

2026-1 정보보안SW융합전공

업데이트 기반 확장 프로그램 공급망 보안 시스템 설계

곽민경, 박혜수, 심재훈, 윤주혁, 정재성(PM)



Index

01

팀 소개

- 팀원 소개

02

프로젝트 개요

- 프로젝트 필요성
- 프로젝트 목표
- 프로젝트 정의

03

프로젝트 진행

- 프로젝트 기술스택
- 시스템 설계
- 요청 및 트리거
- 확장 프로그램 분석
- 관리자 대시보드

04

프로젝트 결론

- 시연 영상
- 기대 효과
- 최종 시스템 설계
- 추후 계획

01. 팀 소개

팀원 소개



곽민경

PA



박혜수

PA



심재훈

PA



윤주혁

PA



정재성

PM

02. 프로젝트 개요

프로젝트 필요성

보안뉴스

깃허브, “내부 저장소 3800개 공격 당해... VS코드 악성 확장 프로그램이 원인”

깃허브가 자사 내부 소프트웨어 저장소 3800개가 사이버 공격을 당했다고 인정했다. 깃허브는 '비주얼 스튜디오(VS) 코드' 마켓플레이스에서 악성 확장...

2주 전



보안뉴스

취약점 찾으려다 암호 다 털렸다... 'Trivy' 오염 사태 비상

보안 스캐너인 '트리비(Trivy)'의 공식 깃허브 액션이 통째로 해킹돼 악성 코드가 삽입되는 초유의 공급망 공격이 발생했다. 보안 취약점을 찾아내야...

2026. 3. 23.



한국정보기술진흥원

npm 패키지 공급망 대규모 공격...170개 이상 패키지 감염

npm 패키지 공급망 대규모 공격...170개 이상 패키지 감염 · TanStack 생태계 피해. TanStack 이코시스템이 가장 심하게 피해를 입었다. · 주요 표적 다수.

4주 전



공급망 공격의 확산

Package Artifact,
Extension Artifact 등을
대상으로 지속적인
공급망 공격이 발생

프로젝트 필요성

Extension
Artifact
보안 공백

1

정상과 악성의
부정확한 기준

2

운영 업체 심사의
한계점

3

사용자가 인지하기
어려운 자동 업데이트

02. 프로젝트 개요

프로젝트 필요성

1 정상과 악성의 부정확한 기준

악성 확장에서 사용하는 코드 기능들은 모두 정상에서도 동일하게 사용되기에 필터링 방식의 분석이 불가능

```
const data = "dark";

chrome.storage.local.set({
  pageData: data
});
```

정상 확장 프로그램이
사용자의 테마를 데이터로 저장하는 코드

```
const data = cookies;

chrome.storage.local.set({
  pageData: data
});
```

악성 확장 프로그램이
사용자의 쿠키를 데이터로 저장하는 코드

프로젝트 필요성

2 운영 업체 심사의 한계점

자동화 검사와 체크리스트 기반 점검으로 패턴 기반 탐지에는 효과적이지만, 코드의 전체 흐름을 악용하는 고도화된 공격까지 식별하기에는 한계점이 존재

Data collection

The content of this form will be displayed publicly on the item detail page. By publishing your item you are certifying that these disclosures accurately reflect the most up-to-date content of your privacy policy.

What personal and sensitive data do you plan to collect from users now or in the future?

- ☒ Personally identifying information
For example: name, address, email address, age, or identification number
- ☐ Health information
For example: heart rate data, medical history, symptoms, diagnoses, or procedures
- ☐ Financial and payment information
For example: transactions, credit card numbers, credit ratings, financial statements, or payment history
- ☒ Authentication information
For example: passwords, credentials, security question, or personal identification number (PIN)
- ☐ Personal communications

프로젝트 필요성

3

사용자가 인지하기 어려운 자동 업데이트

사용자가 인지하기 어려운 자동 업데이트 과정에서 악성 코드가 포함될 경우, 별도의 동의 없이 배포되어 피해 사실을 즉시 확인하기 어려움

Chrome 확장 프로그램 업데이트 수명 주기

표준 업데이트 주기

Chrome은 설치된 확장 프로그램을 최신 버전으로 자동 업데이트하여 사용자가 새로운 기능과 보안 수정사항을 이용할 수 있도록 설계되었습니다. 기본적으로 Chrome은 시작 시와 몇 시간마다 확장 프로그램 업데이트를 확인합니다.

