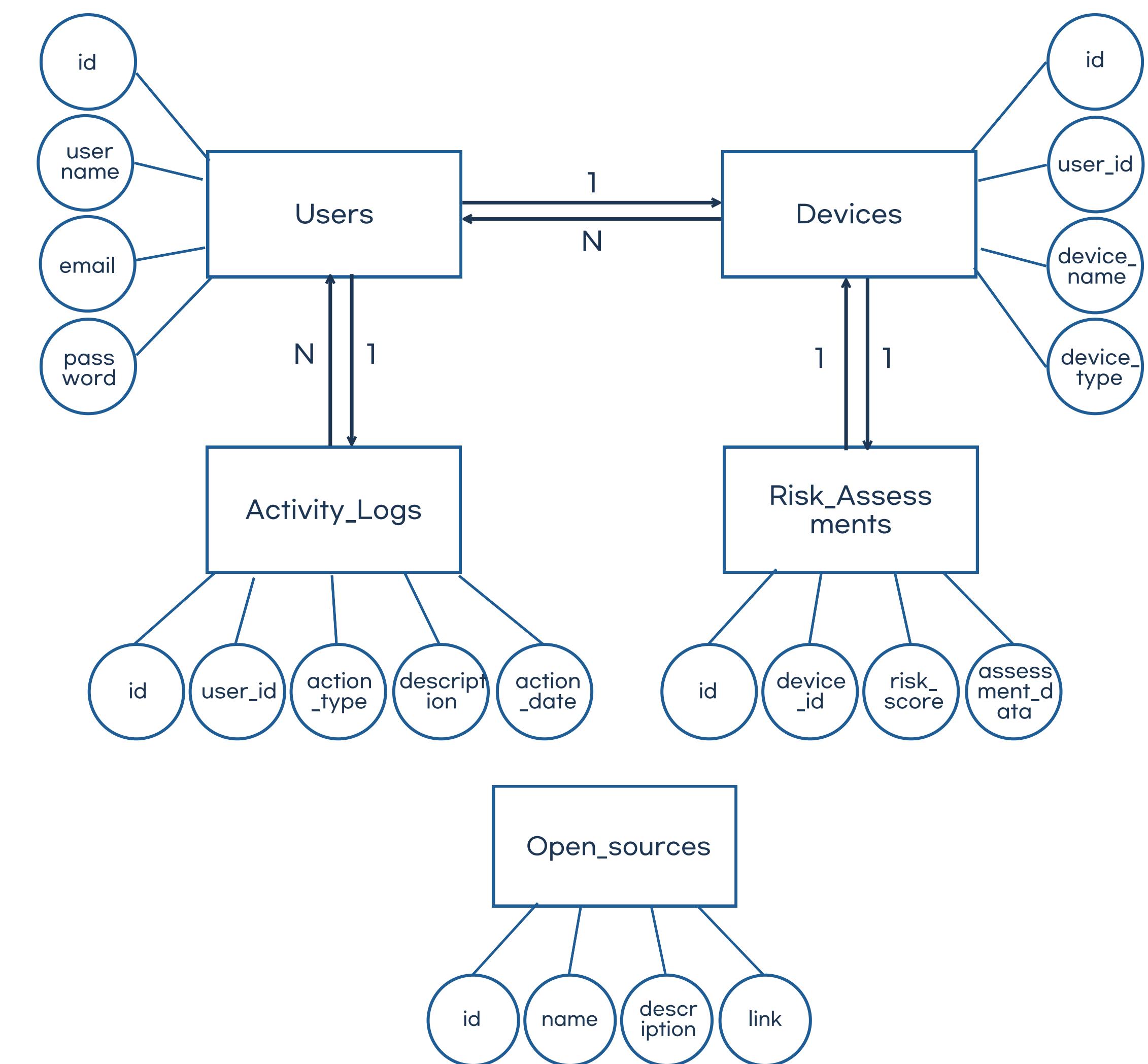
4.1. 개발 환경 및 언어

4.2. 데이터베이스 설계

4.2.1. E-R 다이어그램

4.2.2. 테이블 정의서

4.2.3. 모듈 현황



개발 환경 및 기술

S e c u r o T - D U C K

4.1. 개발 환경 및 언어

4.2. 데이터베이스 설계

4.2.1. E-R 다이어그램

4.2.2. 테이블 정의서

4.2.3. 모듈 현황

컬렉션 이름	필드 이름	데이터 타입	설명
users	id	String	사용자 고유 ID
	username	String	사용자 이름
	email	String	이메일 주소
	password	String	비밀번호
	createdAt	Timestamp	생성 일자

컬렉션 이름	필드 이름	데이터 타입	설명
devices	id	String	장치 고유 ID
	userId	String	사용자 ID
	deviceName	String	장치 이름
	deviceType	String	장치 유형
	createdAt	Timestamp	생성 일자

04

개발 환경 및 기술

S e c u r i o T - D U C K

4.1. 개발 환경 및 언어

4.2. 데이터베이스 설계

4.2.1. E-R 다이어그램

4.2.2. 테이블 정의서

4.2.3. 모듈 현황

컬렉션 이름	필드 이름	데이터 타입	설명
risl_assessments	id	String	위험도 평가 고유 ID
	deviceID	String	장치 ID
	riskScore	Number	위험도 점수
	assessmentData	TimeStamp	평가 일자

컬렉션 이름	필드 이름	데이터 타입	설명
open_sources	id	String	오픈 소스 고유 ID
	name	String	소프트웨어 이름
	description	String	설명
	link	String	웹 링크

컬렉션 이름	필드 이름	데이터 타입	설명
activity_logs	id	String	활동 로그 고유 ID
	userId	String	사용자 ID
	actionType	String	활동 유형
	description	String	설명
	actionData	Timestamp	활동 일자

개발 환경 및 기술

S e c u r i o T - D U C K

4.1. 개발 환경 및 언어

4.2. 데이터베이스 설계

4.2.1. E-R 다이어그램

4.2.2. 테이블 정의서

4.2.3. 모듈 현황

모듈	기능	사용 기술	관련 API
사용자 관리 모듈	사용자 등록, 로그인, 비밀번호 재설정, 프로필 관리	Supabase의 Authentication과 Database 기능	사용자 생성, 정보 업데이트, 비밀번호 재설정
장치 관리 모듈	IoT 장치 추가, 정보 수정, 목록 조회	Supabase의 Authentication과 Database 기능	장치 등록, 정보 수정, 목록 조회
위험도 평가 모듈	위험도 예측, 평가 결과 저장, 기록 조회	Python, upabase Functions, Supabase의 Postgres	위험도 예측, 결과 저장, 기록 조회
보안 오픈 소스 모듈	보안 오픈 소스 등록, 설명 및 링크 관리	Supabase의 Authentication과 Database 기능	오픈 소스 등록, 정보 수정, 목록 조회
활동 로그 모듈	사용자 활동 로그 기록, 활동 내역 조회	Supabase의 Authentication과 Database 기능	로그 기록, 내역 조회
챗봇 모듈	간단한 질의응답, 보안 오픈 소스 추천 지원	Supabase Database와 연결	질문 처리, 응답 생성, 추천 오픈 소스 안내

모듈 간 관계

사용자 관리 모듈 - 장치 관리 모듈: 사용자가 자신의 IoT 장치를 추가 및 관리

장치 관리 모듈 - 위험도 평가 모듈: 각 장치의 보안 위험도 평가 결과를 기록하고 조회

보안 오픈 소스 모듈 - 챗봇 모듈: 사용자가 필요로 하는 보안 도구를 제공, 질의응답을 통해 챗봇 모듈과 연동

활동 로그 모듈 - 전체 모듈: 사용자의 주요 활동을 기록, 모든 모듈과 연동하여 변경 사항 및 액션을 기록

5.1. AI 모델 설명

5.1.1. 모델 개요

5.1.2. 데이터 수집

5.1.3. 데이터셋 설명

5.1.4. 모델 선택

5.2. 점수 예측 알고리즘

5.2.1. 위험도 구간 설정

5.2.2. 알고리즘 구현

5.2.3. 모델 성능 개선

모델 개요



IoT 기기 보안 위험도 예측 모델은 기계 학습 알고리즘을 사용하여 IoT 기기의 보안 위험도를 평가하고 예측한다.

이 모델은 제품 이름과 ISP 정보를 기반으로 보안 점수를 산출하며, 사용자는 이를 통해 기기의 보안 상태를 쉽게 파악할 수 있다.

