Pre-Vision

차세대 파일 보호:
악성코드 탐지, 암호화 및 패키징

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

ⓒSaebyeol Yu. Saebyeol's PowerPoint

목차 a table of contents

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 1

프로젝트 개요

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 1

프로젝트 개요

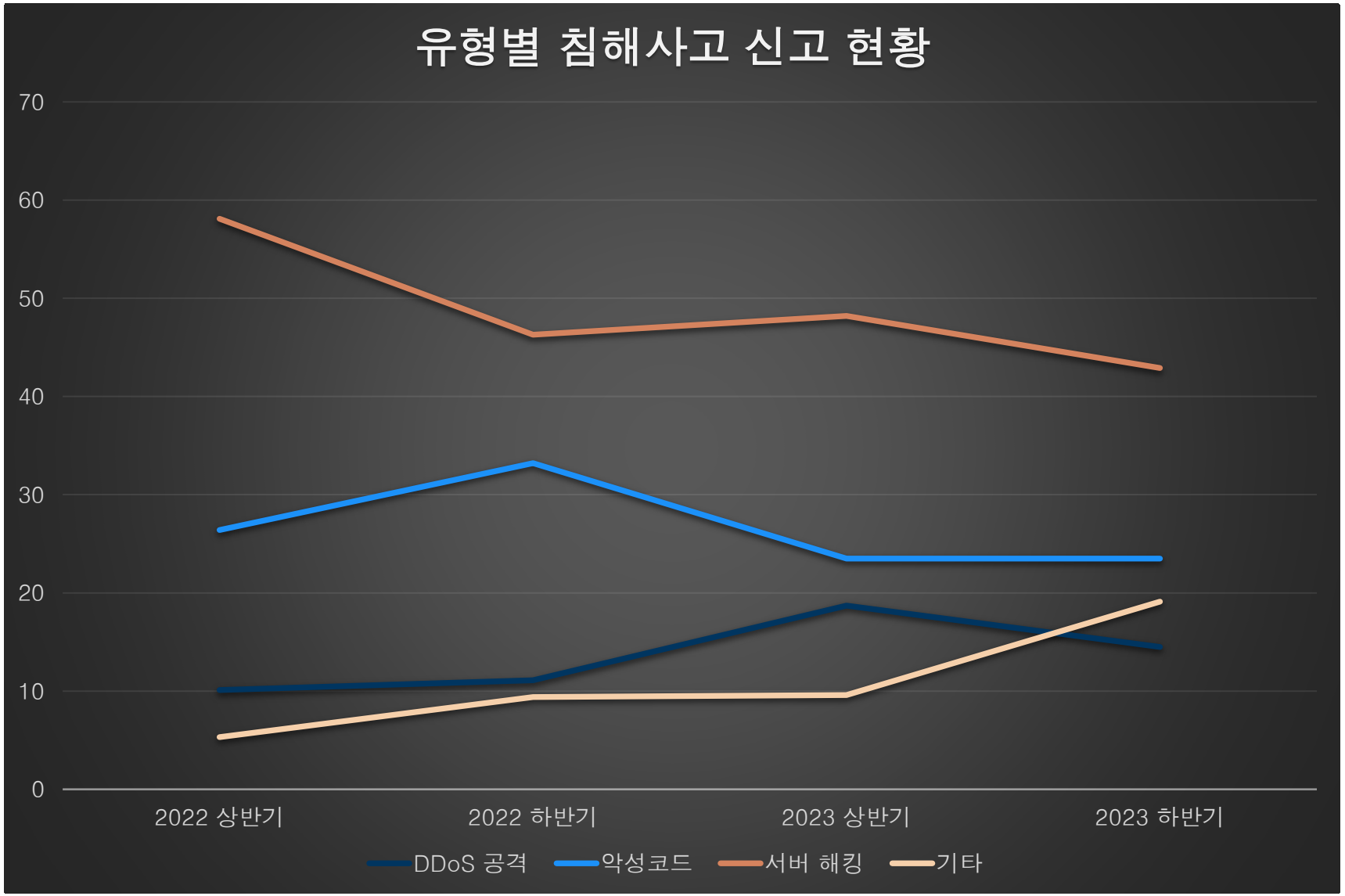
차세대 파일 보호

인터넷의 발달로 윈도우 기반 서비스가 증가하면서 해킹 기법도 빠르게 진화하고 있습니다. 특히 피싱 사이트나 이메일 등을 통해 유포되는 악성 프로그램들은 사용자 파일을 암호화하거나 비밀번호를 탈취하는 등의 심각한 피해를 초래합니다. 또한, 인디게임 시장의 성장과 함께 리버스 엔지니어링을 통해 게임 소스 코드가 불법 복제되거나 악용되는 사례가 늘어나 개발자의 지적 재산과 수익 모델에 큰 위협이 되고 있습니다.