프로젝트 목표

3가지
보안 공백을
해결하기 위한
방법 모색

1

정상과 악성의
부정확한 기준

2

플랫폼 심사의
한계점

3

사용자가 인지하기
어려운 자동 업데이트

프로젝트 정의

Extension Artifact 보안

“ 업데이트 기반 확장 프로그램
공급망 보안 시스템 설계 ”

03. 프로젝트 진행

프로젝트 기술스택

프로젝트
관리 및 협업



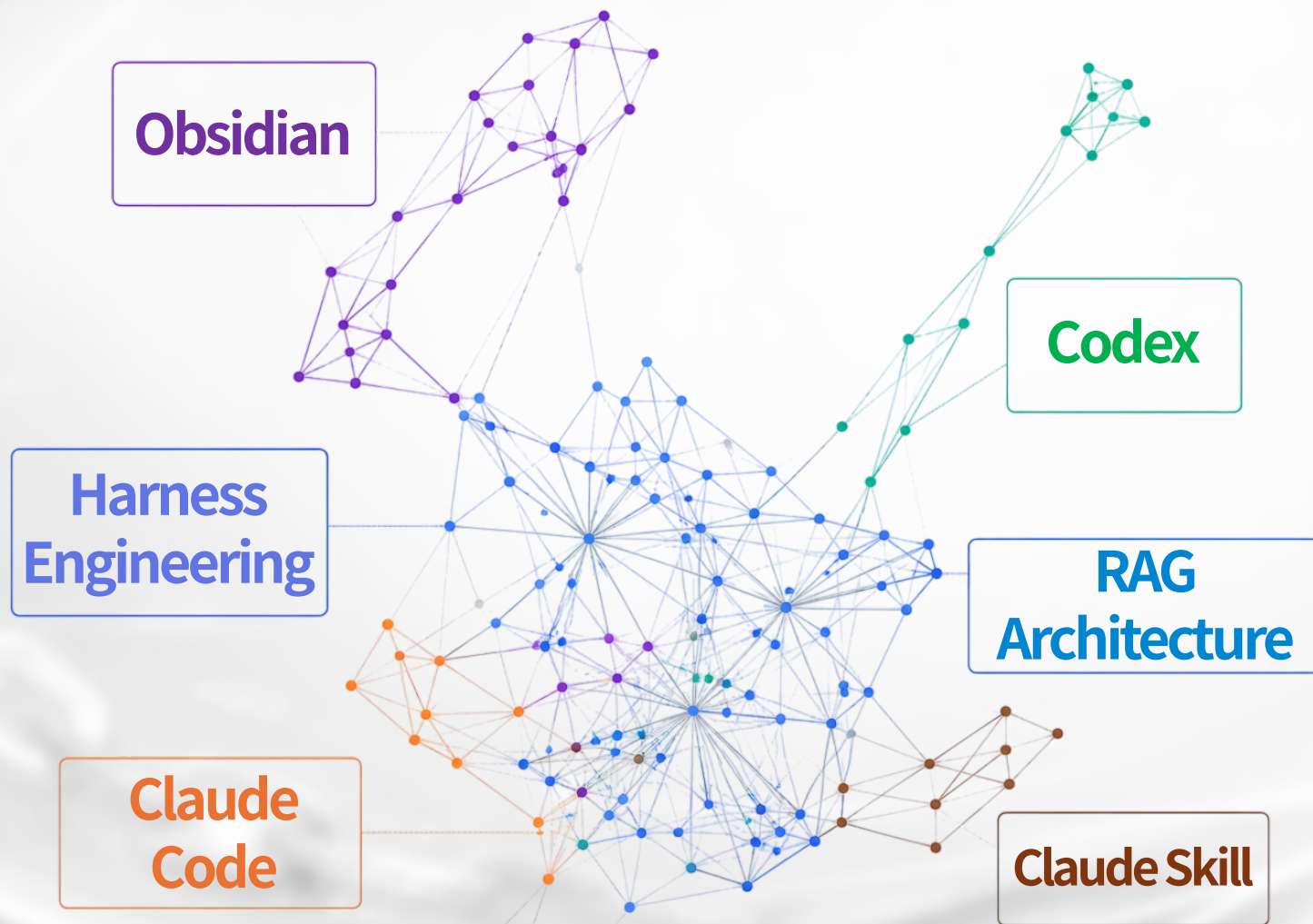
프로젝트
운영



개발 및
분석 엔진

03. 프로젝트 진행

프로젝트 기술스택



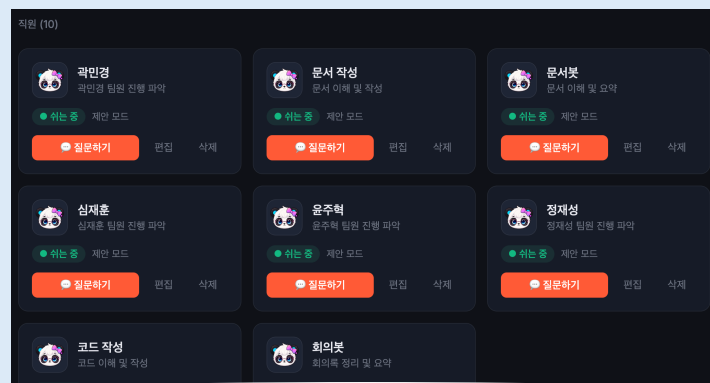
프로젝트 목표를
달성하기 위해
다양한 **AI 기술 학습**

03. 프로젝트 진행

프로젝트 기술스택

학습한 **AI 기술**을 바탕으로

AI 직원 관리



팀/직원 규칙



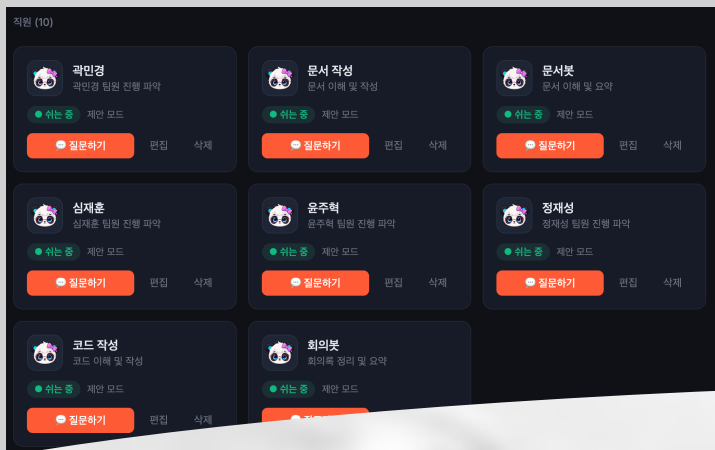
통합 플랫폼을 개발하여 협업에 활용

03. 프로젝트 진행

프로젝트 기술스택

학습한 **AI 기술**을 바탕으로

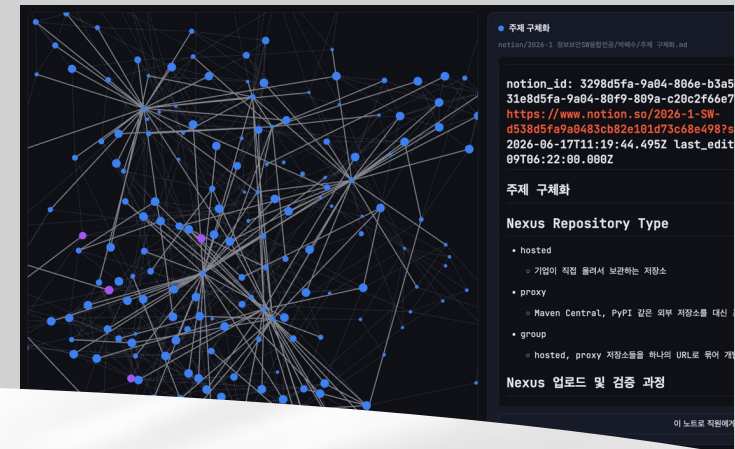
AI 직원 관리



팀/직원 규칙



지식 그래프 참조



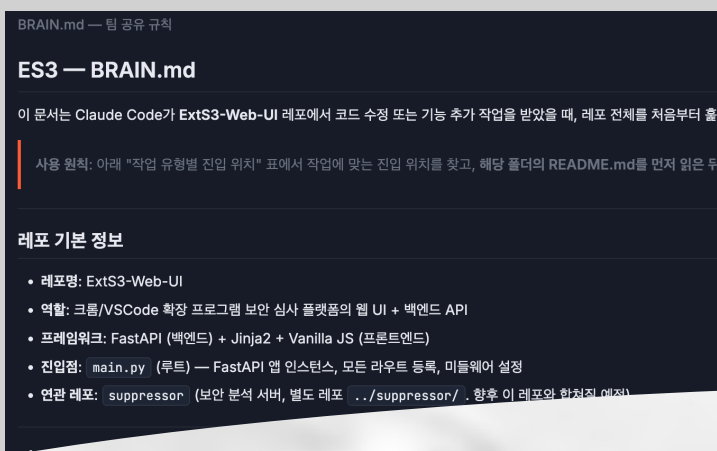
통합 플랫폼을 개발하여 협업에 활용

03. 프로젝트 진행