목표

01

IoT 기기의 보안 위험도를 정량적으로 평가

02

사용자에게 기기의 보안 상태를 시각적으로 제공

03

위험도를 예측하여 적절한 보안 조치를 권장

5.1. AI 모델 설명

5.1.1. 모델 개요

5.1.2. 데이터 수집

5.1.3. 데이터셋 설명

5.1.4. 모델 선택

5.2. 점수 예측 알고리즘

5.2.1. 위험도 구간 설정

5.2.2. 알고리즘 구현

5.2.3. 모델 성능 개선

단계	스크립트	설명	출력 데이터	출력 예시
Shodan 데이터 수집	Shodan_IoTKR.py	Shodan API를 통해 한국의 IoT 기기 정보만 수집	iot_kr.json	{"ip": "192.168.1.1", "port": 80, "device": "Smart Camera"}
IP 주소 추출	Shodan_IP.py	Shodan에서 수집된 데이터로부터 IP 주소만 추출	ip_addresses.txt	192.168.1.1
AbuseIPDB 데이터	AbuseIPDB_IP.py	AbuseIPDB API를 통해 추출한 IP주소의 신고 횟수 및 심각도 정보 수집	merged_reports.json	{"ip": "192.168.1.1", "abuse_count": 10, "severity": "high"}
CVSS 평균 계산	Shodan_cvss.py	Shodan에서 CVSS 평균을 계산하여 IP 주소 별로 저장	ip_with_avg_cvss.txt	192.168.1.1: 6.7
CVE 데이터 수집	Shodan_cve.py	Shodan에서 CVE 정보 수집 및 IP 주소별 CVE 개수 출력	cve_count.json	{"ip": "192.168.1.1", "cve_count": 5}
CVE 연도별 점수	cve_years_score.py	CVE 정보의 연도별 점수 부여 및 계산	initial_cve_years_score.json(1차), cve_years_score.json(2차)	{"ip": "192.168.1.1", "2019": 7.8, "2020": 6.5}
종합 점수 측정	get_total_score.py	수집한 데이터 점수 부여, 종합 보안 점수 계산	ip_with_total_scores.txt	192.168.1.1: 12.5
데이터 합본	new_excel.py	최종 데이터를 합본하여 Excel 파일로 저장	combined_data.xlsx	IP, Total Score, Product, ISP, CVE Count, AVG CVSS, Reported Times, Abuse Confidence Score, Initial CVE Score 데이터
위험도 예측 코드	predict_AI.py	AI 모델을 사용하여 IoT 기기 위험도 예측		def predict_risk(product, isp): ...
오차 확인	AI_test.py	예측 모델의 오차를 확인하고 검증		

5.1. AI 모델 설명

5.1.1. 모델 개요

5.1.2. 데이터 수집

5.1.3. 데이터셋 설명

5.1.4. 모델 선택

5.2. 점수 예측 알고리즘

5.2.1. 위험도 구간 설정

5.2.2. 알고리즘 구현

5.2.3. 모델 성능 개선

데이터셋

속성명	설명	목표 변수	예시
Product	IoT 기기의 제품 이름	특징 변수	lighttpd
ISP	기기가 연결된 인터넷 서비스 제공자	특징 변수	SK Telecom
Total Score	기기의 종합 보안 위험도 점수	목표 변수	22

- **특징:** 제품 이름, ISP 정보, 보안 점수로 구성
- **총 데이터 포인트:** 1000개 이상의 샘플
- **데이터 소스:** Shodan, AbuseIPDB, CVSS 점수, CVE 등

5.1. AI 모델 설명

5.1.1. 모델 개요

5.1.2. 데이터 수집

5.1.3. 데이터셋 설명

5.1.4. 모델 선택

5.2. 점수 예측 알고리즘

5.2.1. 위험도 구간 설정

5.2.2. 알고리즘 구현

5.2.3. 모델 성능 개선

선형 회귀 모델



5.1. AI 모델 설명

5.1.1. 모델 개요

5.1.2. 데이터 수집

5.1.3. 데이터셋 설명

5.1.4. 모델 선택

5.2. 점수 예측 알고리즘

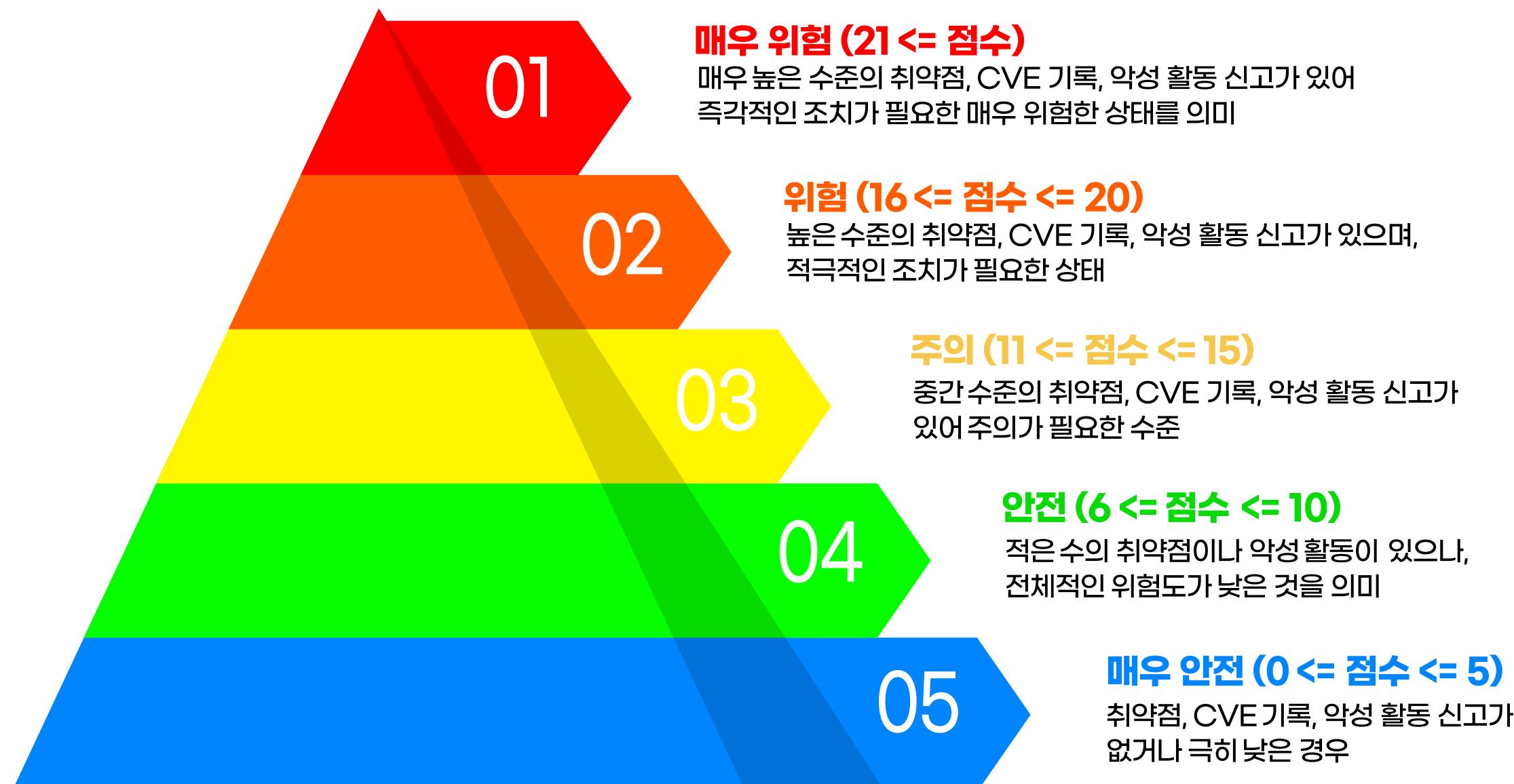
5.2.1. 위험도 구간 설정

5.2.2. 알고리즘 구현

5.2.3. 모델 성능 개선

위험도 구간 5단계

예측된 점수를 기반으로 위험도 구간을 분류하여 사용자가 쉽게 이해할 수 있도록 5단계로 나눔



5.1. AI 모델 설명

5.1.1. 모델 개요

5.1.2. 데이터 수집

5.1.3. 데이터셋 설명

5.1.4. 모델 선택

5.2. 점수 예측 알고리즘

5.2.1. 위험도 구간 설정

5.2.2. 알고리즘 구현

5.2.3. 모델 성능 개선

선형 회귀 모델 구성

입력값: 제품 이름 / ISP

출력값: 예측된 위험도 점수 / 위험도 구간

기기명과 통신사 정보를 입력값으로 받아 위험도 점수를 예측한다.

각 입력 데이터가 보안에 미치는 영향을 수치화하여 선형 방정식 형태로 모델링한다.

훈련 과정

수집된 다양한 데이터를 각각 정규화한 후, 각 데이터의 특성에 따라 구간을 나누고 일정 점수를 부여한다.

이렇게 생성된 점수들을 종합하여 최종 위험도 점수를 계산하고, 이를 바탕으로 예측을 진행한다.

모델의 예측 방식

모델은 학습된 가중치와 절편을 활용해 입력 데이터의 위험도를 계산한다.

예측된 값은 최종 위험도 점수로 환산되어 사용자에게 제공된다.

예측 결과 구간 매핑

예측된 위험도 점수는 미리 정의된 5단계 위험도 구간(매우 안전, 안전, 주의, 위험, 매우 위험)으로 매핑되어 사용자가 쉽게 이해할 수 있도록 한다.

5.1. AI 모델 설명

 5.1.1. 모델 개요

 5.1.2. 데이터 수집

 5.1.3. 데이터셋 설명

 5.1.4. 모델 선택

5.2. 점수 예측 알고리즘

 5.2.1. 위험도 구간 설정

 5.2.2. 알고리즘 구현

 5.2.3. 모델 성능 개선

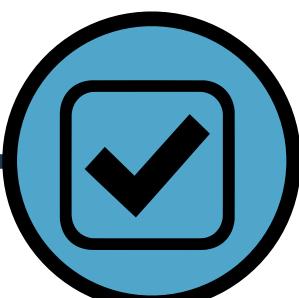
특징 선택

모델에 가장 유의미한 변수를 선택하여
모델의 복잡성을 줄이고 성능을 향상시킨다.
과적합을 방지하고 예측력을 높이도록 한다.

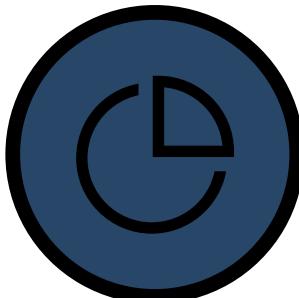


교차 검증

다양한 하이퍼파라미터 설정을 통해 모델
성능을 최적화한다. 이는 학습 데이터의 다양한
분할을 통해 모델의 일반화 성능을 평가한다.



모델 조정



학습률과 정규화 파라미터 등의 조정을 통해
모델의 예측 정확도를 최적화한다.
모델의 학습 과정을 안정화하고 최종 예측
성능을 향상시키는 데 기여한다.