ⓒSaebyeol Yu. Saebyeol's PowerPoint

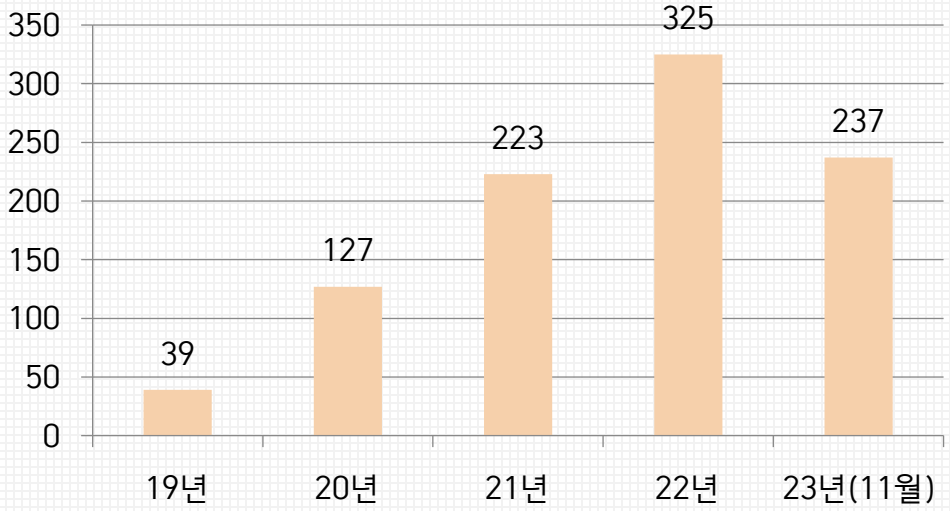
Part 1

한국인터넷진흥원 침해사고 신고 현황

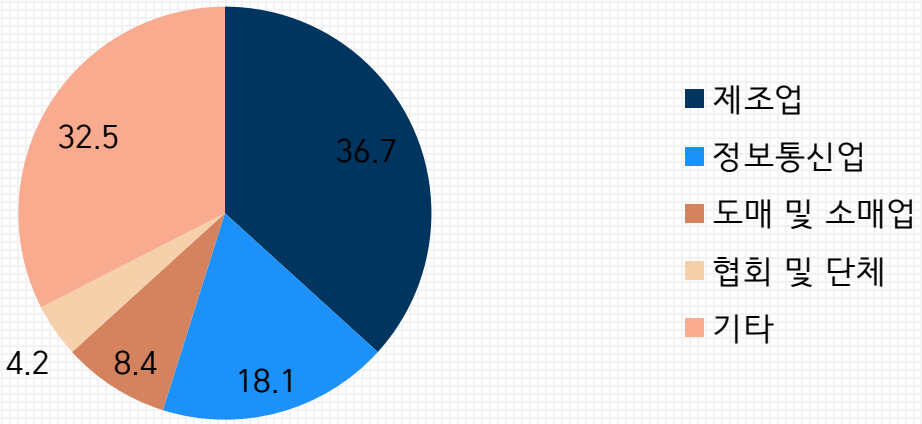


ⓒSaebyeol Yu. Saebyeol's PowerPoint

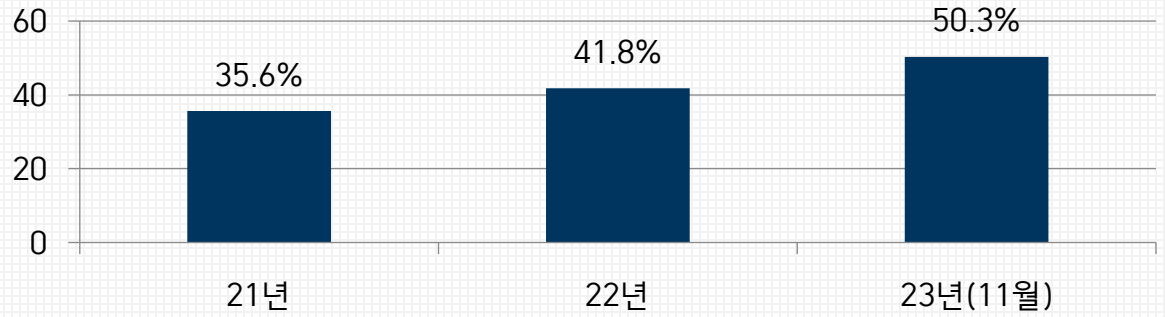
연도별 랜섬웨어 신고 건수



업종별 랜섬웨어 신고 비율(23.11월 기준)



