Pre-Vision 프로젝트 보고서

차세대 파일 보호: 악성코드 탐지, 암호화 및 패키징

Next-Generation File Protection: Malware Detection, Encryption, and Packaging

8 월 29 일

Pre-Vision

작성자: 우건희

목차

I. 프로젝트 개요

인터넷이 발달하면서 윈도우 기반 서비스가 급증하고, 이에 따라 해킹 기법도 빠르게 진화하고 있습니다. 특히 사용자의 암호를 탈취하거나 파일을 암호화하는 악성 프로그램들이 큰 위협으로 떠오르고 있습니다. 이들 악성 프로그램은 피싱 사이트, 피싱 이메일, 크랙 프로그램 등을 통해 퍼지며, 사용자가 이 파일들을 실행하는 순간 컴퓨터 시스템은 랜섬웨어에 의해 전부 암호화되거나, 아이디와 비밀번호를 탈취당하는 등의 심각한 피해를 입을 수 있습니다.

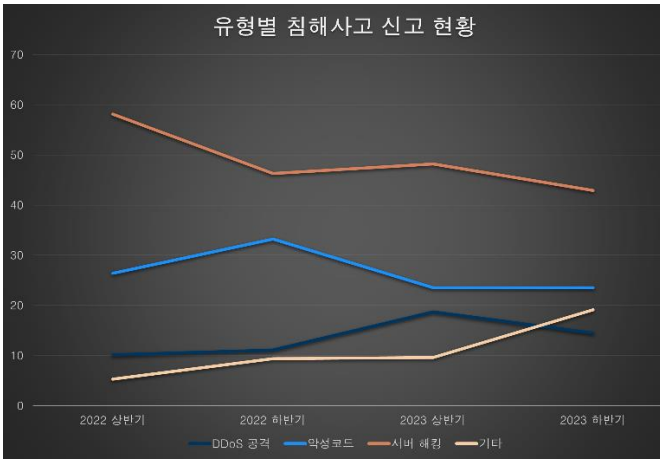
이러한 상황에 대응하기 위해, 저희 시스템은 단순히 악성코드를 탐지하는 것을 넘어 정보보안 전문가와 백신 개발자들에게 실질적인 도움을 제공하고자 설계되었습니다. 사용자가 업로드한 Windows PE 파일을 분석해 악성코드를 찾아내고, 발견된 악성코드에 대한 상세한 정보를 제공함으로써 백신 개발자들이 신속하게 대응할 수 있도록 돕습니다. 이는 악성코드에 대한 보다 효과적이고 체계적인 대응을 가능하게 하며, 새로운 위협에 빠르게 대처할 수 있는 기반을 제공합니다.

반면 악성코드의 위협만큼이나 중요한 문제는 바로 인디게임 개발자들이 직면한 리버스 엔지니어링(리버싱)의 위험입니다. 인디게임 시장이 빠르게 성장하면서 창의적이고 혁신적인 게임들이 쏟아져 나오고 있지만, 그만큼 리버싱을 통해 해커들이 게임의 소스 코드를 분석하고, 이를 불법 복제하거나 악용하는 사례도 늘어나고 있습니다. 이런 행위는 개발자의 지적 재산을 심각하게 침해할 뿐 아니라, 게임의 수익 모델을 무너뜨리고, 궁극적으로는 게임의 생존 자체를 위협하게 됩니다.

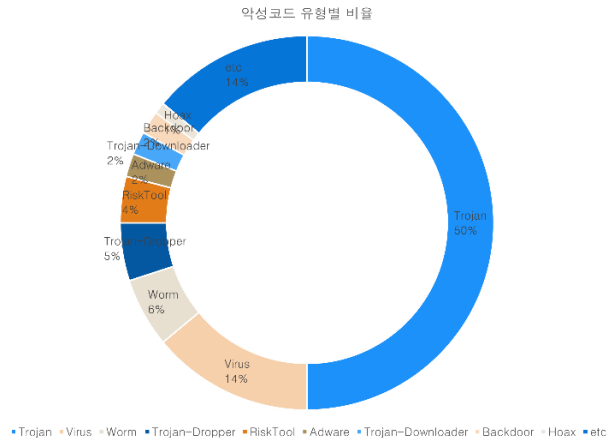
특히, 게임의 핵심 소스 코드가 유출되면 해커들은 이를 이용해 불법 복제본을 제작하거나, 게임 내 유료 아이템이나 광고를 제거해 수익을 저해할 수 있습니다. 또한, 게임 파일에 악성코드를 삽입해 배포함으로써 사용자들에게 큰 피해를 입히고, 결과적으로 개발자의 신뢰성을 떨어뜨릴 위험도 있습니다.

이러한 문제를 해결하기 위해, 저희 시스템은 PE 파일을 업로드하면 즉시 해당 파일을 분석해 악성코드가 포함되어 있는지 확인하고, 악성코드로 판명된 파일에 대해서는 백신 개발에 필요한 정보를 제공합니다. 그리고 악성코드가 발견되지 않은 파일은 자동으로 Protector 도구를 사용해 파일을 암호화하고 패킹함으로서 리버싱을 통한 공격을 막습니다. 이러한 기능 덕분에, 인디게임 개발자들은 리버싱이나 해킹과 같은 보안 문제에 대한 걱정을 덜 수 있습니다.

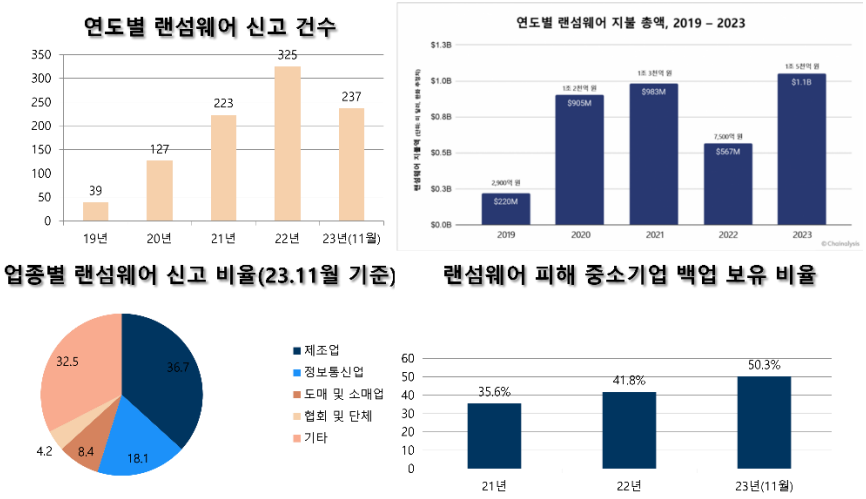
첨부된 자료들은 악성코드의 위험성과 인디게임 시장에서의 동향을 보여줍니다. 저희 시스템을 통해 인디게임 개발자들은 보다 안전한 환경에서 게임을 개발하고, 그들의 창의적인 작업이 해커의 위협으로부터 안전하게 보호될 것입니다.