기능 설명

SeculoT - D U C K

6.1. 주요 기능 개요

6.1.1. 보안 오픈 소스 제공

6.1.2. 즐겨찾기

6.1.3. IoT 기기 위험도 평가

6.1.4. 마이페이지

6.1.4. 챗봇

보안 오픈 소스 제공

Wireshark

<https://www.wireshark.org>

네트워크 패킷을 캡처하고 분석하는 가장 인기 있는 도구입니다.
다양한 프로토콜을 지원하며 사용자 친화적인 GUI를 제공합니다.
다양한 프로토콜을 지원하여 네트워크 문제 해결 및 보안 분석에 유용합니다.

Wireshark는 네트워크 트래픽을 분석하는 강력한 도구로서,
일반 사용자들도 네트워크 문제 해결이나 보안 감시, 네트워크 성능 개선 등
다양한 상황에서 활용할 수 있습니다.

설명	사용자가 다양한 보안 오픈 소스 소프트웨어를 쉽게 찾아볼 수 있도록 도와주는 기능
주요 기능	1. 카테고리별 정리: 보안 도구를 유형별로 분류하여 쉽게 탐색 2. 정보 제공: 기능, 설명, 링크 등을 제공하여 사용자가 선택하는데 도움 3. 즐겨찾기: 사용자가 원하는 도구만 마이페이지에서 확인 가능함
로직	데이터베이스에서 보안 오픈 소스를 가져와 카테고리별로 정리하여 사용자에게 표시 사용자가 검색어를 입력하거나 클릭하면, 해당 키워드와 관련된 오픈 소스를 제공
장점	사용자가 필요로 하는 보안 오픈 소스를 쉽게 찾을 수 있음 다양한 보안 툴에 대한 정보를 제공하여 선택의 폭을 넓힘 신뢰할 수 있는 오픈 소스만 모아서 제공함으로써 보안 강화

기능 설명

S E C U L O T - D U C K

6.1. 주요 기능 개요

6.1.1. 보안 오픈 소스 제공

6.1.2. 즐겨찾기

6.1.3. IoT 기기 위험도 평가

6.1.4. 마이페이지

6.1.4. 챗봇

보안 오픈 소스 종류 (1)

보안분석 도구

네트워크 분석	시스템 분석	웹 어플리케이션 분석
Wireshark	OpenVAS	OWASP ZAP
TCPDump	Nexpose Community Edition	Nikto
Zeek	Nmap	Arachni
Suricate	Vuls	Wapiti
Moloch	OWASP ZAP	Skipfish

취약점 스캐닝 도구

정적 분석 도구	동적 분석 도구
SonarQube	Burp Suite Community Edition
FindBugs	Nikto
Cppcheck	Zed Attack Proxy (ZAP)
Bandit	Arachni
	Golismero

기능 설명

S E C U L O T - D U C K

6.1. 주요 기능 개요

6.1.1. 보안 오픈 소스 제공

6.1.2. 즐겨찾기

6.1.3. IoT 기기 위험도 평가

6.1.4. 마이페이지

6.1.4. 챗봇

보안 오픈 소스 종류 (2)

보안 강화 도구

암호화 도구
OpenSSL
GnuPG
Cryptsetup
VeraCrypt

방화벽 설정 도구
Uncomplicated Firewall (UFW)
Firewall ID
pfSense
IPFire

악성 코드분석 도구
Cuckoo Sandbox
VirusTotal
REMnux
MISP

시스템 모니터링 도구

로그 도구
ELK Stack
Graylog
Fluentd
Logstash
Prometheus
GoAccess

침입 탐지 시스템
Snort
Suricata
OSSEC
Zeek

시스템 모니터링
Prometheus
Grafana
Collectd
Netdata

6.1. 주요 기능 개요

6.1.1. 보안 오픈 소스 제공

6.1.2. 즐겨찾기

6.1.3. IoT 기기 위험도 평가

6.1.4. 마이페이지

6.1.4. 챗봇

보안 오픈 소스 종류 (3)

교육 및 인식 증진 도구

보안 교육 플랫폼	시스템	웹 분석
ELK Stack	OWASP Security Shepherd	OWASP WebGoat
SecurityTub	Damn Vulnerable Linux	Damn Vulnerable Web Application
Safe and Secure Online	OWASP Juice Shop	OWASP Juice Shop
Cyber Aces		
Open Security Training		

6.1. 주요 기능 개요

6.1.1. 보안 오픈 소스 제공

6.1.2. 즐겨찾기

6.1.3. IoT 기기 위험도 평가

6.1.4. 마이페이지

6.1.4. 챗봇



설명	로컬 스토리지를 활용하여 사용자가 원하는 정보를 즐겨찾기에 추가하고 브라우저에서 편리하게 접근할 수 있도록 구현
주요 기능	<ul style="list-style-type: none"> 1. 로컬 스토리지 저장: 사용자가 즐겨찾기 버튼을 클릭할 때, 해당 페이지 정보가 브라우저의 로컬 스토리지에 저장됨 2. 데이터 유지: 동일 브라우저 사용 시 로그인 여부와 관계없이 즐겨찾기 항목 유지 3. 간편한 데이터 접근: 서버와의 통신 없이 빠르게 즐겨찾기 데이터를 불러올 수 있음
로직	<p>데이터 저장: 사용자가 즐겨찾기 버튼을 클릭하면, JavaScript를 사용하여 로컬 스토리지에 JSON 형식으로 데이터 저장</p> <p>데이터 불러오기: 페이지가 로드될 때마다 로컬 스토리지에서 즐겨찾기 데이터를 가져와 화면에 표시</p> <p>삭제 기능: 즐겨찾기 목록에서 항목을 삭제할 때, 해당 데이터를 로컬 스토리지에서 제거</p>
장점	<p>빠른 로딩 속도: 서버 요청 없이 클라이언트 측에서 즉각적인 데이터 접근</p> <p>간편한 확인: 일일이 카테고리를 확인하지 않아도 접근 가능</p>

06 기능 설명

SeculoT - D U C K

6.1. 주요 기능 개요

6.1.1. 보안 오픈 소스 제공

6.1.2. 즐겨찾기

6.1.3. IoT 기기 위험도 평가

6.1.4. 마이페이지

6.1.4. 챗봇

IoT 기기 위험도 평가

The screenshot shows two main sections of the SeculoT platform. On the left, the 'Safety Assessment' section features a large image of a laptop displaying various charts and graphs. It includes input fields for '기기 이름을 입력해주세요' and '통신사를 입력해주세요', and a button labeled '인증'. On the right, the 'Dash Board' section displays a 'Risk Score' of 4, with a status indicator showing 'VERY SAFE'. Below this, there are sections for 'lighttpd' and 'SK Telecom', each with a small icon and a status bar. A legend at the bottom defines risk levels: VERY DANGEROUS (21점 이상), DANGEROUS (16~20점), CAUTION (11~15점), SAFE (6~10점), and VERY SAFE (0~5점). A message at the bottom right says '매우 안전합니다.'

설명	AI 모델을 통해 IoT 기기의 보안 위험도를 예측하는 기능
주요 기능	1. 위험도 점수 예측: 사용자가 입력한 기기 정보를 기반으로 위험도 점수를 예측 2. 위험도 구간 제공: 예측된 점수를 기준으로 5자기 구간으로 나누어 제공 3. 결과 시각화: 점수와 구간을 시각적으로 표시하여 이해를 도움
로직	사용자가 기기 정보 (제품명, ISP)를 입력 입력된 정보를 AI 모델에 전달하여 위험도 점수 예측 예측된 점수를 기준으로 위험도 구간을 설정 예측 결과를 시각적으로 표시하여 사용자에게 제공
장점	사용자는 자신의 기기 보안 상태를 쉽게 파악할 수 있음 위험도 구간을 통해 구체적인 보안 조치가 필요함을 직관적으로 이해할 수 있음 데이터 기반의 보안 평가로 신뢰성 높은 정보를 제공