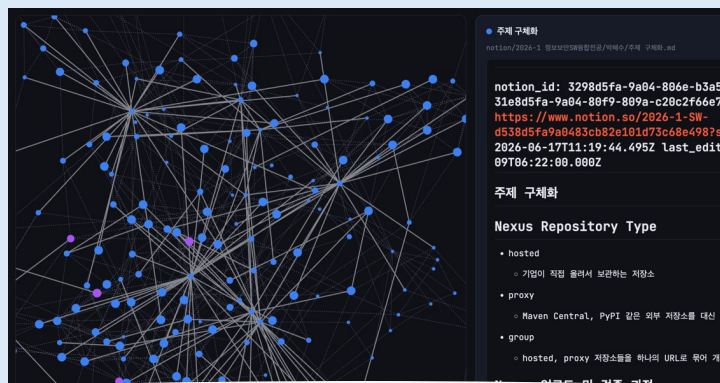
프로젝트 기술스택

학습한 **AI 기술**을 바탕으로

팀/직원 규칙



지식 그래프 참조



통합 플랫폼을 개발하여 협업에 활용

03. 프로젝트 진행

시스템 설계

기존 npm, maven 등을 보안하기 위해
기업에서 사용 중인 **Repository Manager**

외부 서버에서 보안 검사를 마친 후
내부 개발자가 이용할 수 있도록 저장해두는 저장소

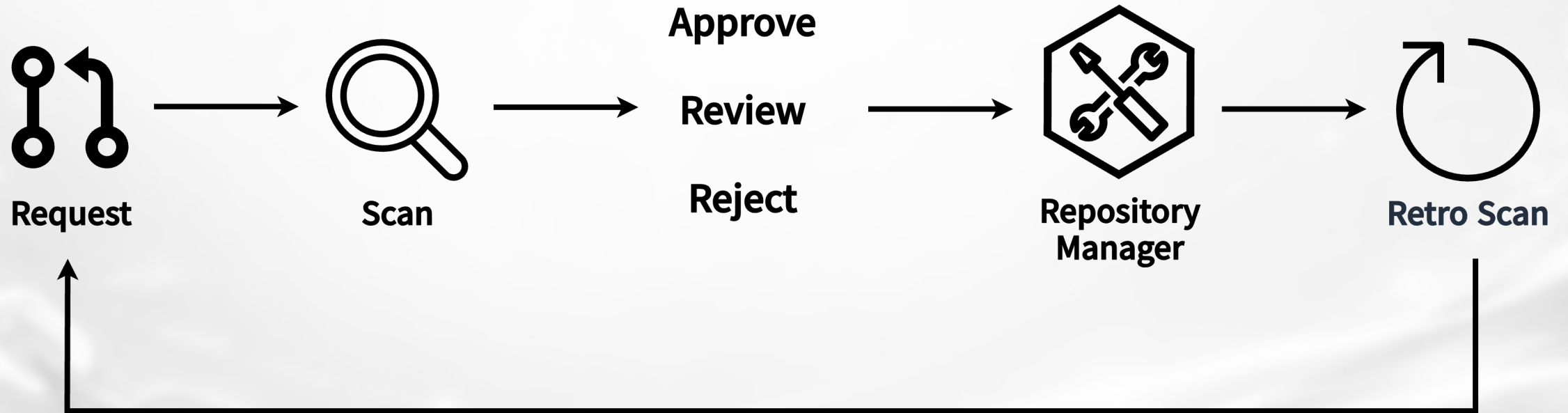
확장 프로그램도 저장 가능하기에
통합이 용이한 구조를 설계하고자 활용



**Repository
Manager**

03. 프로젝트 진행

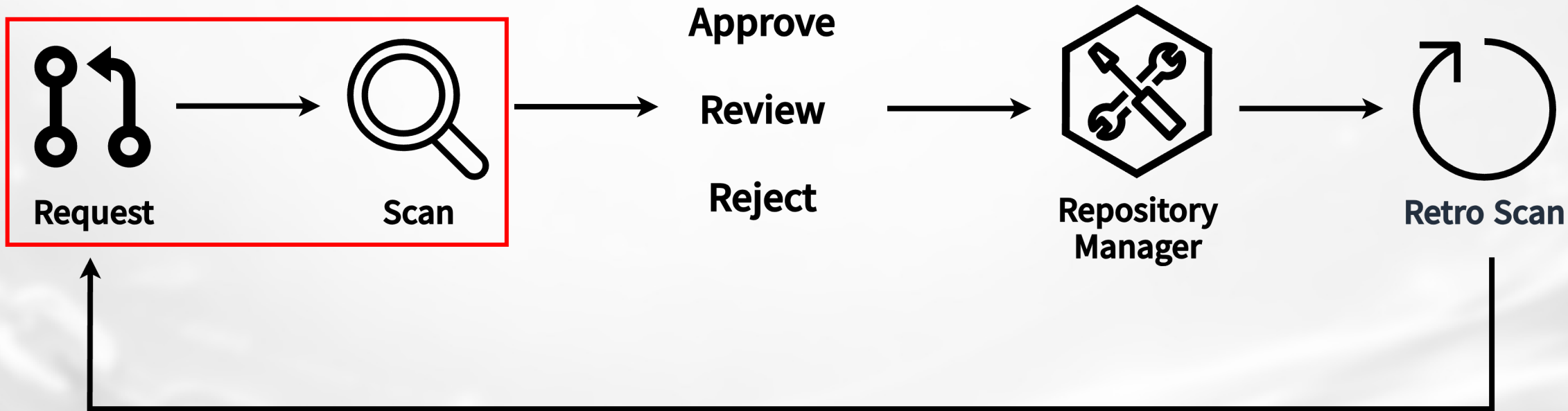
시스템 설계



03. 프로젝트 진행

요청 및 트리거

저장소에 존재하지 않은 확장 프로그램을 사용하고 싶은 경우 분석 요청을 전송



03. 프로젝트 진행

요청 및 트리거

프로그램 검색



ID로 검색



이름으로 검색



번역기

검색



Google Chrome



Mozilla Firefox



Microsoft Edge



VS Code



Safari

확장 ID 또는
이름을 통한 검색

Marketplace
카테고리 선택

03. 프로젝트 진행

요청 및 트리거

앱 탐색 > 검색 결과

'번역기' 검색 결과 28건

검색 결과