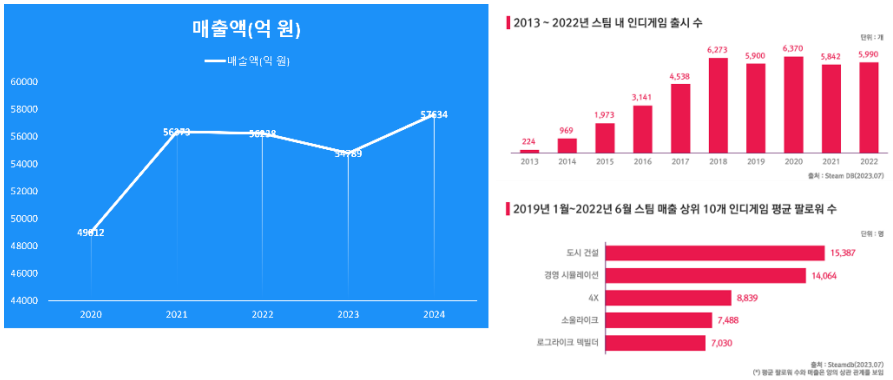
[그림 1]



[그림 2]



[그림 3]



[그림 4]

게임을 리버스 엔지니어링으로부터 보호하는 방법으로 사용하는 것이 데누보이다
하지만 인디 게임은 혼자서 만드는 게임임으로 데누보의 가격이 많이 부담스럽다
최근 유명한 AAA 타이틀을 제공하는 회사 또한 높은 가격으로 데누보 서비스를 제외하고 있다.

타이틀	가격
AAA 타이틀	10만유로 (13,000만원)
AA 타이틀	5만유로(6,500만원)
인디	1만유로(1,300만원)
패키지당 설치	2500유로(330만원)

[그림 5]

II. 기대효과

저희 프로젝트는 악성코드 탐지와 PE 파일 해킹으로부터 시스템을 보호하는 데 중점을 두고 있으며, 이를 통해 다양한 기대 효과를 얻을 수 있을 것입니다. 먼저, 저희 시스템은 PE 파일을 분석하여 악성코드를 탐지하고, 그 결과를 바탕으로 백신 개발자들에게 필요한 정보를 제공함으로써 새로운 위협에 빠르게 대응할 수 있도록 도와줍니다. 이는 전체적인 보안 수준을 높이는 데 크게 기여할 뿐만 아니라, 백신 개발자들이 보다 효과적인 백신을 만들 수 있도록 지원해 사이버 보안 산업의 전반적인 역량을 강화하는 데에도 도움이 될 것입니다.

특히, 저희 프로젝트는 인디게임 개발자들에게 매우 유용할 것으로 기대됩니다. 인디게임은 리버스 엔지니어링(리버싱)으로 인한 소스 코드 유출, 불법 복제, 악성코드 삽입 등 여러 가지 위험에 노출되어 있습니다. 하지만, 저희 시스템을 통해 파일을 암호화하고 보호함으로써 이런 위험에서 개발자들의 소중한 작품을 안전하게 지킬 수 있을 것입니다. 이는 인디게임 시장의 성장을 돕고, 개발자들이 더욱 창의적인 작업에 집중할 수 있는 환경을 마련해 줄 것입니다.

경제적인 측면에서도 저희 시스템은 중요한 역할을 할 것입니다. 악성코드 감염으로 인한 피해를 미리 방지함으로써, 기업과 개발자들은 보안 사고로 인한 재정적 손실을 줄일 수 있습니다. 또한, 게임 파일을 안전하게 보호함으로써 불법 복제로 인한 매출 손실도 예방할 수 있어, 경제적 이익을 극대화할 수 있을 것입니다. 특히, 인디게임 개발자들은 타사의 비싼 게임 파일 보호 시스템을 도입하지 않아도 저희의 시스템으로 최소한의 보호를 할 수 있을 것입니다.

결국, 저희 프로젝트는 사이버 보안과 인디게임 산업의 발전에 크게 기여할 것입니다. 악성코드 탐지와 파일 보호 분야에서 새로운 표준을 세우며, 관련 업계의 수준을 한층 높이고, 혁신적인 보안 솔루션으로 자리 잡을 것입니다.