기능 설명

S E C U L O T - D U C K

6.1. 주요 기능 개요

6.1.1. 보안 오픈 소스 제공

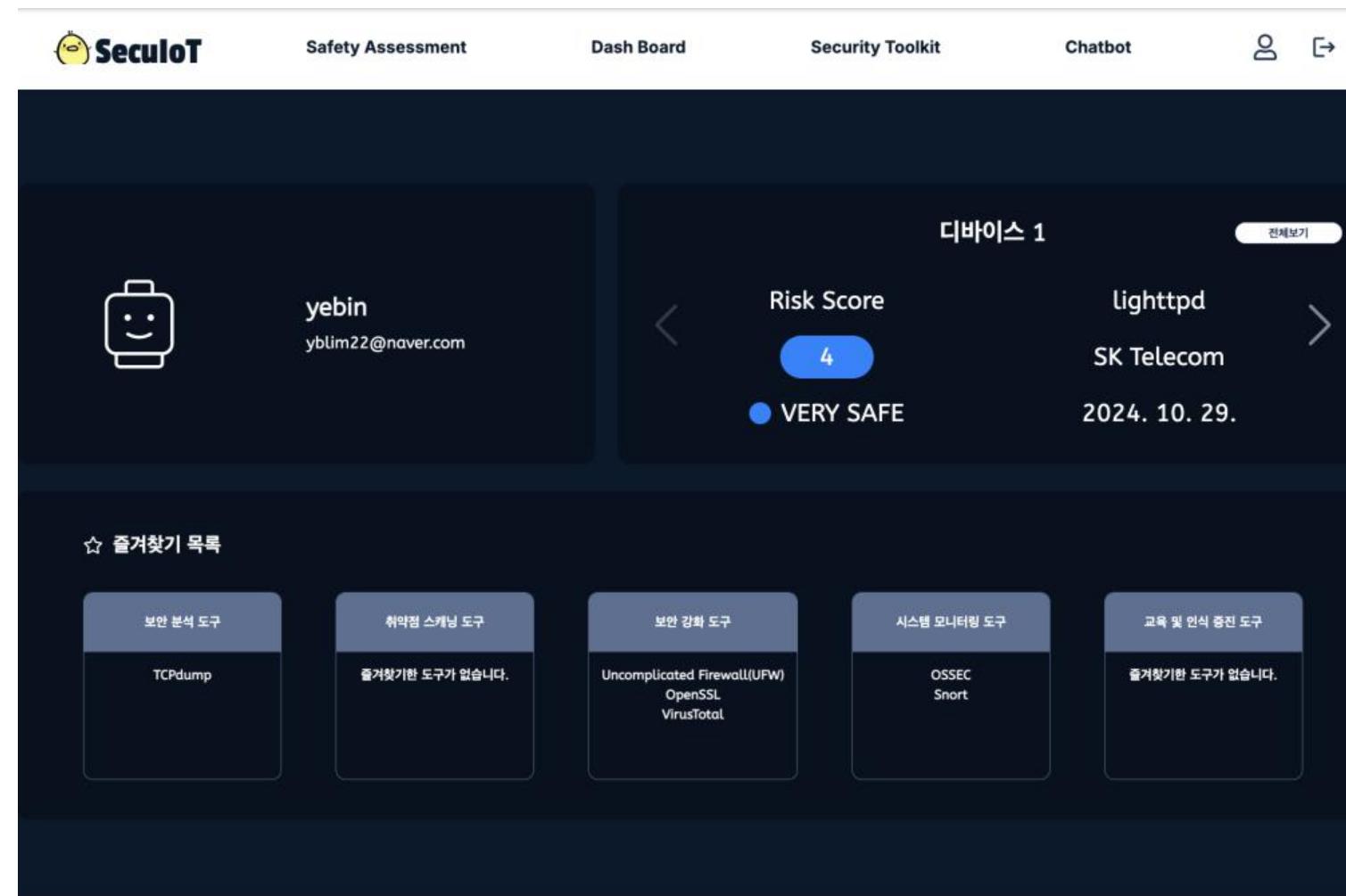
6.1.2. 즐겨찾기

6.1.3. IoT 기기 위험도 평가

6.1.4. 마이페이지

6.1.4. 챗봇

마이페이지



설명	사용자가 자신의 계정 정보를 관리하고 IoT 기기 및 평가 기록을 확인할 수 있는 기능
주요 기능	<ul style="list-style-type: none"> 1. 계정 관리: 사용자가 계정 정보를 수정하고 비밀번호를 관리 2. 기기 관리: 사용자가 자신의 IoT 기기 목록을 확인하고, 기기 정보를 추가 또는 수정 3. 평가 기록: 사용자가 수행한 위험도 평가 결과와 히스토리를 확인 4. 즐겨찾기: 즐겨찾기로 설정한 오픈 소스를 모아볼 수 있음
로직	사용자가 로그인하여 마이페이지에 접근 / 계정 정보를 확인 및 수정 IoT 기기 목록을 확인하고, 기기 정보를 추가하거나 수정 위험도 평가 기록을 확인하고, 과거 평가 결과를 조회 즐겨찾기의 오픈 소스 클릭시 해당 오픈 소스 화면으로 넘어감
장점	사용자가 자신의 계정과 기기 정보를 효과적으로 관리할 수 있음 위험도 평가 결과를 지속적으로 확인하여 기기의 보안 상태를 모니터링할 수 있음 개인화된 관리 기능을 제공하여 사용자 편의성을 높임

기능 설명

SeculioT - D U C K

6.1. 주요 기능 개요

6.1.1. 보안 오픈 소스 제공

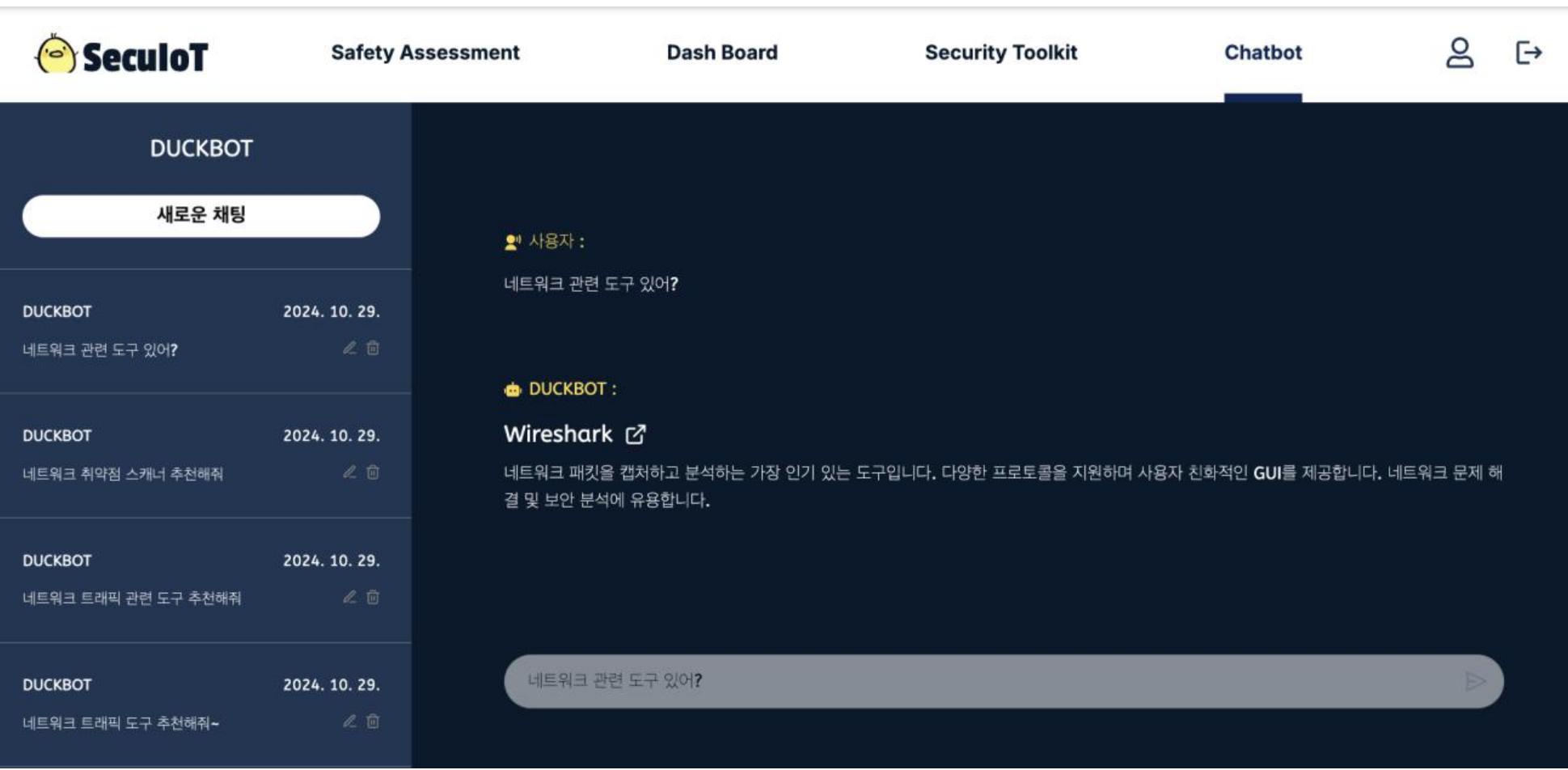
6.1.2. 즐겨찾기

6.1.3. IoT 기기 위험도 평가

6.1.4. 마이페이지

6.1.4. 챗봇

챗봇



설명	챗봇은 키워드 매칭 기법을 사용하여 사용자의 질문에 대해 신속하게 적합한 답변을 제공
주요 기능	1. 키워드 추출 및 매칭: 사용자가 입력한 질문에서 주요 키워드를 자동으로 추출하고, 사전에 정의된 키워드와 비교하여 가장 적합한 답변을 제공. 2. 질문 분석 및 대응: 사용자의 입력을 분석하여 관련 보안 정보나 오픈 소스 자료를 안내
로직	질문 분석: 사용자가 입력한 텍스트에서 주요 키워드를 추출 키워드 매칭: 추출된 키워드를 기준으로 데이터베이스에 저장된 답변과 매칭하여 적절한 정보를 검색 답변 제공: 매칭된 결과를 사용자에게 자연어 형태로 응답
장점	효율적인 정보 제공: 간단한 키워드 분석을 통해 빠르고 정확한 답변 제공 가능 확장 가능성: 키워드 데이터베이스를 지속적으로 업데이트하여 다양한 질문에 대응 가능

프로젝트의 기대효과 및 발전 가능성

S e c u r i o T - D U C K

7.1. 기대효과

7.2. 발전 가능성

기대효과

사용자 보안 인식 제고

설명: IoT 기기의 위험도를 손쉽게 평가할 수 있어 사용자의 보안 인식이 높아진다.

구체적 효과: 사용자들이 자신의 기기에 대한 위험도를 쉽게 파악하고, 보안 조치를 취하게 된다. 이를 통해 전체적인 IoT 기기의 보안 수준이 향상된다.

간단한 챗봇 질의응답 지원

설명: 챗봇 기능을 통해 사용자가 필요한 보안 오픈 소스를 쉽게 찾을 수 있다.

구체적 효과: 사용자가 신속하게 정보를 얻고, 보안 관련 질문에 대해 실시간으로 답변을 받을 수 있다.

보안 솔루션 접근성 향상

설명: 보안 오픈 소스 소프트웨어를 쉽게 검색하고 접근할 수 있다.