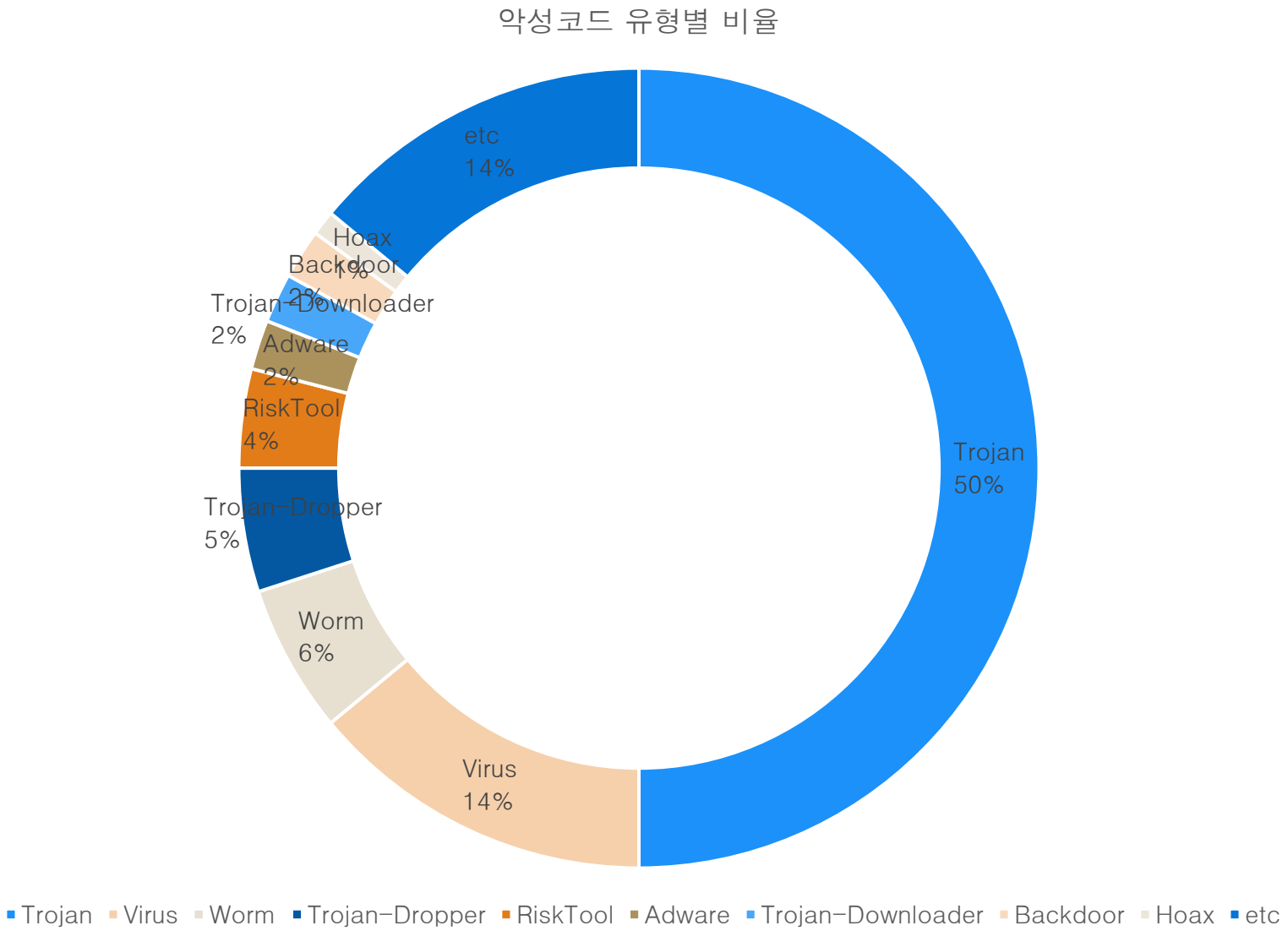
랜섬웨어 피해 중소기업 백업 보유 비율



ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 1

악성코드 유형별 비율

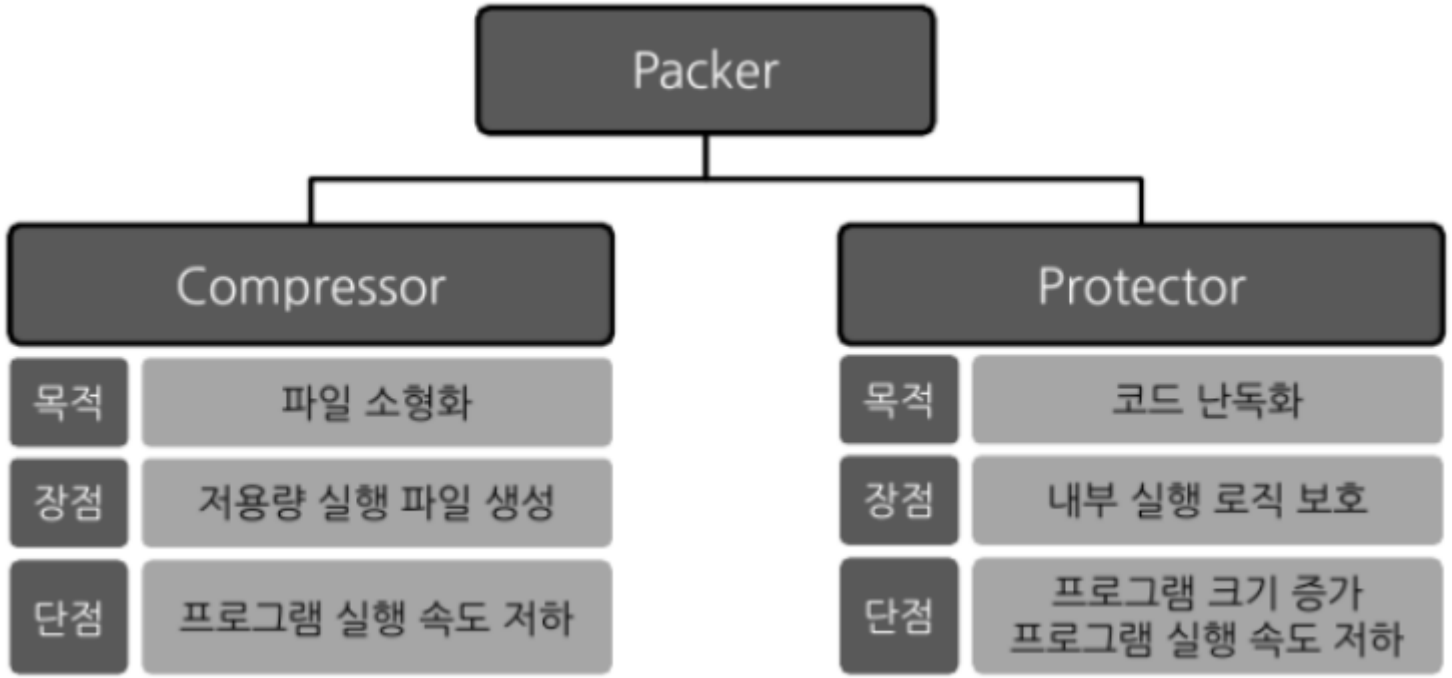