III. 팀원 구성 및 역할

우건희

직책 : PM

역할

① PE 파일 모듈 개발
② 프로젝트 일정관리
③ 프로젝트 문서 관리
④ PE 파일 구조 조사
⑤ 클라우드 구축

김선우

직책 : PL

역할

① 웹페이지 개발
② 바이러스 토탈 API 연동 모듈 개발
③ DB 구축
④ 악성코드 해시화
⑤ 블랙리스트 개발

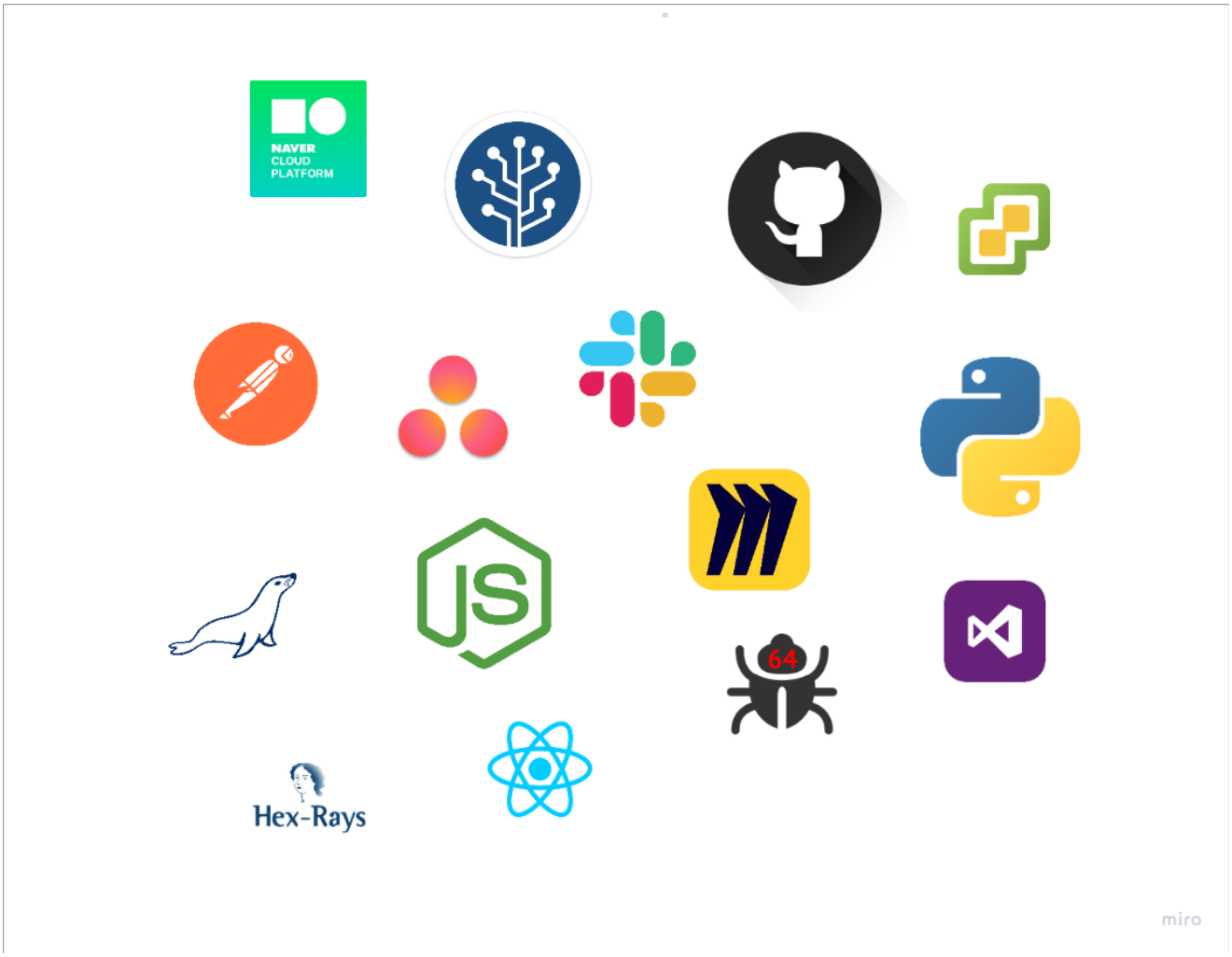
김효진

직책 : PA

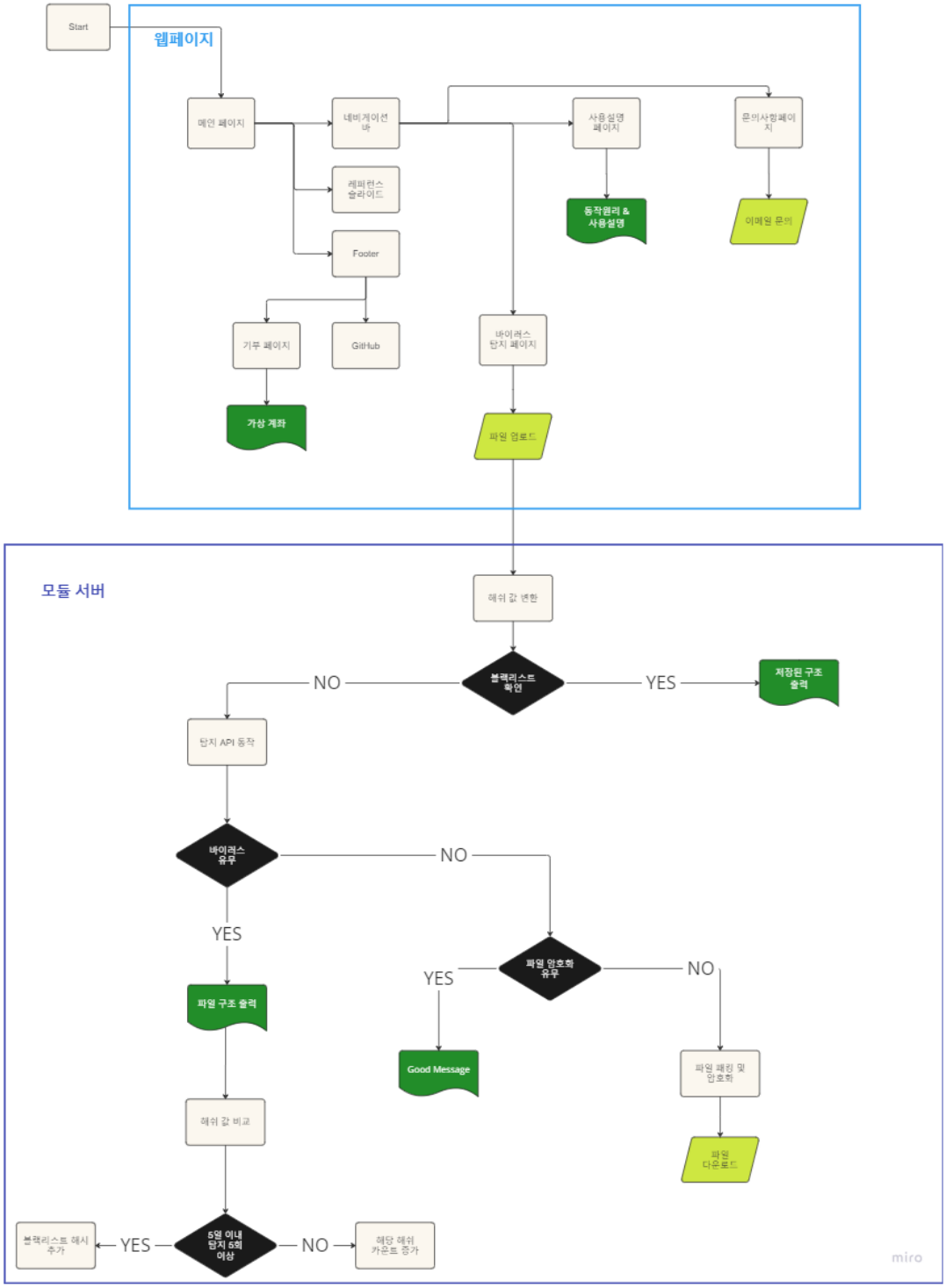
역할

① 프로젝트 일정 관리
② 프로젝트 문서 관리
③ 문서 템플릿 정의
④ QA
⑤ 악성코드 데이터 수집
⑥ 데이터 분류

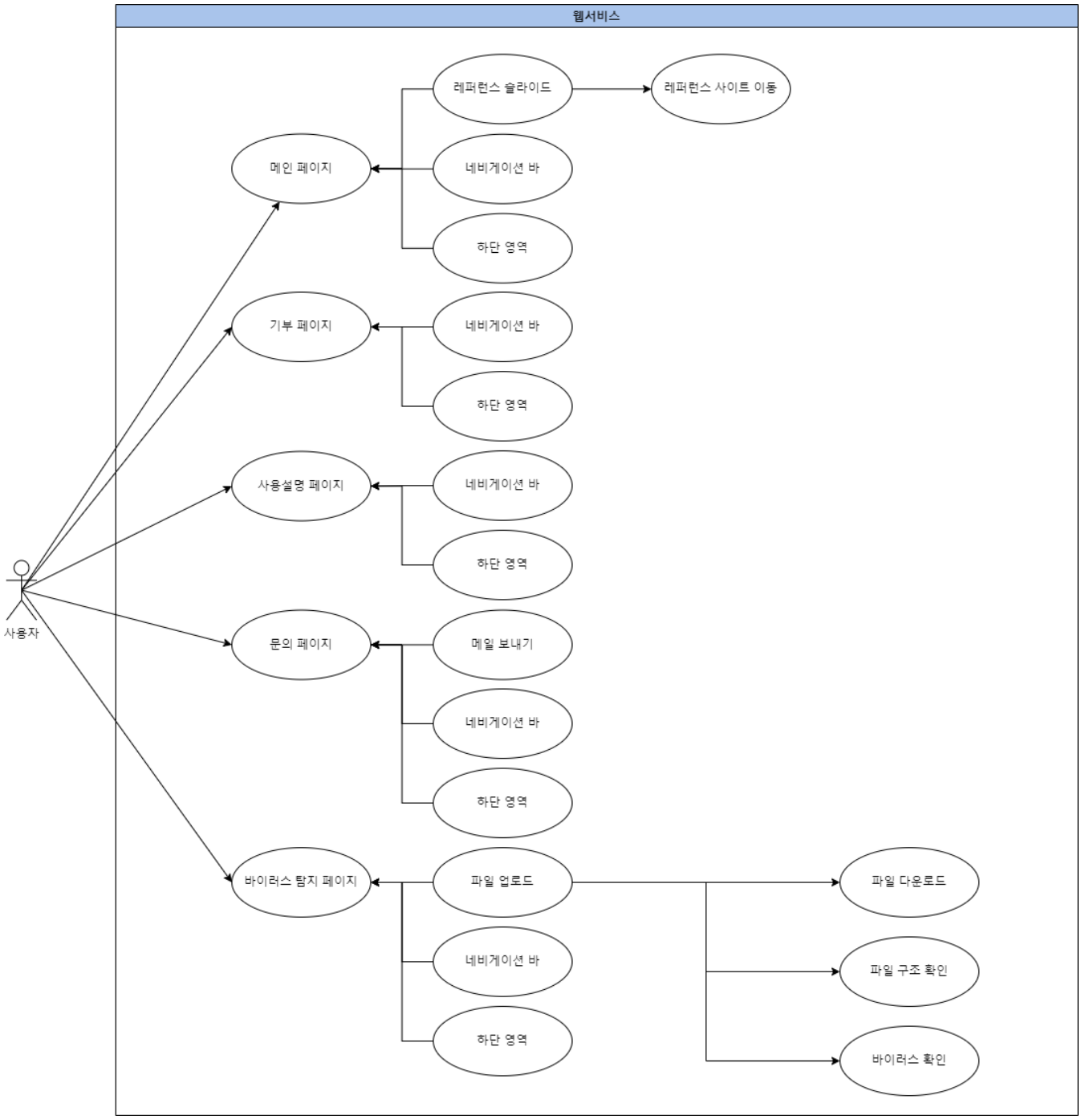
IV. 협업 도구



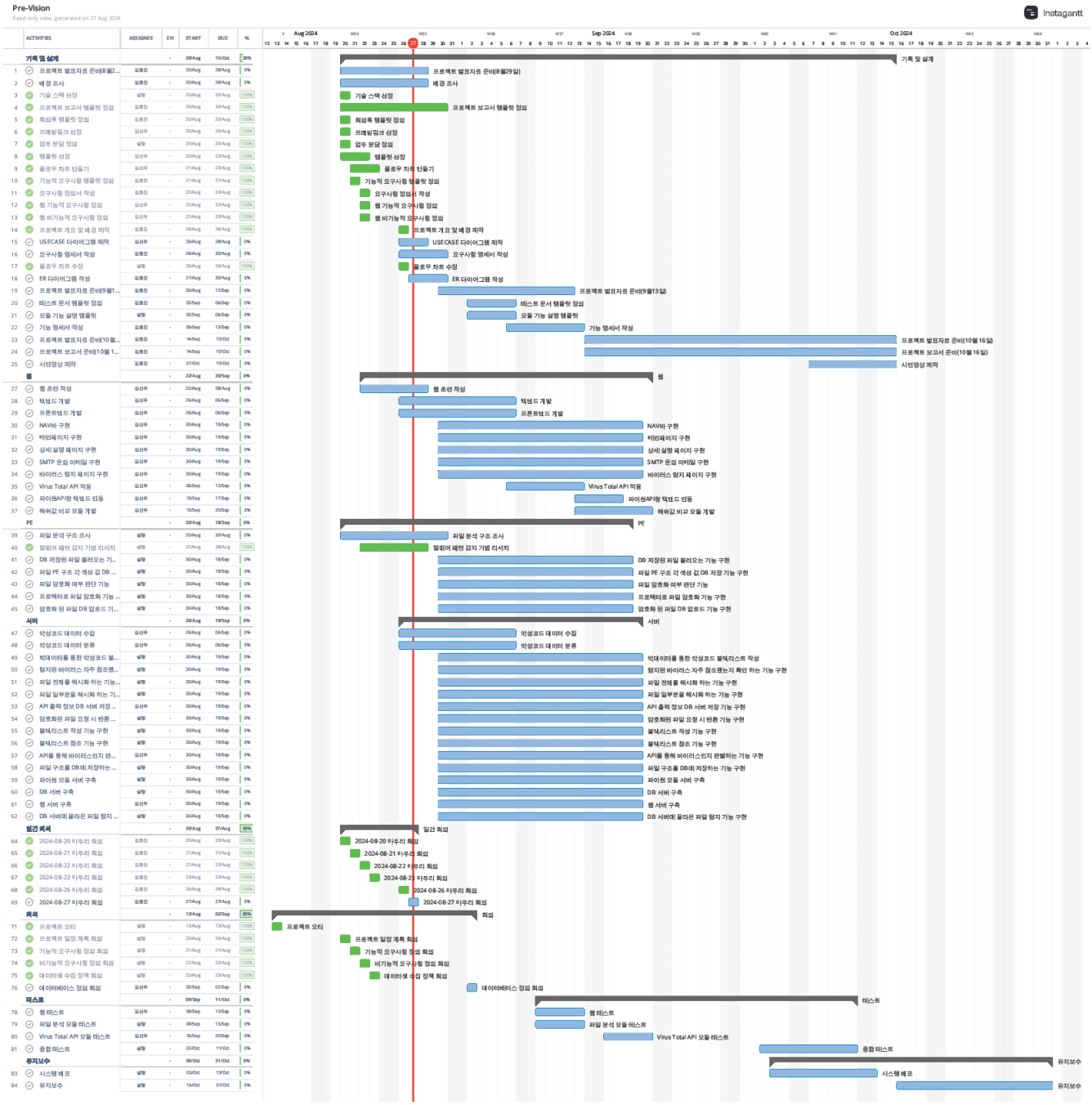
V. FLOW CHART


Start
웹페이지
메인 페이지
네비게이션 바
사용설명 페이지
문의사항페이지
레퍼런스 슬라이드
Footer
동작원리 & 사용설명
이메일 문의
기부 페이지
GitHub
바이러스 탐지 페이지
가상 계좌
파일 업로드
모듈 서버
해쉬 값 변환
블랙리스트 확인
NO
YES
저장된 구조 출력
단지 API 동작
바이러스 유무
NO
YES
파일 암호화 유무
YES
NO
파일 구조 출력
Good Message
파일 패킹 및 암호화
해쉬 값 비교
파일 다운로드
블랙리스트 해시 추가
YES
5일 이내 탐지 5회 이상
NO
해당 해쉬 카운트 증가
miro

VI. USECASE


웹서비스
레퍼런스 슬라이드
레퍼런스 사이트 이동
메인 페이지
네비게이션 바
하단 영역
기부 페이지
네비게이션 바
하단 영역
사용설명 페이지
네비게이션 바
하단 영역
문의 페이지
메일 보내기
네비게이션 바
하단 영역
바이러스 탐지 페이지
파일 업로드
네비게이션 바
하단 영역
파일 다운로드
파일 구조 확인
바이러스 확인
사용자