구체적 효과: 사용자들이 다양한 보안 오픈 소스를 쉽게 찾을 수 있어, 보안 강화에 필요한 도구를 신속하게 활용할 수 있다.



7.1. 기대효과

7.2. 발전 가능성



01

AI 모델의 정교화

더 많은 데이터를 학습하여 IoT 기기 위험도 예측 모델의 정밀도를 향상시킬 수 있다.
지속적인 데이터 수집과 모델 개선을 통해 더 높은 정확도의 위험도 예측이 가능해진다.

02

추가 보안 기능 통합

기기 관리, 네트워크 모니터링 등 추가적인 보안 기능을 통합할 수 있다.
현재의 기능에 더해 네트워크 보안 상태 모니터링, 실시간 위협 탐지 등의 기능을 추가할 수 있다.

03

모바일 애플리케이션 개발

웹 기반 시스템을 확장하여 모바일 애플리케이션으로 개발할 수 있다.
모바일 앱으로 개발하여 사용자가 언제 어디서나 기기의 보안 상태를 모니터링하고 평가할 수 있게 할 수 있다.

04

맞춤형 보안 솔루션 제공

데이터 분석을 통해 사용자 기기 특성에 맞는 맞춤형 보안 솔루션을 제안할 계획이다.
예를 들어, 특정 유형의 IoT 기기에 자주 발생하는 보안 취약점을 자동으로 감지하고 이에 대한 해결책을 추천하는 기능을 추가할 수 있다.

05

보안 오픈 소스 데이터베이스 확장

현재 제공하는 보안 오픈 소스의 범위를 확장하여 더욱 다양한 도구와 솔루션을 포함할 수 있다.
신규 보안 오픈 소스와 최신 보안 트렌드를 반영하여 데이터베이스를 지속적으로 업데이트하고 확장할 수 있다.

추가- TC (1)

TC ID	테스트 항목	테스트 목적	테스트 절차	기대 결과	실제 결과	Pass/Fail
TC01	회원가입 페이지 이동	회원가입 버튼 클릭 시 회원가입 페이지로 이동하는지 확인	메인 페이지 → '회원가입' 버튼 클릭	회원가입 페이지로 정상 이동	동일	Pass
TC02	로그인 페이지 이동	로그인 버튼 클릭 시 로그인 페이지로 이동하는지 확인	메인 페이지 → '로그인' 버튼 클릭	로그인 페이지로 정상 이동	동일	Pass
TC03	안전 평가 페이지 이동	안전 평가 버튼 클릭 시 페이지로 이동하는지 확인	메인 페이지 → '안전 평가' 버튼 클릭	안전 평가 페이지로 정상 이동	동일	Pass
TC04	보안 도구 페이지 이동	보안 도구 버튼 클릭 시 페이지로 이동하는지 확인	메인 페이지 → '보안 도구' 버튼 클릭	보안 도구 페이지로 정상 이동	동일	Pass
TC05	보안 도구 페이지 이동	보안 도구 버튼 클릭 시 페이지로 이동하는지 상태창 확인	메뉴창 → '보안 도구' 상태창 열기, 클릭	보안 도구 페이지로 정상 이동	동일	Pass
TC06	챗봇 페이지 이동	챗봇 버튼 클릭 시 챗봇 페이지로 이동하는지 확인	메인 페이지 → '챗봇' 버튼 클릭	챗봇 페이지로 정상 이동	동일	Pass
TC07	메인 페이지 이동	로고 클릭 시 메인 페이지로 이동하는지 확인	로그인 후 대시보드 → 로고 클릭	메인 페이지로 정상 이동	동일	Pass
TC08	회원가입 기능	회원가입 시 모든 필드 입력 후 정상 동작 여부 확인	회원가입 페이지 → 필드 입력 후 제출	회원가입 성공 후 로그인 페이지로 이동	동일	Pass
TC09	회원가입 기능	회원가입 시 모든 필드 입력 후 비정상 동작 여부 확인	회원가입 페이지 → 필드 공란 후 제출	공란인 곳 입력하라는 메세지 출력	동일	Pass
TC10	개인정보 동의 체크	동의 체크박스가 정상 작동하는지 확인	회원가입 페이지 → 동의 체크박스 체크 후 제출	동의 없이는 제출 불가, 동의 시 제출 가능	동일	Pass

추가- TC (2)

TC ID	테스트 항목	테스트 목적	테스트 절차	기대 결과	실제 결과	Pass/Fail
TC11	로그인 기능	올바른 계정으로 로그인 시 정상 로그인이 되는지 확인	로그인 페이지 → 아이디/비밀번호 입력 후 로그인 클릭	대시보드 페이지로 정상 이동	동일	Pass
TC12	로그인 실패 확인	잘못된 계정으로 로그인 시 오류 메시지가 출력되는지 확인	로그인 페이지 → 잘못된 아이디/비밀번호 입력 후 로그인 클릭	이메일(비밀번호) 정확히 입력하라는 메세지	동일	Pass
TC13	비밀번호 재설정 요청	등록된 이메일로 비밀번호 재설정 요청이 정상적으로 처리되는지 확인	로그인 페이지 → '비밀번호 찾기' 버튼 클릭 → 이메일 입력	비밀번호 재설정 이메일이 전송됨	동일	Pass
TC14	비밀번호 재설정 완료	이메일 링크를 통해 새 비밀번호 설정 후 정상 동작 여부 확인	비밀번호 재설정 이메일 링크 → 새 비밀번호 설정	새로운 비밀번호로 정상 로그인 가능	동일	Pass
TC15	위험도 평가 결과 확인	입력된 기기에 대해 정확한 위험도 점수가 반환되는지 확인	안전 평가 페이지 기기 정보 입력 후 결과 확인	예상 점수 및 구간이 표시됨	동일	Pass
TC16	즐겨찾기 추가 기능	보안 도구를 즐겨찾기에 추가할 수 있는지 확인	보안 도구 페이지 도구 선택 즐겨찾기 버튼 클릭	선택한 도구가 즐겨찾기에 정상 추가	동일	Pass
TC17	즐겨찾기 페이지 조회	즐겨찾기 추가 후 정상적으로 목록 조회되는지 확인	마이페이지 → 즐겨찾기 항목 확인	추가된 항목이 표시됨	동일	Pass
TC18	위험도 평가 기록 저장	기기 평가 후 기록이 마이페이지에 저장되는지 확인	안전 평가 후 마이페이지 이동	평가 기록이 저장 및 표시됨	동일	Pass
TC19	챗봇 응답 기능	사용자가 질문 시 적절한 응답이 반환되는지 확인	챗봇 페이지 → 질문 입력 후 전송	질문과 관련된 보안 정보가 반환됨	동일	Pass
TC20	대시보드 위젯 확인	대시보드에서 위젯이 정상적으로 표시되고 작동하는지 확인	대시보드 페이지 위젯 내용 및 동작 확인	모든 위젯이 정상적으로 표시되고 작동	동일	Pass

추가- TC (3)

TC ID	테스트 항목	테스트 목적	테스트 절차	기대 결과	실제 결과	Pass/Fail
TC21	마이페이지 기기 관리	기기삭제가 정상 동작하는지 확인	마이페이지 삭제 후 확인	기기 정보가 정상 반영됨	동일	Pass
TC22	보안 오픈 소스 목록 확인	보안 도구 페이지에서 모든 등록된 오픈 소스 목록 확인	보안 도구 페이지 → 오픈 소스 목록 스크롤	모든 항목이 정확히 표시됨	동일	Pass
TC23	보안 오픈 소스 세부 링크 확인	특정 보안 오픈 소스의 상세 설명 및 링크 확인	보안 도구 페이지에서 링크 클릭	링크가 올바르게 연결됨	동일	Pass
TC24	로그아웃 기능	로그아웃 버튼 클릭 시 정상 로그아웃이 되는지 확인	마이페이지 → '로그아웃' 버튼 클릭	로그인 종료	동일	Pass

1차 심사 후 개선 사항 - 프로젝트 개요



DUCK 팀입니다..!

프로젝트 소개

IoT 기기의 보안 위험을 예측하고, 보안 오픈 소스 소프트웨어를 제공하여
사용자들이 보안 정보를 쉽게 찾고 활용할 수 있도록 돋는 웹 플랫폼



프로젝트 목적

인공지능을 통한 IoT 기기의 위험도 수준 예측과
보안 오픈 소스를 소개하고 간편하게 사용하게 도움

1차 심사 후 개선 사항 - 피드백 및 개선 방향



아쉬운 점

IoT 기기의 보안 위험을 예측 이후 직접적인 솔루션이 나오지 않음

-> 솔루션 부재



개선 방향

IoT 위험도 예측 결과 + 보안 솔루션 제공

사용자에게 실질적인 보안 대응 방안을 제시하여,
단순 예측 뿐만 아니라 솔루션 제공의 통합 시스템으로 발전

1차 심사 후 개선 사항 - UI/UX 개선

Safety Assessment Dash Board Security Toolkit Chatbot

Risk Score
20

lighttpd SK Telecom

DANGEROUS

높은 수준의 취약점, CVE 기록, 악성 활동 신고가 있으며, 적극적인 조치가 필요한 상태입니다.

추가 검사와 보안 시스템 강화 등의 조치가 필요합니다.
네트워크 보안 시스템 점검을 추천드립니다.

점수 분석 결과

점수 분석 결과 확인 버튼 추가

구간별 원인 / 문제 / 해결 방안 제공

DANGEROS

원인

- 기기 펌웨어가 최신 상태가 아닐 가능성이 높습니다.
- 알려진 취약점이 패치되지 않은 상태로 남아 있어 공격자에게 악용될 가능성이 있습니다.
- 기기가 사용 중인 통신 프로토콜(TCP/IP)에서 인증 및 암호화가 취약합니다.
- 중간자 공격(Man-in-the-Middle Attack)에 노출될 위험이 있으며, 기기 내부 데이터가 탈취될 가능성이 있습니다.