정렬: 추천순 | 사용자순 | 별점순 | 최신순



CHROME
추천 162

Google Translate

View translations easily as you browse the web. By the Googl...

★ 4.2 33M users

업데이트 September 6, 2024

View Detail



CHROME
추천 184

DeepL: translate and write with AI

Translate while you read and write with DeepL Translate, th...

★ 4.7 4M users

업데이트 June 16, 2026

View Detail



CHROME
추천 170

Immersive Translate: AI Web, PDF & Video Translator

Free Translate Website, Translate PDF & Epub eBook,...

★ 4.0 3M users

업데이트 June 11, 2026

View Detail



CHROME
추천 177

ImTranslator: Translator, Dictionary, TTS

Translator, Dictionary, Voice ImTranslator translates selecte...

★ 4.4 900K users

업데이트 June 1, 2026

View Detail



CHROME
추천 175



CHROME
추천 165



CHROME
추천 154



CHROME
추천 174

크롤링을 통해 가져온
확장 프로그램들을
조회 가능

03. 프로젝트 진행

요청 및 트리거



EDITOR'S CHOICE

Google Translate

요청하기

즉시 검사

사용하고자 하는 확장
분석 요청 가능

앱 설명

View translations easily as you browse the web. By the Google Translate team. Highlight or right-click on a section of text and click on Translate icon next to it to translate it to your language. Learn more about Google Translate at <https://support.google.com/translate>. By installing this extension, you agree to the Google Terms of Service and Privacy Policy at <https://www.google.com/intl/en/policies>. UPDATE (v.2.0): Now you can highlight or right-click a text and translate it vs. translate the entire page. You can also