VII. 프로젝트 일정


Pre-Vision
Read-only view, generated on 27 Aug 2024
Instagantt
ACTIVITIES
ASSIGNEE
EH
START
DUE
%
Aug 2024
Sep 2024
Oct 2024
기획 및 설계
프로젝트 발표자료 준비(8월29일)
배경 조사
기술 스택 선정
프로젝트 보고서 템플릿 정의
회의록 템플릿 정의
프레임워크 선정
업무 분담 정의
템플릿 선정
플로우 차트 만들기
기능적 요구사항 템플릿 정의
요구사항 정의서 작성
웹 기능적 요구사항 정의
웹 비기능적 요구사항 정의
프로젝트 개요 및 배경 제작
USECASE 다이어그램 제작
요구사항 명세서 작성
플로우 차트 수정
ER 다이어그램 작성
프로젝트 발표자료 준비(9월13일)
테스트 문서 템플릿 정의
모듈 기능 설명 템플릿
기능 명세서 작성
프로젝트 발표자료 준비(10월 16일)
프로젝트 보고서 준비(10월 16일)
시연영상 제작
웹
웹 초안 작성
탭뷰도 개발
프론트엔드 개발
NAV바 구현
테이블페이지 구현
상세 설명 페이지 구현
SMTP 문의 이메일 구현
바이러스 탐지 페이지 구현
Virus Total API 적용
파이썬API랑 탭뷰도 연동
해쉬값 비교 모듈 개발
PE
파일 분석 구조 조사
멀웨어 패턴 감지 기법 리서치
DB 저장된 파일 불러오는 기능 구현
파일 PE 구조 각 섹션 값 DB 저장 기능 구현
파일 암호화 여부 판단 기능
프로텍터로 파일 암호화 기능 구현
암호화 된 파일 DB 업로드 기능 구현
서버
악성코드 데이터 수집
악성코드 데이터 분류
빅데이터를 통한 악성코드 블랙리스트 작성
탐지된 바이러스 자주 참조했는지 확인 하는 기능 구현
파일 전체를 해시화 하는 기능 구현
파일 일부분을 해시화 하는 기능 구현
API 출력 정보 DB 서버 저장 기능 구현
암호화된 파일 요청 시 반환 기능 구현
블랙리스트 작성 기능 구현
블랙리스트 참조 기능 구현
API를 통해 바이러스인지 판별하는 기능 구현
파일 구조를 DB에 저장하는 기능 구현
파이썬 모듈 서버 구축
DB 서버 구축
웹 서버 구축
DB 서버에 올라온 파일 탐지 기능 구현
일간 회의
2024-08-20 마무리 회의
2024-08-21 마무리 회의
2024-08-22 마무리 회의
2024-08-23 마무리 회의
2024-08-26 마무리 회의
2024-08-27 마무리 회의
회의
프로젝트 오티
프로젝트 일정 계획 회의
기능적 요구사항 정의 회의
비기능적 요구사항 정의 회의
데이터셋 수집 정책 회의
데이터베이스 정의 회의
테스트
웹 테스트
파일 분석 모듈 테스트
Virus Total API 모듈 테스트
종합 테스트
유지보수
시스템 배포
유지보수

VIII. WBS

분류	작업명	담당자	시작일	종료일	상태
기획 및 설계	배경 조사	김효진	2024-08-20	2024-08-28	
	기술 스택 선정	우건희	2024-08-20	2024-08-20	완료
	프로젝트 보고서 템플릿 정의	김효진	2024-08-20	2024-08-30	완료
	회의록 템플릿 정의	김효진	2024-08-20	2024-08-20	완료
	프레임워크 선정	김선우	2024-08-20	2024-08-20	완료
	업무 분담 정의	우건희	2024-08-20	2024-08-20	완료
	템플릿 선정	김선우	2024-08-20	2024-08-22	완료
	플로우 차트 만들기	김선우	2024-08-21	2024-08-23	완료
	기능적 요구사항 템플릿 정의	김효진	2024-08-21	2024-08-21	완료
	요구사항 정의서 작성	김효진	2024-08-22	2024-08-22	완료
	웹 기능적 요구사항 정의	김선우	2024-08-22	2024-08-22	완료
	웹 비기능적 요구사항 정의	김선우	2024-08-22	2024-08-22	완료
	프로젝트 개요 및 배경 제작	김효진	2024-08-26	2024-08-26	완료
	USECASE 다이어그램 제작	김선우	2024-08-26	2024-08-28	
	요구사항 명세서 작성	김효진	2024-08-26	2024-08-30	
	플로우 차트 수정	우건희	2024-08-26	2024-08-26	완료
	ER 다이어그램 작성	김효진	2024-08-27	2024-08-30	
	프로젝트 발표자료 준비(9월13일)	김효진	2024-08-30	2024-09-12	
	테스트 문서 템플릿 정의	김효진	2024-09-02	2024-09-06	
	모듈 기능 설명 템플릿	우건희	2024-09-02	2024-09-06	
	기능 명세서 작성	김효진	2024-09-06	2024-09-13	
	프로젝트 발표자료 준비(10월 16일)	김효진	2024-09-14	2024-10-15	
	프로젝트 보고서 준비(10월 16일)	김효진	2024-09-14	2024-10-15	
	시연영상 제작	김효진	2024-10-07	2024-10-15	
웹	웹 초안 작성	김선우	2024-08-22	2024-08-28	
	백엔드 개발	김선우	2024-08-26	2024-09-06	
	프론트엔드 개발	김선우	2024-08-26	2024-09-06	
	NAV바 구현	김선우	2024-08-30	2024-09-19	
	메인페이지 구현	김선우	2024-08-30	2024-09-19	
	상세 설명 페이지 구현	김선우	2024-08-30	2024-09-19	
	SMTP 문의 이메일 구현	김선우	2024-08-30	2024-09-19	
	바이러스 탐지 페이지 구현	김선우	2024-08-30	2024-09-19	
	Virus Total API 적용	김선우	2024-09-06	2024-09-13	
	파이썬API랑 백엔드 연동	김선우	2024-09-13	2024-09-17	
	해쉬값 비교 모듈 개발	김선우	2024-09-13	2024-09-20	
PE	파일 분석 구조 조사	우건희	2024-08-20	2024-08-30	
	멀웨어 패턴 감지 기법 리서치	우건희	2024-08-22	2024-08-28	완료
	DB 저장된 파일 불러오는 기능 구현	우건희	2024-08-30	2024-09-18	
	파일 PE 구조 각 섹션 값 DB 저장 기능 구현	우건희	2024-08-30	2024-09-18	
	파일 암호화 여부 판단 기능	우건희	2024-08-30	2024-09-18	
	프로텍터로 파일 암호화 기능 구현	우건희	2024-08-30	2024-09-18	
	암호화 된 파일 DB 업로드 기능 구현	우건희	2024-08-30	2024-09-18	
서버	악성코드 데이터 수집	김선우	2024-08-26	2024-09-06	
	악성코드 데이터 분류	김선우	2024-08-26	2024-09-06	
	빅데이터를 통한 악성코드 블랙리스트 작성	우건희	2024-08-30	2024-09-19	
	탐지된 바이러스 자주 참조됐는지 확인 하는 기능 구현	우건희	2024-08-30	2024-09-19	
	파일 전체를 해시화 하는 기능 구현	우건희	2024-08-30	2024-09-19	
	파일 일부분을 해시화 하는 기능 구현	우건희	2024-08-30	2024-09-19	
	API 출력 정보 DB 서버 저장 기능 구현	김선우	2024-08-30	2024-09-19	
	암호화된 파일 요청 시 반환 기능 구현	우건희	2024-08-30	2024-09-19	
	블랙리스트 작성 기능 구현	우건희	2024-08-30	2024-09-19	
	블랙리스트 참조 기능 구현	우건희	2024-08-30	2024-09-19	
	API를 통해 바이러스인지 판별하는 기능 구현	김선우	2024-08-30	2024-09-19	
	파일 구조를 DB에 저장하는 기능 구현	우건희	2024-08-30	2024-09-19	
	파이썬 모듈 서버 구축	우건희	2024-08-30	2024-09-19	
	DB 서버 구축	우건희	2024-08-30	2024-09-19	
	웹 서버 구축	김선우	2024-08-30	2024-09-19	
	DB 서버에 올라온 파일 탐지 기능 구현	우건희	2024-08-30	2024-09-19	
일간 회의	2024-08-20 마무리 회의	김효진	2024-08-20	2024-08-20	완료
	2024-08-21 마무리 회의	김효진	2024-08-21	2024-08-21	완료
	2024-08-22 마무리 회의	김효진	2024-08-22	2024-08-22	완료
	2024-08-23 마무리 회의	김효진	2024-08-23	2024-08-23	완료
	2024-08-26 마무리 회의	김효진	2024-08-26	2024-08-26	완료
	2024-08-27 마무리 회의	김효진	2024-08-27	2024-08-27	
회의	프로젝트 오티	우건희	2024-08-13	2024-08-13	완료
	프로젝트 일정 계획 회의	우건희	2024-08-20	2024-08-20	완료
	기능적 요구사항 정의 회의	우건희	2024-08-21	2024-08-21	완료
	비기능적 요구사항 정의 회의	우건희	2024-08-22	2024-08-22	완료
	데이터셋 수집 정책 회의	우건희	2024-08-23	2024-08-23	완료
	데이터베이스 정의 회의	김선우	2024-09-02	2024-09-02	
테스트	웹 테스트	김선우	2024-09-09	2024-09-13	
	파일 분석 모듈 테스트	우건희	2024-09-09	2024-09-13	
	Virus Total API 모듈 테스트	김선우	2024-09-16	2024-09-20	
	종합 테스트	우건희	2024-10-02	2024-10-11	
유지보수	시스템 배포	우건희	2024-10-03	2024-10-13	
	유지보수	우건희	2024-10-16	2024-10-31	