문제

- 기기가 갑자기 깨지거나 다시 시작되는 등 정상적으로 작동하지 않을 수 있습니다.
- 명령에 대한 응답이 느리거나 오류가 자주 발생할 수 있습니다.
- 기기를 통해 수집된 민감한 사용자 정보가 외부로 전송될 수 있습니다.
- 해당 기기가 허브 역할을 할 경우, 같은 네트워크에 있는 다른 IoT 기기까지 공격 범위에 포함될 수 있습니다.

해결

- 기기의 펌웨어를 즉시 최신 버전으로 업데이트하세요.
- 통신 프로토콜(TCP/IP)에서 강력한 암호화 방식을 사용하도록 설정하세요.
▶ OpenSSL
- 네트워크 트래픽을 모니터링하고, 의심스러운 활동이 발견되면 Wireshark와 같은 도구를 사용해 상세 분석을 수행하세요.
▶ Wireshark
- 기기가 비정상적으로 작동하는 경우, 악성코드 분석 도구를 활용해 기기 내부 소프트웨어를 점검하세요.
▶ Cuckoo Sandbox
- 기기를 신뢰할 수 있는 네트워크에 연결하고, 방화벽 및 침입 탐지 시스템을 통해 네트워크 보안을 강화하세요.
▶ Firewalld

데이터베이스 확장 및 솔루션 매칭 시스템

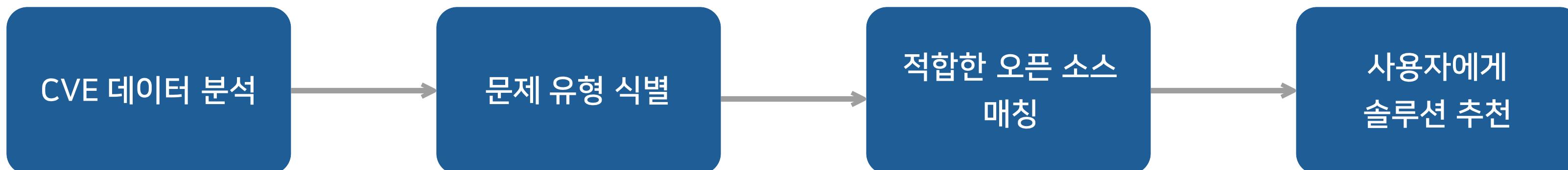
- 위험도 점수와 문제 유형 매칭
- 점수가 높을 수록 문제 유형 증가
- 오픈 소스 솔루션 추천 테이블 설계

위험도 구간	문제 유형	추천 솔루션	설명
매우 위험	DDoS 공격 가능성	Snort	실시간 패킷 분석 및 침입 탐지
위험	취약한 포트 노출	OpenVAS	취약점 스캔 및 관리
주의	권한 관리 오류	OSSEC	로그 분석 및 권한 모니터링

(예시)

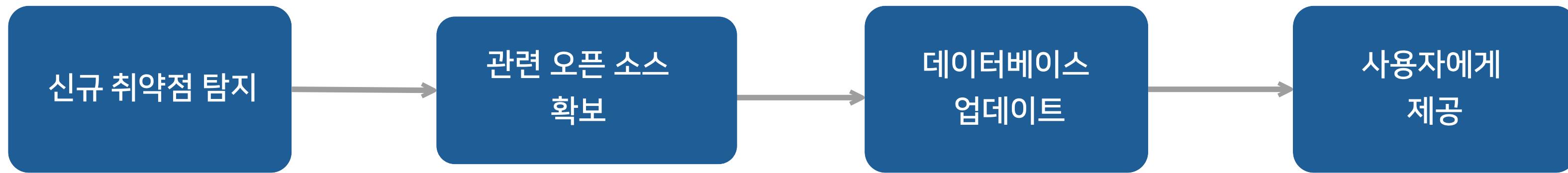
CVE와 매칭된 솔루션 데이터

- CVE 데이터를 기반으로 취약점 정보를 분석
- 기기에 적합한 오픈 소스 솔루션 추천
- 사용자 친화적인 방식으로 제안



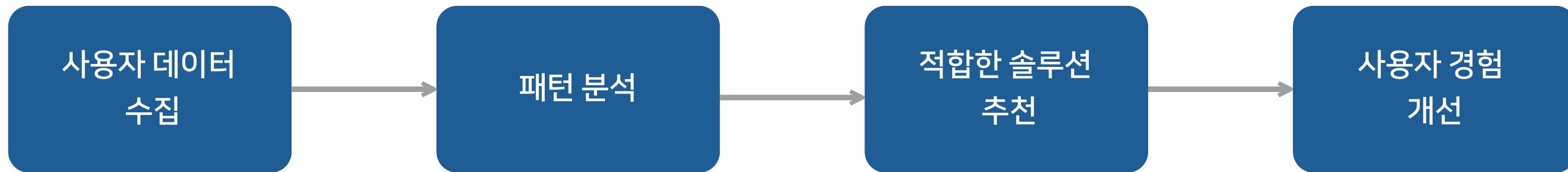
오픈 소스 데이터 정기 업데이트

- 오픈 소스 데이터를 정기적으로 업데이트하여 신규 취약점과 관련된 오픈 소스 솔루션을 지속적으로 업데이트
- 이를 위해 API 기반 자동화 시스템을 구축하여 최신 보안 데이터를 빠르게 반영



사용자 맞춤형 솔루션 추천

- 사용자의 기기 사용 패턴, 기기 유형 등을 분석하여 개인화된 솔루션 추천 시스템을 도입
- 장기적으로 AI 기반 추천 알고리즘(예: 협업 필터링, 컨텍스트 기반 추천)을 통해 사용자 경험을 강화



1차 심사 후 개선 사항 - 구현 계획 및 기대효과

구현 계획

- 오픈 소스 및 보안 커뮤니티, 데이터베이스와 연동하여 최신 보안 솔루션을 확보
- Shodan API와 사용자 피드백 데이터를 활용해 솔루션의 정확도와 관련성을 지속적으로 개선

오픈 소스 데이터베이스
(CVE, Shodan 등)



솔루션 매칭 알고리즘

사용자 맞춤형 솔루션 제공

기대 효과

사용자의 보안 대응 능력을 향상

솔루션 매칭과 개인화 추천을 통해 시스템 신뢰도를 제고

지속 가능한 데이터 기반 발전이 가능하며, 신규 데이터를 통해 더욱 정교한 솔루션을 제공

2201636 임예빈

졸업작품을 진행하며 3년간 배운 IT 전반적인 전공 지식을 활용할 수 있어서, 프로젝트를 진행하며 더 배워나간 것 같습니다. 개발 뿐이 아닌, 기획부터 디자인, 프론트와 백엔드 개발까지 전반적으로 참여하며 프로젝트가 흘러가는 방향과 진행법 등을 직접 경험해볼 수 있어 뜻깊었습니다.

장기적인 팀 프로젝트는 처음 해보았는데, 팀원들과 협동하며 일을 분배하고 작업하는 과정에서 팀플 경험을 쌓을 수 있었습니다.

개발이 처음이니 어려운 부분도 있었지만, 오류를 해결해나가며 프로젝트를 완료할 수 있어서 뿌듯하고 3년간의 배운 지식을 적용해보며 끝까지 해내서 다행이었습니다.

2201614 서윤지

졸업 작품을 준비하는 과정에서 많은 것을 배우고 경험할 수 있었습니다. 처음 아이디어를 구상하고 프로젝트 기획을 진행하며 현실적인 한계를 느끼기도 했고, 기술적인 문제에 부딪혀 좌절을 겪기도 했습니다.

하지만 팀원들과 함께 하나하나 문제를 해결하며 프로젝트가 점차 완성되는 모습을 보며 큰 성취감을 느꼈습니다. 개발을 진행하며 이론적으로만 알던 개념들이 실제 프로젝트에서 어떻게 구현되는지, 그리고 실무에서 얼마나 중요한지를 체감할 수 있었습니다.

사용자의 경험을 고려한 UI/UX와 다양한 기술 적용을 통해, 단순히 '작동하는' 프로그램이 아닌 '사용할 수 있는' 프로그램을 만드는 것이 얼마나 중요한지 깨달았습니다. 이러한 경험을 통해 나은 개발자로 성장하는데 큰 도움이 되었다고 생각합니다.

2201637 임유빈

이번 졸업작품을 하면서 제대로 된 팀플레이가 무엇이고, 처음부터 마지막까지 개발 과정이 어떻게 되는지 새롭게 알게 된 경험 이었습니다.

팀장의 역할은 생각보다 대단하고, 많은 책임감을 가지고 임해야 한다는 것을 느끼게 되었고, 팀원으로서 해가 되지 않도록 책임감을 가지며 임할 수 있었습니다.

많은 수정 과정을 통해 보이지 않던 언어들도 하나씩 보이게 되면서 알아가는 재미도 느낄 수 있었던 시간이었습니다.

많은 것을 알지 못한 상태에서 하였지만 좋은 팀원들과 여러 번 시도해 보며 서로가 발전하는 모습을 보게 되어 서로 응원하며 끝까지 마무리할 수 있었습니다.

힘들었지만 뿌듯하고 많은 것을 배울 수 있어서 굉장히 뜻깊고 잊지 못할 경험이 될 것 같습니다.