ⓒSaebyeol Yu. Saebyeol's PowerPoint

패킹이란?

패킹?

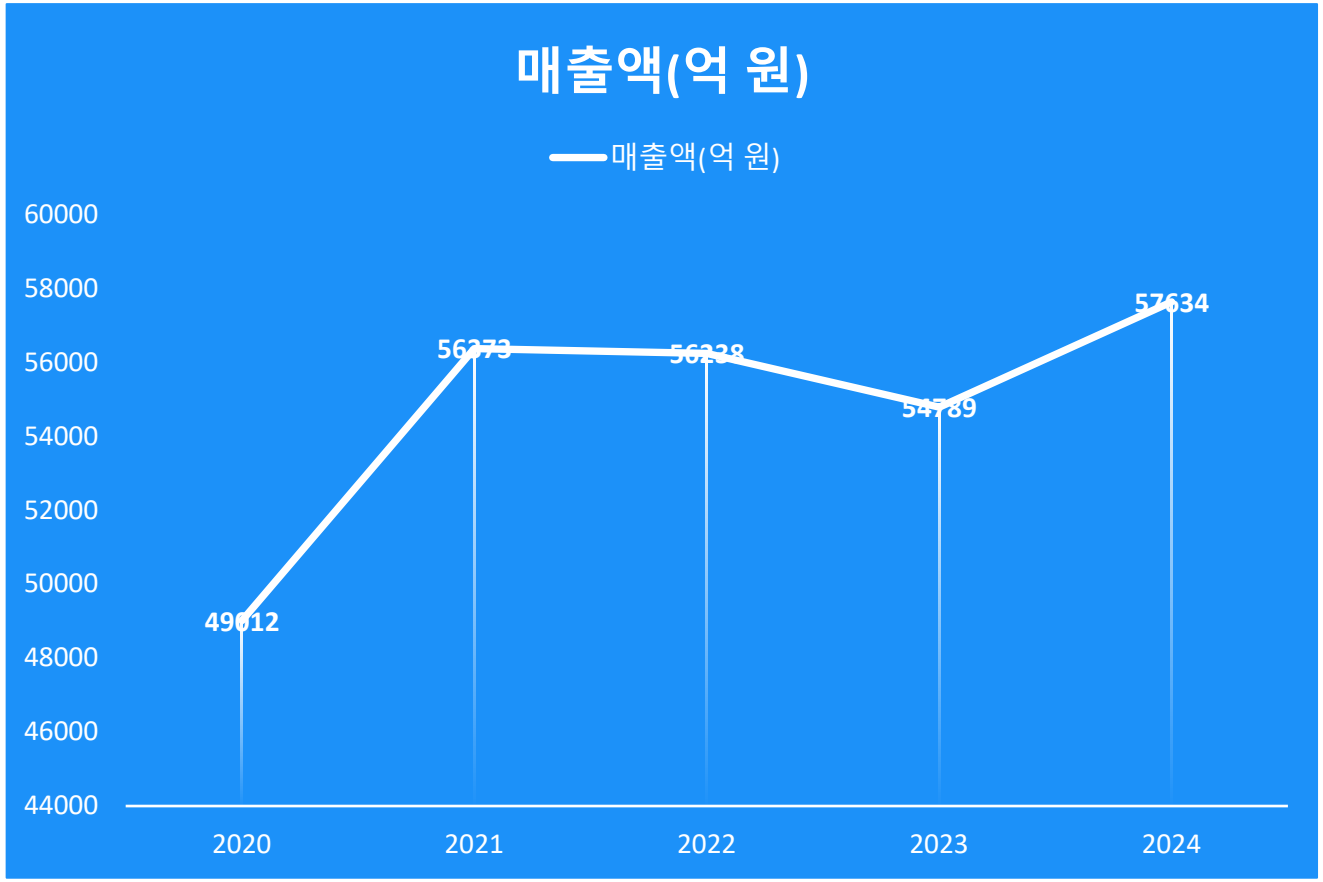
프로그램 코드 크기를 줄이려고 압축하거나 프로그램 분석을 어렵게 만들려고 암호화하는 것