요구사항 정의서

문 서 명	요구사항 정의서	문서번호	TR-003	작성자	우건희
	서버	작 업	요구사항파악	작성일	2024.08.27
				버 전	1.1

번호	업무	요구사항 ID	요구사항 명	비고
1	신규기능 선정	FR-301	빅데이터를 통한 악성코드 블랙리스트 작성	
2		FR-302	암호화된 파일 요청 시 반환 기능	
3		FR-303	파일 전체를 해시화 하는 기능	
4		FR-304	파일 일부분을 해시화 하는 기능	
5		FR-305	API 출력 정보 DB 서버 저장 기능	
6		FR-306	탐지된 바이러스 자주 참조됐는지 확인하는 기능	
7		FR-307	블랙리스트 작성 기능	
8		FR-308	블랙리스트 참조 기능	
9		FR-309	API 를 통해 바이러스인지 판별하는 기능	
10		FR-310	파일 구조를 DB 에 저장하는 기능	
11		FR-311	DB 서버에 올라온 파일 탐지 기능	
12		FR-312	파이썬 모듈 서버 구축	
13		FR-313	DB 서버 구축	
14		FR-314	웹 서버 구축	
15				

<>

1

문 서 명	요구사항 정의서	문서번호	TR-002	작성자	우건희
	PE	작 업	요구사항파악	작성일	2024.08.27
				버 전	1.1

번호	업무 영역	요구사항 ID	요구사항 명	비고
1	신규기능 선정	FR-201	DB 저장된 파일 불러오는 기능	
2		FR-202	파일 PE 구조 각 섹션 값 DB 저장 기능	
3		FR-203	파일 암호화 여부 판단 기능	
4		FR-204	프로텍터를 통한 파일 암호화 기능	
5		FR-205	암호화 된 파일 DB 업로드 기능	
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

문 서 명	요구사항 정의서	문서번호	TR-001	작성자	김선우
	웹	작 업	요구사항파악	작성일	2024.08.27
				버 전	1.1

번호	업무 영역	요구사항 ID	요구사항 명	비고
1	신규기능 선정	FR-101	메인 로고 클릭 시 메인페이지 Redirect 기능	
2		FR-102	기부 페이지 Redirect기능	
3		FR-103	사용설명 페이지 Redirect 기능	
4		FR-104	문의 페이지 Redirect 기능	
5		FR-104-01	SMTP 이용해 관리자와 메일을 주고 받는 기능	
6		FR-105	개발팀 Github 페이지 Redirect 기능	
7		FR-106	파일업로드페이지 Redirect 기능	
8		FR-106-01	파일업로드되면 스캔(바이러스 탐지)하고 구조출력	
9		FR-106-01-1	바이러스가 없으면 암호화유무 파악 후 파일 암호화	
10		FR-107	reference 이미지 각각 페이지로 redirect 기능	

문 서 명	비기능적 요구사항 정의서	문서번호	TR-101	작성자	김선우
	웹	작 업	요구사항 파악	작성일	2024.8.27
				버 전	1.0

번호	유형	요구사항 ID	요구사항 명	비고
1	신규기능 선정	NFR-101	성능 : 파일 스캔 결과의 신속한 출력	
2		NFR-102	성능 : 파일 크기 제한	
3		NFR-103	성능 : 다수의 사용자의 동시접속 원할	
4		NFR-104	안정성 : 예상치 못한 오류 발생시 사용자에게 명확한 메세지 출력	
5		NFR-105	안정성 : 사용자 데이터의 손실 및 변조방지	
6		NFR-106	보안 : 파일의 중요한 정보를 안전하게 관리	
7		NFR-107	보안 : 외부 공격으로부터 시스템 보호	
8		NFR-108	보안 : 서비스 처리가 끝난 사용자의 파일은 즉시 제거	
9		NFR-109	사용성 : 사용자에게 직관적인 UI 제공	
10		NFR-110	사용성 : 사용자가 이해할 수 있는 명확한 오류 메세지 제공	
11		NFR-111	유지보수성 : 체계적인 코드관리를 통해 유지보수 용이	
12		NFR-112	유지보수성 : 시스템 운영 로그를 기록하여 문제 발생시 원인 분석 용이	

IX. 요구사항 명세서

문 서 명	요구사항 명세서 – 웹	문서번호	FR-101	작성자	김선우
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정	
요구사항 ID	FR-101	요구사항 명	메인 로고 클릭 시 메인페이지 Redirect 기능
개요	메인페이지로 쉽게 이동하게 Redirect 기능 추가		
요구사항 내역 / 상세설명	사용자가 어느페이지에 있더라도 좌측상단에 로고버튼만 클릭하면 메인페이지로 이동할 수 있게 Redirect 기능.		
요구사항 내역 / 유형	기능		
요구사항 내역 / 중요도	상	난이도	하

<회사 로고>

1

문 서 명	요구사항 명세서 - 웹	문서번호	FR-102	작성자	김선우
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정	
요구사항 ID	FR-102	요구사항 명	기부 페이지 Redirect 기능
개요	사용자가 원하면 기부페이지로 이동할 수 있는 기능.		
요구사항 내역	상세설명	사용자가 메인페이지에서 해당 태그를 클릭하면 기부페이지로 Redirect 할 수 있다.	
	유형	기능	
	중요도	하	난이도	하

문 서 명	요구사항 명세서 - 웹	문서번호	FR-103	작성자	김선우
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정	
요구사항 ID	FR-103	요구사항 명	사용설명페이지 Redirect 기능
개요	쉽게 사용할 수 있게 사용설명페이지로 Redirect 해서 상세한 설명을 알려준다.		
요구사항 내역	상세설명	누구가 쉽게 사용할 수 있게 해당 태그를 사용자가 클릭 시 사용설명페이지로 Redirect 하고 상세한 동작원리 & 사용설명서를 보여준다.	
	유형	기능	
	중요도	상	난이도	하

문 서 명	요구사항 명세서 - 웹	문서번호	FR-104	작성자	김선우
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-104	요구사항 명	문의페이지 Redirect 기능
개요		사용자가 서비스를 이용하하면서 언제든지 관리자에게 문의가능.		
요구사항 내역	상세설명	사용자가 서비스를 이용중 오류발생 & 불만사항 & 궁금한 점이 생길 시 언제든지 관리자에게 문의가 가능하다.		
	유형	기능		
	중요도	상	난이도	