시연 영상

시연 순서

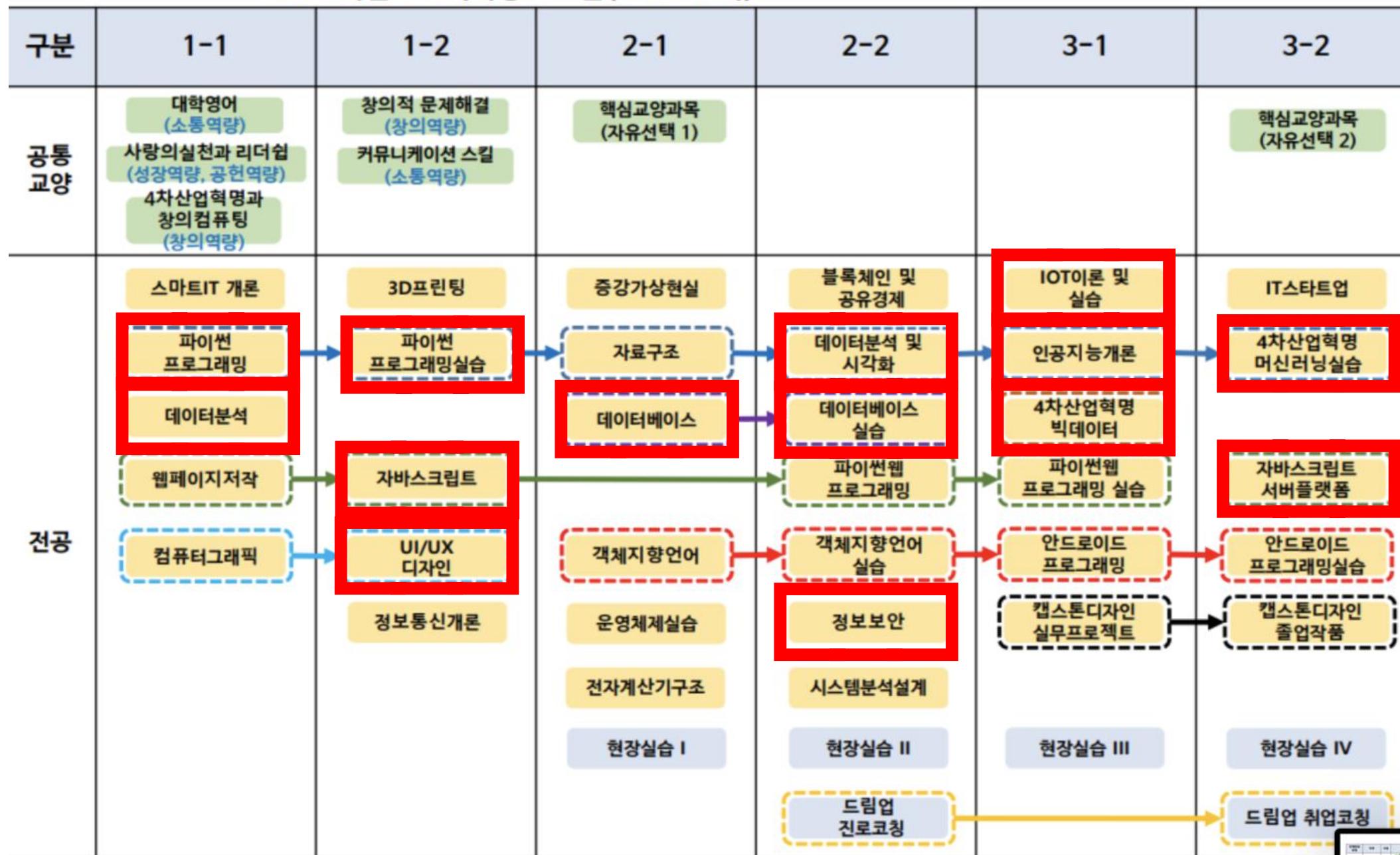
1. 회원가입
2. 비밀번호 찾기
3. 로그인
4. 메인 페이지
5. Safety Assessment 페이지 - IoT 기기 위험도 분석
6. 대시보드
7. 툴킷 페이지 (몇 페이지만 확인) + 즐겨찾기 추가, 취소
8. 챗봇
9. 마이페이지 - 장치 확인, 즐겨찾기 확인
10. 로그아웃

QnA

appendix1: 프로젝트 선택 동기

캡스톤 디자인(capstone design)이란 공학계열 학생이 실제 현장에서 부딪히는 문제를 해결할 수 있도록 학부과정 동안 배운 이론을 토대로 작품을 기획, 설계, 제작하는 전 과정을 경험하게 하는 교육 과정을 뜻한다.

2021학년도 교육과정 로드맵(스마트IT과)



교육과정 중 흥미 있던 교과목,
프로젝트에 실제 활용한 과목 표시

팀원 전체가 흥미있고 좀 더 배우고 싶던 과목인
정보보안, IoT, 인공지능 수업에서 배운 내용을
바탕으로 전체적인 주제를 선정

주된 목적은 react, SQL 등 과목별로 학습하여 다루었던
지식을 적용하고 다양한 기술을 종합적으로 직접 사용해
보는 경험을 쌓는 것

appendix2: 프로젝트 필요성 및 타겟 사용자 (1)

Q. 이 프로젝트를 사람들이 필요로 할까?

Q. 왜 IoT 기기의 위험도 예측과 보안 오픈 소스 제공을 주제로 삼았나?

보안 문제는 일부 특화된 사용자들 사이에서 수요가 존재함

다양한 기기 사용이 증가함에 따라 보안의 중요성도 커지고 있으며, 이 프로젝트는 보안에 관심 있는 사용자들에게 보안 상태 확인과 정보 제공으로 관심 상승에 도움을 주는 데 의의가 있음

수요가 높지 않지만 일부 사용자들은 수요가 있으며, 마찬가지로 공급도 적기에 수요자들이 몰릴 것

<보안 중요성에 대한 수요 증가에 대한 뉴스와 보고서 (추가 버전)>

요약

- IoT 기기 사용 증가와 보안 위협: 2024년에는 IoT 기기 사용이 급격히 증가하면서, 이러한 기기를 목표로 하는 사이버 공격이 대폭 증가했다. 예를 들어, 2024년 초에 발생한 Roku의 해킹 사건에서는 57만 개 이상의 계정이 영향을 받았으며, 이는 IoT 기기의 보안 취약성을 여실히 드러냈다. 이런 사건들은 IoT 기기 보안이 개인 정보 보호와 네트워크 무결성을 위해 필수적임을 강조한다.

[Infosecurity Magazine: IoT Vulnerabilities Skyrocket, Becoming Key Entry Point for Attackers, 2024]

[ThriveDX Media: Internet of Things (IoT) Cyberattacks in 2024 – Causes and Implications]

- 산업계의 우려와 대응: 산업 전문가들은 IoT 기기를 보호하지 않을 경우, 기업의 사이버 복원력에 큰 공백이 생긴다고 경고하고 있다. 특히, 병원, 제조업체, 정부 기관과 같은 조직은 연결된 IoT 기기들을 통해 효율성을 높이고 있지만, 이러한 기기들이 사이버 범죄자들의 주요 목표가 되고 있다.

[IoTnews: IoT security remains a top concern for enterprises in 2024]

appendix3: 기술 선택 및 구현 과정

Q. 프로젝트에서 사용한 AI 모델은 어떻게 선택했고, 그 이유는 무엇인가?

선형 회귀 모델을 선택

데이터셋이 제한된 특징으로 구성되어 있고, 위험도 점수라는 연속적인 값을 예측해야 했기 때문에,
간단하지만 해석이 쉬운 모델을 우선으로 고려함

Q. AI 모델의 정확도를 어떻게 평가했으며, 그 결과는 어땠나?

평균 절대 오차(MAE)를 통해 모델의 정확도를 평가
결과는 비교적 낮은 MAE 값으로, 모델이 신뢰할 만한 수준임을 확인

Q. 데이터 수집은 어떻게 이루어졌는가?

주로 Shodan API와 AbuseIPDB 사용
Shodan을 통해 IoT 기기의 IP 주소, CVE 정보, CVSS 점수 등을 수집하였고, AbuseIPDB에서 보안 취약점 관련
신고 기록을 확보

금전적(Shodan 등 한 달 구독료 십만원 이상, 캡스톤 지원 불가), 시간적 문제로 각각 한달 구독 후 데이터를 수집

appendix4: 예측 시스템(1)

Q. 인공지능 위험도 분석 예측 시스템에 올바르지 않은 기기나 통신사가 들어가도 점수가 측정되는데, 오류가 아닌가?

1. 현재 시스템은 데이터에 없는 기기나 통신사도 점수를 측정할 수 있지만, 이로 인해 정확도가 낮아질 가능성이 있음

이는 데이터 수집을 위해 Shodan과 같은 서비스를 한 달 구독했기 때문이며, 금전적(사비 구독료, 캡스톤 지원비 사용 불가 항목) 및 시간적 제약(한정된 기간)으로 인해 충분한 데이터를 확보하지 못하였기 때문임

→ 해당 문제는 이미 예상한 부분

2. 데이터 수집 초기 단계에서 충분한 데이터가 확보되지 않은 상태에서, 정보가 누락된 통신사나 기기가 많을 것으로 예상

→ 따라서 예측 시스템이 모든 상황을 커버할 수 있도록 초기부터 예측 모델을 확장 가능하게 설계함
이는 프로젝트가 확장되고, 더 많은 데이터를 확보할 때 정확도를 향상시키기 위한 대비책

3. 결론

장기적으로는 데이터가 주기적으로 갱신되면서 점점 더 많은 통신사와 기기에 대한 정보를 수집할 수 있을 것이며, 매달 데이터 업데이트를 통해 데이터셋을 확장하고, 이를 AI 모델이 학습하면서 예측 정확도가 점진적으로 향상될 것임. 이러한 방식은 초기 단계에서의 예산 및 시간 제약을 고려한 합리적인 선택이었으며, 데이터 수집의 한계를 해결하면서도 시스템의 유연성을 유지하기 위한 전략적 접근임