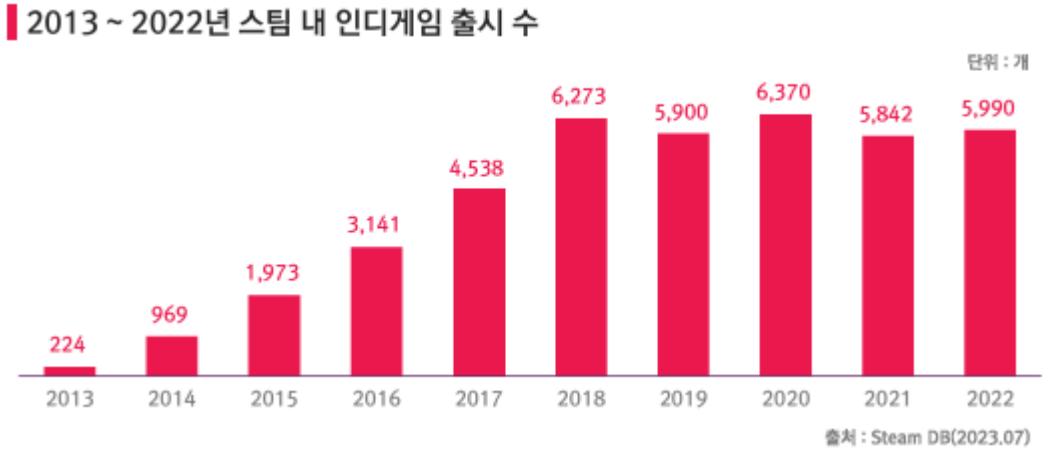


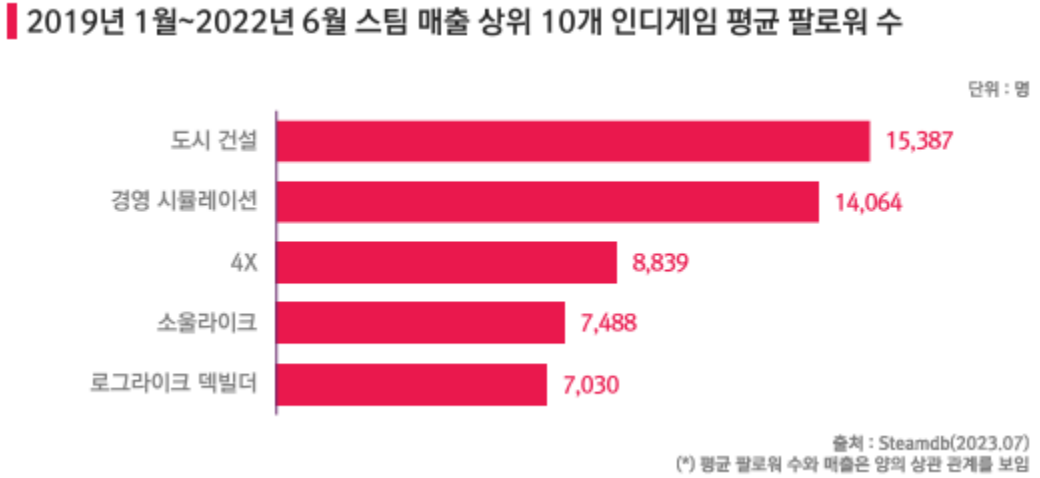
ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 1

인디게임 산업 동향







ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 1

게임사들이 많이 쓰는 데누보

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)

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 1

프로젝트 목표

악성 코드 탐지

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.

암호화 및 프로텍터를 통한 패킹 기법

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.

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 1

프로젝트 기대효과

악성코드 탐지 및 신속 대응

PE 파일을 분석하여 악성코드를 탐지하고, 백신 개발자들에게 필요한 정보를 제공함으로써 새로운 위협에 빠르게 대응할 수 있도록 지원합니다.

인디게임 개발자 보호

리버스 엔지니어링으로 인한 소스 코드 유출, 불법 복제, 악성코드 삽입 등의 위험을 예방하여 인디게임 개발자들이 창의적인 작업에 집중할 수 있도록 돕습니다.

경제적 이익 극대화

보안 사고로 인한 재정적 손실을 줄이고, 게임 파일 보호를 통해 불법 복제로 인한 매출 손실을 예방하여 경제적 이익을 극대화할 수 있습니다.

사이버 보안 산업 발전 기여

악성코드 탐지와 파일 보호 분야에서 새로운 표준을 제시하며, 관련 업계의 전반적인 수준을 높이고, 혁신적인 보안 솔루션을 제공합니다.