상세 정보

버전 2.0.16

최근 업데이트 September 6, 2024

03. 프로젝트 진행

요청 및 트리거



EDITOR'S CHOICE

Google Translate

요청하기즉시 검사

2가지 종류의 요청이 존재

앱 설명

View translations easily as you browse the web. By the Google Translate team. Highlight or right-click on a section of text and click on Translate icon next to it to translate it to your language. Learn more about Google Translate at <https://support.google.com/translate>. By installing this extension, you agree to the Google Terms of Service and Privacy Policy at <https://www.google.com/intl/en/policies>. UPDATE (v.2.0): Now you can highlight or right-click a text and translate it vs. translate the entire page. You can also

상세 정보

버전	2.0.16
최근 업데이트	September 6, 2024

03. 프로젝트 진행

요청 및 트리거

요청하기

즉시 검사

신규 확장 프로그램의 평판이 쌓이는 시간을 기다리는 **Holding**



신규 확장 프로그램

Chrome에 추가

공유

테마 23 사용자

5점 만점에 0점 ☆☆☆☆☆

평점 없음 · [검색결과 및 리뷰에 관해 자세히 알아보기](#)

필터링 기준
모든 리뷰

정렬 기준
날짜순

언어
한국어



현재 이 항목에 대한 리뷰가 없습니다.

03. 프로젝트 진행

요청 및 트리거

요청하기

즉시 검사

급하게 확장 프로그램을 사용해야 하는 경우 **즉시 검사**



신규 확장 프로그램

0.0 ★ ⓘ

This extension is officially certified by Google...



즉시 검사 권한이
존재하는 사용자

지금 이 확장 프로그램을
바로 사용해야 하는 상황이에요!

03. 프로젝트 진행

요청 및 트리거

내 파일 업로드 |

N/A

파일 선택

설정

프로그램 업로드 전, 검사를 위한 설정을 입력하세요.

취소

검사 실행



확장 프로그램 정보 (Extension Info)

업로드 유형

첫 업로드

추가 업로드

새로운 확장을 처음 업로드합니다. 버전은 자동으로 1.0.0으로 설정됩니다.

확장 프로그램 이름

예: My Extension

버전 (자동)