이러한 개선 작업은 단순한 단기적 보완책이 아니라, 향후 시스템의 확장성과 장기적인 안정성을 고려한 계획적 조치이며, 프로젝트가 발전함에 따라, 수집된 데이터를 바탕으로 더욱 정교한 예측이 가능해질 것이며, 더 많은 사용자들에게 신뢰할 수 있는 보안 정보를 제공할 수 있을 것

appendix5: 예측 시스템(2)

Q. (앞서 질문과 연결되어) 그렇다면 없는 기기나 통신사는 아예 점수가 뜨지 않게 하지 그랬나?

처음에는 없는 데이터에 대해 예측을 막는 방향을 고려

→ 하지만 이렇게 할 경우, 데이터가 없는 기기나 통신사가 너무 많아 예측 시스템의 유연성이 크게 제한될 수 있다고 판단
프로젝트 초기 단계에서는 아직 충분한 데이터를 확보하지 못한 상황이었기 때문에, 예측 범위를 가능한 넓게 설정하여 모든 상황을 고려할 수 있는 모델을 설계하는 것이 더 적절하다고 생각

데이터 수집이 진행되면서 점점 더 많은 기기와 통신사 정보가 추가될 것이고, 모델은 이 추가 데이터를 통해 점차 정밀해질 것

→ 현재는 기초적인 예측을 기반으로 데이터를 축적하고 있으며, 데이터가 누적됨에 따라 더욱 신뢰성 있는 결과를 제공할 수 있음

이 접근법은 초기 단계에서 시스템의 확장성과 적응성을 고려한 결정이었으며, 더 많은 데이터를 수집하고 업데이트하는 과정에서 예측 정확도는 크게 향상될 것이며, 따라서 현재 시스템이 없는 데이터를 예측하는 것은 단순한 기능적 한계가 아니라, 장기적인 확장성과 정확도를 높이기 위한 선택임을 강조하고 싶고, 추후 데이터를 충분히 확보한 후에는 예측 정확도를 높이기 위한 다양한 조치를 고려할 계획

appendix6: 챗봇

Q. 챗봇은 어떻게 동작하는가?

챗봇은 키워드 매칭 기법을 사용하여 작동

사용자가 입력한 질문에서 특정 키워드를 추출하고, 데이터베이스에 저장된 오픈소스별 관련 정보(키워드)를 매칭하여 답변을 제공
만약 적절한 키워드가 없을 경우, 관련 정보를 찾을 수 없다는 메시지를 출력하도록 설계됨

Q. 키워드 매칭의 한계와 개선 가능성?

현재 챗봇은 키워드 매칭 기법을 기반으로 작동하기 때문에, 사용자가 입력한 질문에서 특정 키워드를 추출하고, 데이터베이스에 저장된 답변과 일치하는 키워드를 찾음. 하지만 이 방법은 복잡한 문장 구조를 제대로 분석하지 못하거나, 유사한 의미를 가진 표현을 정확히 처리하지 못하는 한계가 있음

→ 개선 가능성: 이러한 한계를 보완하기 위해, 향후 자연어 처리 기술을 도입하여 보다 정교한 분석을 시도

Q. 키워드 데이터베이스를 얼마나 자주 업데이트할 계획인가?

키워드 매칭 기법에서 중요한 것은 키워드 데이터베이스의 업데이트임. 보안 정보는 빠르게 변화하기 때문에, 챗봇의 정확한 응답을 위해 주기적인 데이터베이스 갱신이 필요하여, 새로운 보안 위협이 발생하거나 오픈 소스 도구가 추가될 때마다 키워드를 업데이트

정기적인 업데이트 계획(월 2회 업데이트)이나 중요한 보안 이벤트 발생 시 즉각 업데이트하는 방법

appendix7: 즐겨찾기-로컬 스토리지

Q. 로컬 스토리지에 저장된 데이터가 제3자에게 노출될 가능성은 없나?

로컬 스토리지는 클라이언트 측 브라우저에 데이터를 저장하기 때문에, 특정한 브라우저 환경에서만 접근이 가능함

→ 따라서 보안성이 낮은 데이터만 로컬 스토리지에 저장하고 있음. 중요한 데이터는 서버에 암호화하여 저장함으로써 보안을 강화할 계획 이를 통해, 사용자 정보나 민감한 데이터가 로컬 스토리지에 노출되지 않도록 함

Q. 로컬 스토리지에 데이터를 저장할 때 JSON 형식을 사용하는 이유는 무엇인지?

JSON 형식은 간결하고, 읽기 쉽고, JavaScript와의 호환성이 뛰어나며, 로컬 스토리지에 데이터를 저장할 때 JSON을 사용하면 데이터를 직관적으로 관리하고 쉽게 저장 및 불러올 수 있음. 또한, JSON은 다양한 웹 애플리케이션에서 표준적으로 사용되는 데이터 형식이기 때문에, 로컬 스토리지와 같은 클라이언트 측 저장 공간에서 데이터를 다루기에 매우 적합하여 사용함

Q. 로컬 스토리지는 특정 브라우저에 한정되는데, 다른 기기에서도 동일한 즐겨찾기를 사용할 수 있는 방법은 없나?

현재는 단순성과 빠른 구현을 위해 로컬 스토리지를 사용하고 있지만, 다중 기기 간의 동기화는 지원되지 않음

→ 이는 프로젝트 초기 단계에서 빠른 구현을 목표로 한 결정

→ 하지만, 향후 프로젝트 확장 시 클라우드 기반 저장 시스템으로 업그레이드하여, 사용자 계정을 통해 다중 기기에서도 즐겨찾기를 동기화할 수 있는 기능을 추가할 계획

appendix8: 데이터베이스

Q. Supabase 데이터베이스가 프로젝트 확장에 적합한 이유는?

Supabase는 확장성이 뛰어나기 때문에, 프로젝트가 성장함에 따라 데이터베이스를 손쉽게 확장할 수 있음
예를 들어, 더 많은 IoT 기기 데이터를 처리해야 할 경우, Supabase의 스케일링 기능을 통해 서버 성능을 조정할 수 있음
또한, 클라우드 환경에서의 확장은 자동화된 백업과 복구 기능을 제공하여, 대규모 데이터를 안전하게 관리할 수 있음

Q. Supabase의 보안성은 어떻게 보장되는가?

Supabase는 PostgreSQL의 보안 기능을 활용하여 데이터 보호를 강화하고 있으며, 데이터 전송 시 SSL/TLS 암호화를 사용하며,
역할 기반 접근 제어(RBAC)를 통해 사용자의 권한을 세분화할 수 있습니다. 이를 통해, 민감한 데이터에 대한 접근을 제한하고, 보안
규정을 준수할 수 있음. 또한, API 키를 통해 데이터베이스 접근을 제어하여, 데이터가 외부로 노출되는 위험을 줄였음

Q. 데이터베이스로 Supabase를 선택한 이유는?

Supabase는 오픈 소스 기반의 실시간 데이터베이스로, 웹 애플리케이션과의 연동이 용이하며, 실시간 데이터 처리가 가능하다는 장점
특히, Supabase는 PostgreSQL을 기반으로 하여 안정성과 확장성이 뛰어나고, 보안 기능도 내장되어 있어 사용자 데이터를 안전하게 관리
또한, 개발 초기 단계에서 빠른 프로토타이핑이 가능하고, 클라우드 기반의 서비스를 통해 데이터베이스를 손쉽게 관리할 수 있음

appendix9: 대시보드

Q. 대시보드에 표시된 수치들은 실제 데이터를 기반으로 한 것인가?

현재 대시보드에 표시된 수치는 임의의 값으로 설정된 예시 데이터이며,
이는 시스템의 시각화 및 기능 구현을 확인하기 위해 설정된 값으로, 실제 데이터를 활용한 것이 아님.

현재 단계에서는 데이터가 충분히 확보되지 않았기 때문에, 이런 방식으로 데이터가 시각화될 것이라는 예시를 보여주기 위해 임의의 값을 사용하였다. 하지만, 시스템이 운영되면서 실제 IoT 기기와 위험도 평가 데이터를 축적할 계획이며, 2주에서 한 달 간격으로 데이터베이스를 업데이트하여 대시보드의 수치가 실제 데이터를 기반으로 표시되도록 개선할 것임.

이로 인해, 사용자들은 향후 대시보드를 통해 실제 기기와 보안 상태에 대한 정확한 인사이트를 얻을 수 있을 것이며, 이러한 주기적인 업데이트를 통해 데이터의 최신성을 유지하고, 시스템의 신뢰성을 높이는 것을 목표로 하고 있다.

appendix10: 데이터 업데이트 방향

Q. 추후 데이터 업데이트는 어떻게 이루어질 예정인가?

1. Shodan API를 활용한 실시간 데이터 수집

현재 사용 중인 Shodan API를 통해 실시간 보안 데이터를 매주 또는 매월 지속적으로 수집

이 API를 통해 수집된 데이터는 IoT 기기의 취약점 정보와 보안 위협에 대한 최신 데이터를 반영하여 데이터베이스를 갱신

2. 사용자 피드백 반영

사용자가 제공하는 피드백을 통해 데이터베이스의 정확성을 보완할 계획

예를 들어, 사용자가 특정 기기에 대한 정보를 추가하거나 수정할 경우, 이를 검토하여 데이터베이스에 반영

이를 통해 사용자 참여를 유도하고, 데이터의 신뢰성을 높일 수 있음

3. 자동화된 데이터 검증 및 정제

수집된 데이터는 자동화된 검증 및 정제 절차를 통해 처리

이 과정에서 중복되거나 부정확한 데이터를 걸러내고, 신뢰성 있는 데이터만을 사용하여 예측 모델을 개선

감사합니다.

DUCK - 임예빈, 서윤지, 임유빈