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 2

팀원 구성 및 역할

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 2

팀원 구성 및 역할

PL

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

김선우

PM

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

우건희

PA

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

김효진

ⓒSaebyeol Yu. Saebyeol's PowerPoint

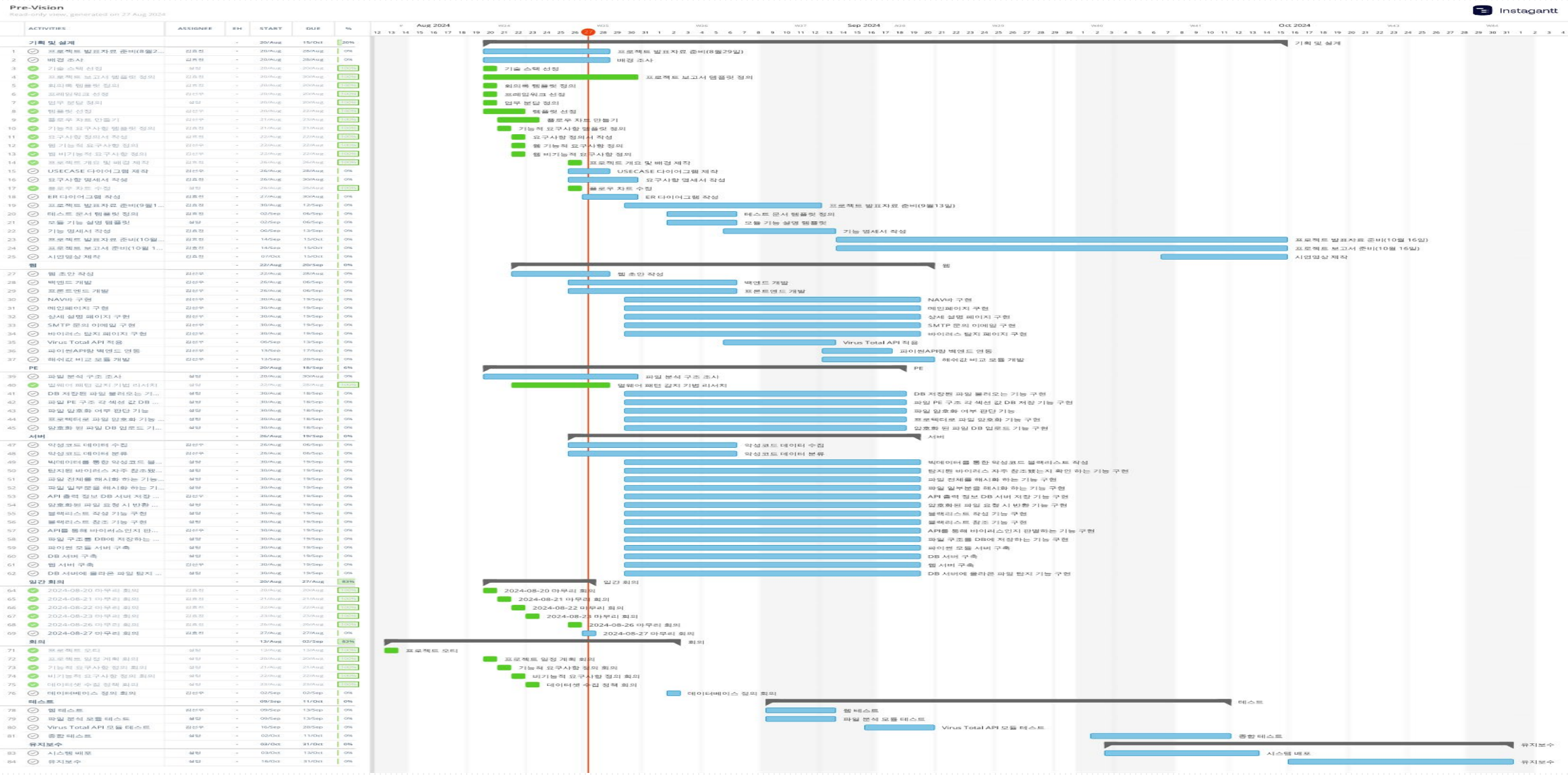
Part 3

프로젝트 일정

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 3