문 서 명	요구사항 명세서 - 웹	문서번호	FR-104-01	작성자	김선우
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-104-01	요구사항 명	SMTP 이용하여 관리자와 메일을 주고 받는 기능.
개요		사용자가 문의사항을 제출할 때 SMTP 를 이용해 관리자와 메일을 주고 받는다.		
요구사항 내역	상세설명	사용자가 문의사항을 제출할할 때 SMTP(Simple Mail Transfer Protocol)를 사용하여 메일을 주고 받는다.		
	유형	기능		
	중요도	상	난이도	중

문 서 명	요구사항 명세서 - 웹	문서번호	FR-105	작성자	김선우
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-105	요구사항 명	개발팀 Github 페이지 Redirect 기능
개요		사용자가 해당 태그를 클릭 시 개발팀 Github 페이지로 이동할 수 있다.		
요구사항 내역	상세설명	사용자가 해당 태그를 클릭 시 개발팀 Github 페이지로 이동해서 소스코드를 볼 수 있다.		
	유형	기능		
	중요도	중	난이도	하

문 서 명	요구사항 명세서 - 웹	문서번호	FR-106	작성자	김선우
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-106	요구사항 명	파일업로드페이지 Redirect 기능
개요		사용자가 서비스 이용을 위해 실제 파일을 업로드할 수 있게 페이지로 Redirect 한다.		
요구사항 내역	상세설명	사용자가 서비스 이용을 위해 실제 파일을 업로드할 수 있게 해당 페이지에서 파일 업로드함.		
	유형	기능		
	중요도	상	난이도	하

문 서 명	요구사항 명세서 - 웹	문서번호	FR-106-01	작성자	김선우
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정	
요구사항 ID	FR-106-01	요구사항 명	파일이 업로드되면 스캔(바이러스 탐지)하고 구조출력
개요	사용자가 파일을 업로드했을 시 즉시 스캐닝해서 바이러스를 탐지한다.		
요구사항 내역 / 상세설명	사용자가 파일을 업로드했을 시 즉시 스캐닝해서 바이러스를 탐지하고 UI 로 스캔이 정상작동중이라는걸 보여준다. 개발팀 DB 서버의 블랙리스트에 있는 바이러스가 검출되었을 시 구조를 출력. 블랙리스트에 없을 시 탐지 API 가 동작해서 해당 API 에서 바이러스 탐지 후 구조를 출력.		
요구사항 내역 / 유형	기능		
요구사항 내역 / 중요도	상	난이도	상

문 서 명	요구사항 명세서 - 웹	문서번호	FR-106-01-1	작성자	김선우
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정	
요구사항 ID	FR-106-01-1	요구사항 명	바이러스가 없으면 암호화 유무파악 후 즉시 파일 암호화
개요	FR-106-01 기능이후에 바이러스가 없다면 암호화유무를 파악 후 즉시 파일 암호화해서 사용자에게 제공		
요구사항 내역 / 상세설명	FR-106-01 기능이 완료되면 바이러스가 없으면 파일의 암호화 유무를 파악하고 암호화가 안되어있다면 즉시 파일암호화해서 사용자에게 제공한다.		
요구사항 내역 / 유형	기능		
요구사항 내역 / 중요도	상	난이도	상

문 서 명	요구사항 명세서 - 웹	문서번호	FR-107	작성자	김선우
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정	
요구사항 ID	FR-107	요구사항 명	Reference 이미지 각각 페이지로 Redirect 기능
개요	개발팀에서 참고한 레퍼런스사이트와 이미지를 메인페이지에서 UI 로 보여준다.		
요구사항 내역	상세설명	개발팀에서 참고한 레퍼런스사이트와 이미지를 메인페이지에서 사용자에게 직관적인 UI 로 보여준다.	
	유형	기능	
	중요도	중	난이도	중

문 서 명	요구사항 명세서 - PE	문서번호	FR-201	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정	
요구사항 ID	FR-201	요구사항 명	DB 저장된 파일 불러오는 기능
개요	DB 에 저장되어 있는 파일을 처리하기 위해 모듈 서버에 불러온다.		
요구사항 내역	상세설명	사용자가 업로드 버튼을 통해 DB 에 저장한 파일을 처리하기 위한 전처리 과정이다. 해당 파일을 DB 에서 불러와서 FR-200 번대의 기능을 수행한다.	
	유형	기능	
	중요도	상	난이도	중

문 서 명	요구사항 명세서 - PE	문서번호	FR-202	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-202	요구사항 명	파일 PE 구조 각 섹션 값 DB 저장 기능
개요		파일의 PE 구조를 분석하고 섹션 값을 DB에 저장한다.		
요구사항 내역	상세설명	사용자가 업로드 버튼을 통해 DB 서버에 저장한 파일을 가져와서 해당 파일의 PE 구조를 분석한다. 출력된 각 섹션의 데이터를 DB에 저장한다.		
	유형	기능		
	중요도	상	난이도	하

문 서 명	요구사항 명세서 - PE	문서번호	FR-203	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-203	요구사항 명	파일 암호화 여부 판단 기능
개요		악성코드가 아닌 파일에 한해 파일이 암호화되어 있는지 확인한다.		
요구사항 내역	상세설명	사용자가 업로드 버튼을 통해 DB에 저장한 파일이 악성코드가 아닐 경우, FR-202 기능을 통하여 구조를 파악한 후 Entropy 알고리즘을 통해 각 섹션의 엔트로피를 계산 계산된 엔트로피가 높다면 암호화 또는 난독화가 적용된 것 파일이고 해당 파일일 경우는 웹페이지에서 Good Message를 출력한다. 만약 엔트로피가 낮다면 해당 파일이 암호화 또는 난독화가 적용되지 않은 파일이고 해당 파일일 경우 FR-204 기능으로 진행된다.		
	유형	기능		
	중요도	상	난이도	상

문 서 명	요구사항 명세서 - PE	문서번호	FR-204	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-204	요구사항 명	프로텍터를 통한 파일 암호화 기능
개요		오픈소스 프로텍터를 사용해 파일을 암호화한다.		
요구사항 내역	상세설명	PE-Protector 라는 오픈 소스 protector 를 통해 파일을 패킹하면서 암호화한다.		
	유형	기능		
	중요도	상	난이도	상

문 서 명	요구사항 명세서 - PE	문서번호	FR-205	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-205	요구사항 명	암호화된 파일 DB 업로드 기능
개요		암호화된 파일을 DB 에 업로드 한다.		
요구사항 내역	상세설명	FR-204 기능을 실행되어 암호화가 진행된 파일에 대해 DB 에 해당 파일을 업로드 한다.		
	유형	기능		
	중요도	상	난이도	하

문 서 명	요구사항 명세서 - 서버	문서번호	FR-301	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-301	요구사항 명	빅데이터를 통한 악성코드 블랙리스트 작성
개요		빅데이터의 해시 정보로 악성코드 블랙리스트화		
요구사항 내역	상세설명	악성코드 해시 정보가 들어있는 빅데이터를 모은 후 해당 빅데이터에서 필요한 정보 추출(해시, 파일 섹션 정보 등) 해당 정보로 ER 도식화 및 데이터베이스 생성		
	유형	기능		
	중요도	상	난이도	하