1.0.0

브라우저

Google Chrome

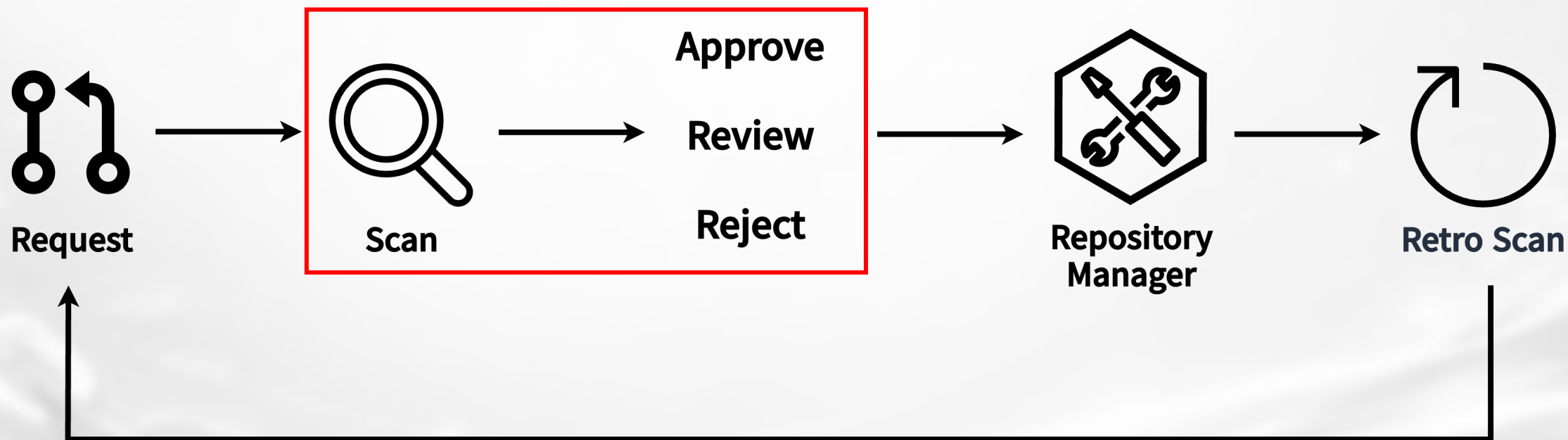


업로드 권한이 있는 사용자가
직접 개발한 확장 프로그램을 업로드 시
분석 요청이 발생

03. 프로젝트 진행

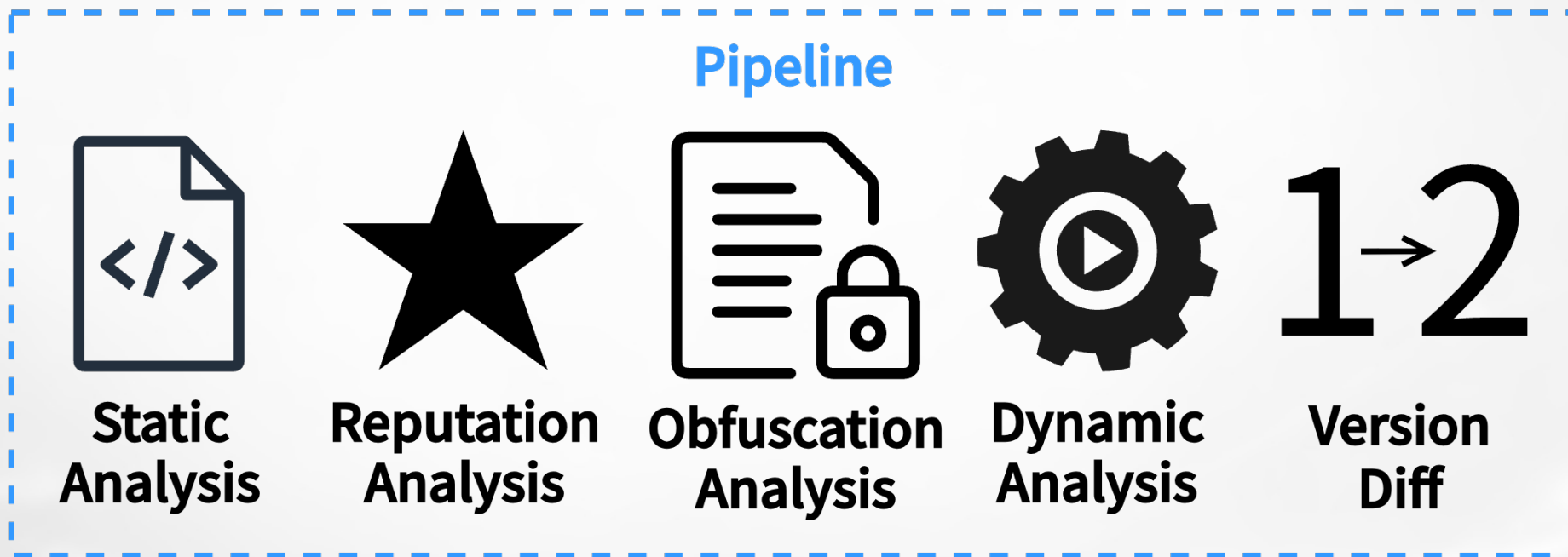
확장 프로그램 분석

요청이 발생하면 대상 확장 프로그램 검사 후 결과 반환



03. 프로젝트 진행