프로젝트 일정



ⓒSaebyeol Yu. Saebyeol's PowerPoint

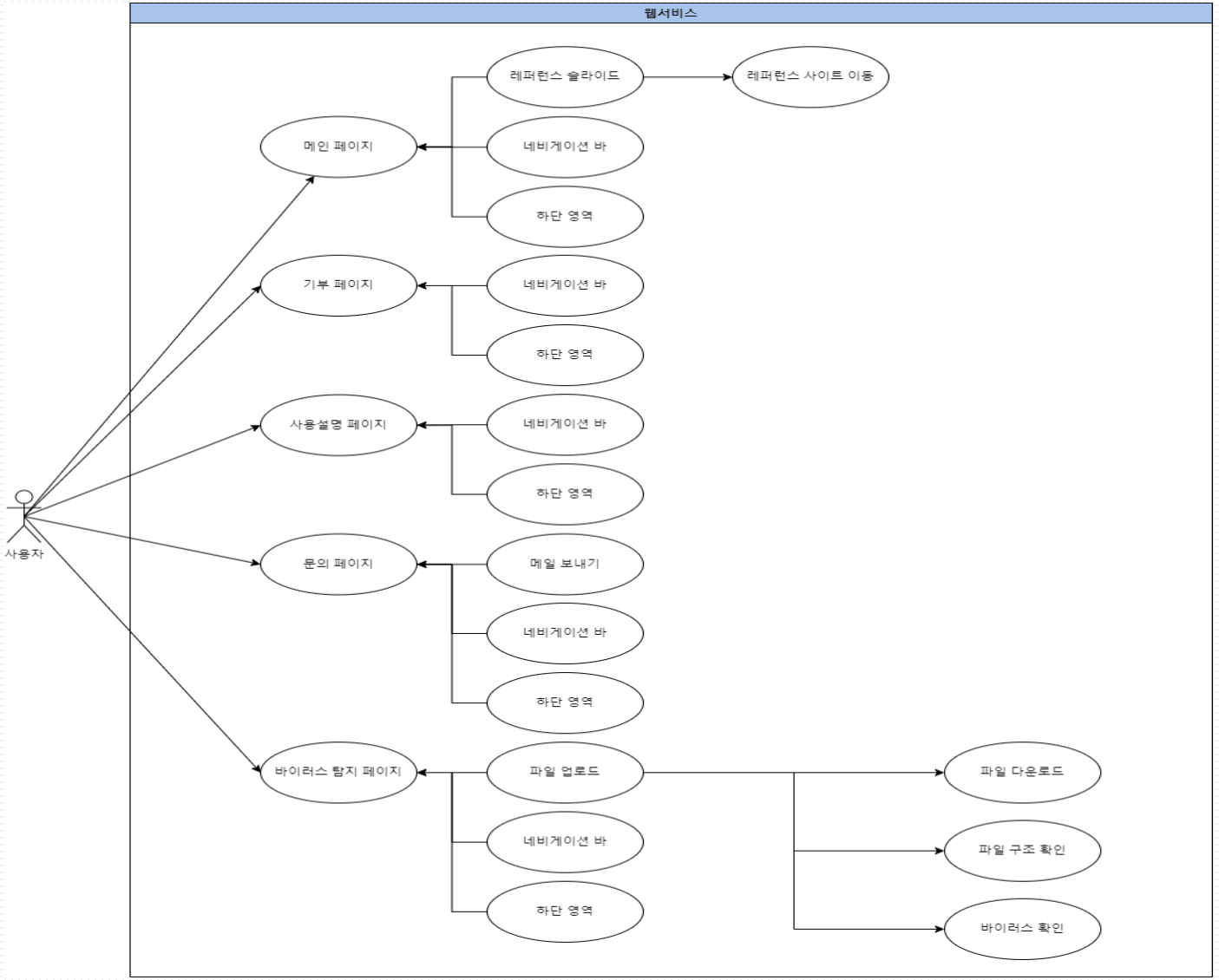
Part 4

요구사항

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 4

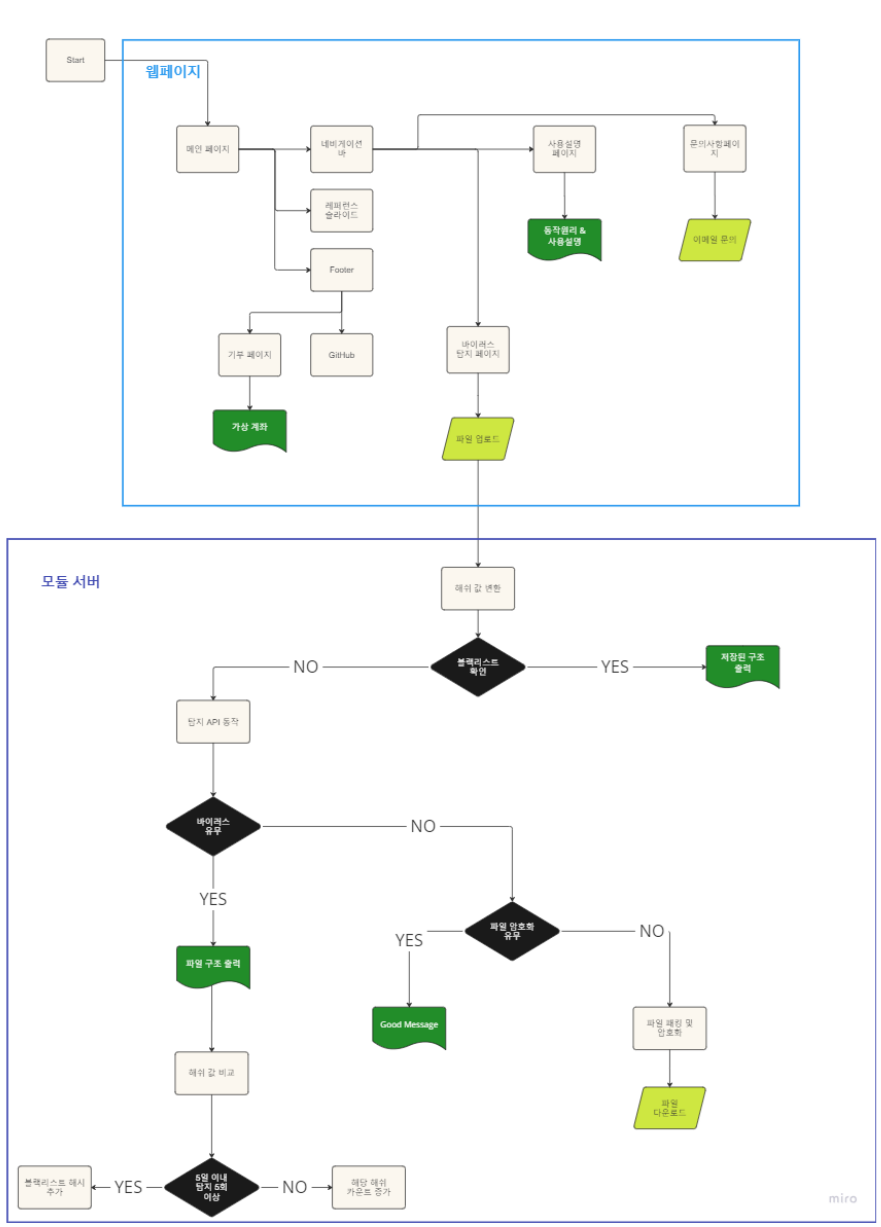
USE CASE



ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 4

시스템 흐름도



ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 4

요구사항 정의서

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	

ebyeol Yu. Saebyeol's PowerPoint

Part 4

요구사항 정의서