문 서 명	요구사항 명세서 - 서버	문서번호	FR-302	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-302	요구사항 명	암호화된 파일 요청 시 반환 기능
개요		웹 서비스가 암호화된 파일을 요청하면 반환		
요구사항 내역	상세설명	사용자가 웹 브라우저에서 암호화된 파일을 다운 받는 버튼을 클릭했을 시 DB 에서 저장된 파일 반환해 줌		
	유형	기능		
	중요도	상	난이도	중

문 서 명	요구사항 명세서 - 서버	문서번호	FR-303	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-303	요구사항 명	파일 전체를 해시화 하는 기능
개요		블랙리스트 작성을 위한 파일 해시화		
요구사항 내역	상세설명	사용자로부터 업로드 된 파일 FR-310 기능 진행과 동시에 해당 내용을 바탕으로 파일 해시화 및 DB 서버 저장		
	유형	기능		
	중요도	상	난이도	중

문 서 명	요구사항 명세서 - 서버	문서번호	FR-304	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-304	요구사항 명	파일 일부분을 해시화 하는 기능
개요		블랙리스트 작성을 위해 파일 일부분을 해시화		
요구사항 내역	상세설명	사용자로부터 업로드 된 파일을 FR-310 기능을 실행함과 동시에 악성코드가 많이 삽입되는 섹션만 따로 종합해서 해시화 한 후 DB 에 저장 전체를 통한 블랙리스트시 사용되지 않을 수도 있음		
	유형	기능		
	중요도	하	난이도	중

문 서 명	요구사항 명세서 - 서버	문서번호	FR-305	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-305	요구사항 명	API 출력 정보 DB 서버 저장 기능
개요		악성코드 탐지 API 를 통해 얻은 중요한 정보를 DB 서버에 저장한다.		
요구사항 내역	상세설명	사용자가 올린 악성코드 파일을 악성코드 탐지 API 로 분석한다. 해당 API 를 통해 나온 정보와 악성코드 유무 판별 등을 구축된 DB 서버에 저장한다.		
	유형	기능		
	중요도	상	난이도	하

문 서 명	요구사항 명세서 - 서버	문서번호	FR-306	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-306	요구사항 명	탐지된 바이러스 자주 참조됐는지 확인하는 기능
개요		악성코드 바이러스 탐지 참조 확인 기능		
요구사항 내역	상세설명	기존 블랙리스트에 없던 악성코드가 API 를 통해 단기간에 5 번 이상 탐지가 됐는지 확인하고 탐지가 될 때 마다 DB 서버의 탐지 카운트가 증가하는 기능		
	유형	기능		
	중요도	중	난이도	중

문 서 명	요구사항 명세서 - 서버	문서번호	FR-307	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-307	요구사항 명	블랙리스트 작성 기능
개요		블랙리스트 DB에 추가하는 기능이다.		
요구사항 내역	상세설명	FR-306 기능을 통해 해당 악성코드 파일이 자주 참조되었다면 파일의 PE 섹션에 중요 정보, API를 통해 나온 정보 등을 통합하여 블랙리스트 DB에 추가한다.		
	유형	기능		
	중요도	중	난이도	상

문 서 명	요구사항 명세서 - 서버	문서번호	FR-308	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-308	요구사항 명	블랙리스트 참조 기능
개요		악성코드 탐지 시간을 줄이기 위한 블랙리스트(빅데이터) 참조 기능		
요구사항 내역	상세설명	사용자가 업로드 버튼을 통해 파일을 업로드하게 되면 해당 파일의 해쉬 값이 블랙리스트에 있는 값인지 확인하는 기능 만약 블랙리스트에 있는 값이면 기존에 블랙리스트에 저장되어 있는 PE 섹션의 중요한 값을 반환해줌		
	유형	기능		
	중요도	중	난이도	중

문 서 명	요구사항 명세서 - 서버	문서번호	FR-309	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-309	요구사항 명	API 를 통해 바이러스인지 판별하는 기능
개요		사용자가 파일을 업로드 했을 때 해당 파일이 악성코드가 삽입된 파일인지 여부를 판별		
요구사항 내역	상세설명	사용자가 업로드 버튼을 통해 파일을 업로드 하면 해당 파일이 바이러스인지 확인한 후 다음 기능을 수행함 FR-305		
	유형	기능		
	중요도	상	난이도	상

문 서 명	요구사항 명세서 - 서버	문서번호	FR-310	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-310	요구사항 명	파일 구조를 DB 에 저장하는 기능
개요		사용자 파일을 분석해 해당 구조를 DB 에 저장하는 기능		
요구사항 내역	상세설명	바이러스 탐지 이후 해당 파일의 구조를 정적 분석을 통해 얻고 해당 정보를 DB 에 저장한다		
	유형	기능		
	중요도	상	난이도	하

문 서 명	요구사항 명세서 - 서버	문서번호	FR-311	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-311	요구사항 명	DB 서버에 올라온 파일 탐지 기능
개요		사용자가 올린 파일이 DB 서버에 올라왔는지 확인하는 기능		
요구사항 내역	상세설명	사용자가 업로드 버튼을 통해 파일을 DB 서버에 업로드 하게 될 시 모듈 서버에서 DB 서버에 파일이 올라왔는지 확인을 하고 모듈이 작동되야 하기 때문에 DB 서버를 탐지하는 기능이 필요함		
	유형	기능		
	중요도	상	난이도	상

<회사 로고>

문 서 명	요구사항 명세서 - 서버	문서번호	FR-312	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-312	요구사항 명	파이썬 모듈 서버 구축
개요		파이썬 모듈을 실행하기 위한 서버 구축		
요구사항 내역	상세설명	해당 서버에서는 PE 파일 구조 파악, 프로텍터를 통한 암호화, API 를 통한 악성코드 탐지, 블랙리스트 참조 등 핵심 모듈들이 실행되는 서버 악성코드 탐지 API 가 실행될 수 있는 환경으로 구축해야 하기 때문에 클라우드 환경에서는 제약이 있을 수 있음 따라서 클라우드 환경에 제약이 있다면 VM 을 사용하여 구축		
	유형	기능		
	중요도	상	난이도	하

<회사 로고>

문 서 명	요구사항 명세서 - 서버	문서번호	FR-313	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-313	요구사항 명	DB 서버 구축
개요		파일 구조 데이터, 블랙리스트 데이터 등을 저장하기 위한 DB 서버 구축		
요구사항 내역	상세설명	API 를 통해서 나온 핵심 정보 저장하기 위한 DB, 악성코드 빅데이터를 통해 만들 블랙리스트 DB, 파일 구조를 저장할 DB 등을 관리하기 위한 DB 서버다. 파이썬 모듈 서버와 같이 해당 DB 서버에 악성코드가 올라가야 하기 때문에 클라우드 서버가 제한될 수 있다. 따라서 마찬가지로 VM을 활용한 서버 구축도 고려해야 한다. DB 서버 구축 이후 ER 다이어그램을 통한 DB, Table 정의를 해야한다.		
	유형	기능		
	중요도	상	난이도	하

문 서 명	요구사항 명세서 - 서버	문서번호	FR-314	작성자	우건희
				작성일	2024.08.27
				버 전	1.1

업무 영역		신규기능 선정		
요구사항 ID		FR-314	요구사항 명	웹 서버 구축
개요		사용자가 웹페이지에 접속할 수 있도록 웹 서버 구축		
요구사항 내역	상세설명	사용자가 서비스를 이용하기 위해 웹 서버를 구축한다. 웹 서버의 프론트는 리액트, 백엔드는 노드 JS 가 사용될 것이다.		
	유형	기능		
	중요도	상	난이도	하