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				

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 4

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				

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 4

비기능 요구사항 정의서

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	

1

ⓒSaebyeol Yu. Saebyeol's PowerPoint

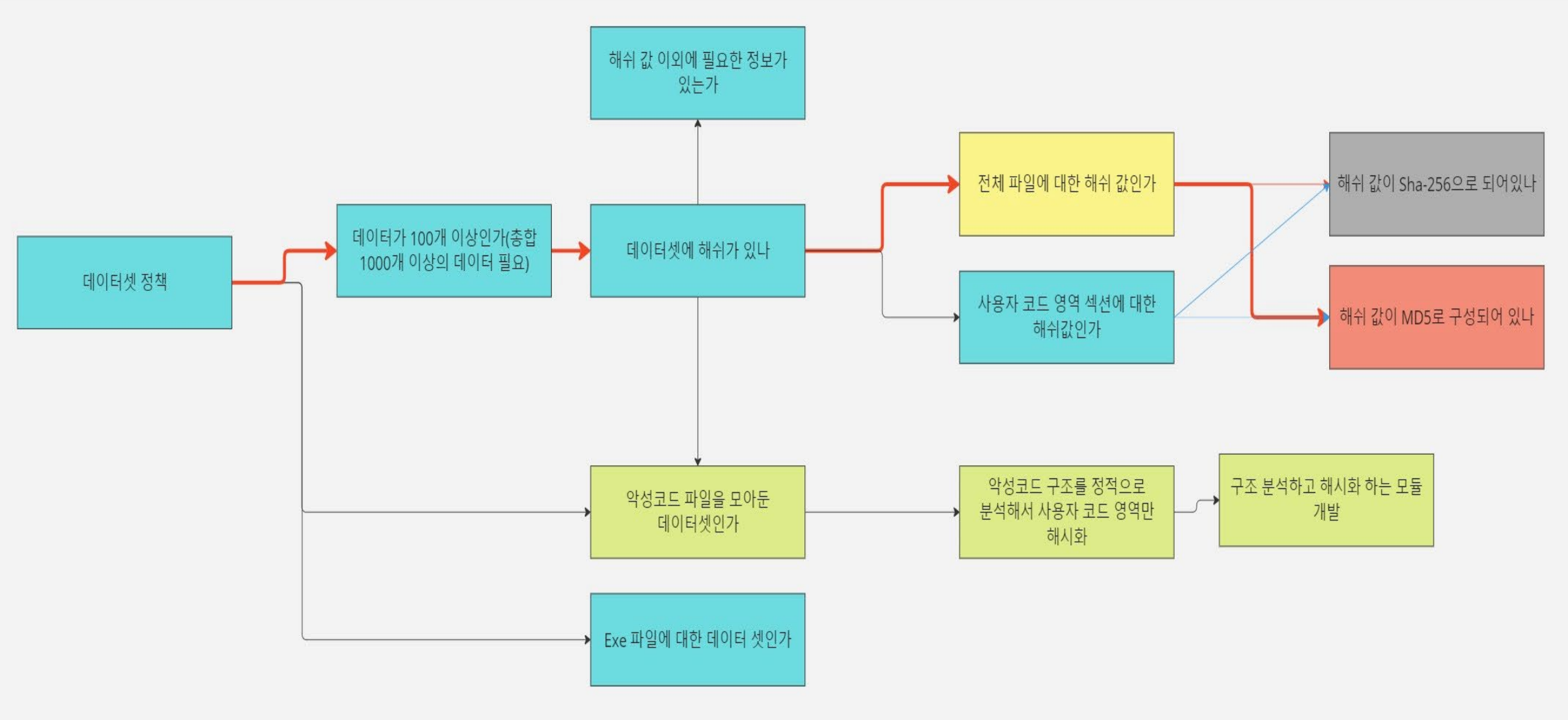
Part 5

데이터셋 수집 정책

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 5

데이터셋 수집 정책



ⓒSaebyeol Yu. Saebyeol's PowerPoint