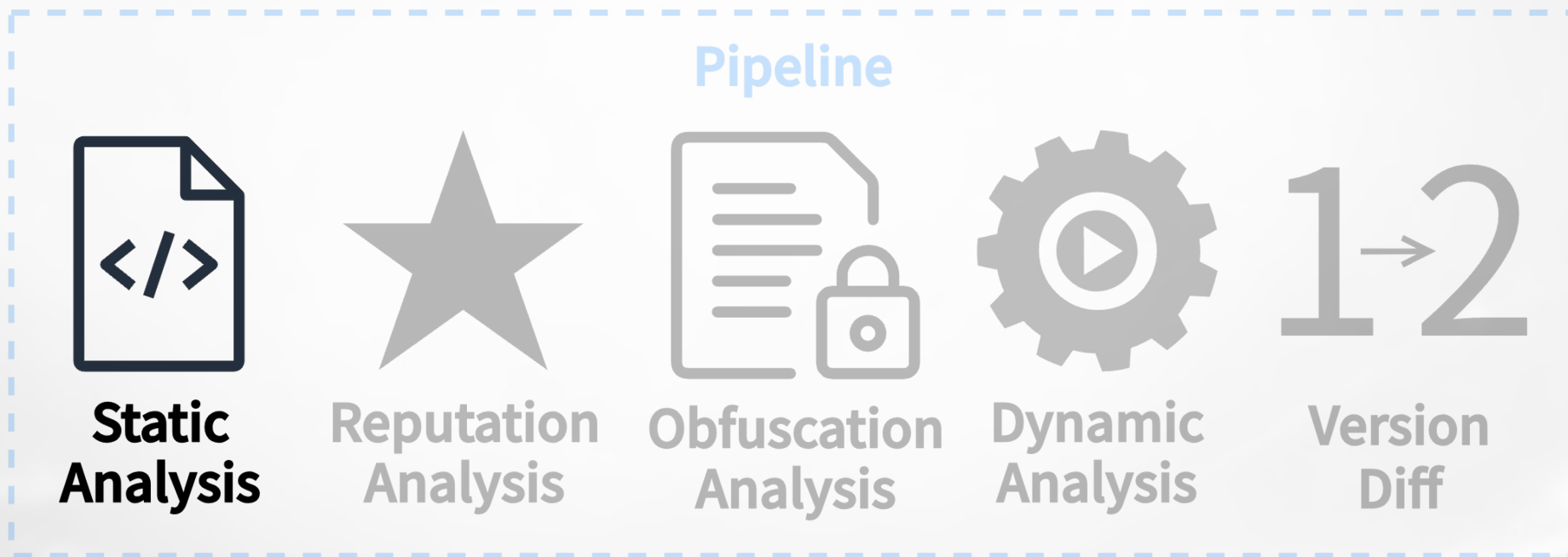
확장 프로그램 분석



4가지의 필수 검사와 1가지 조건부 검사를 진행

03. 프로젝트 진행

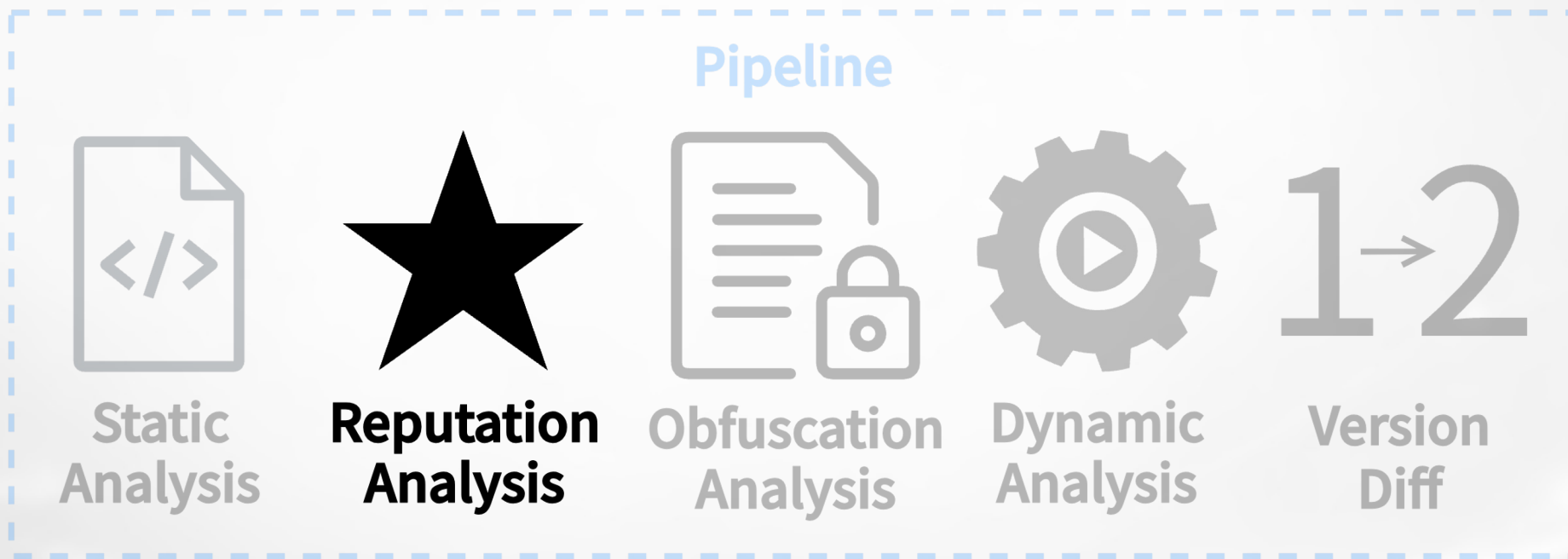
확장 프로그램 분석



확장 프로그램의 권한, 코드 구조를 기반으로
추후 보안 담당자의 분석 편의성을 높이기 위한 **정적 분석**

03. 프로젝트 진행

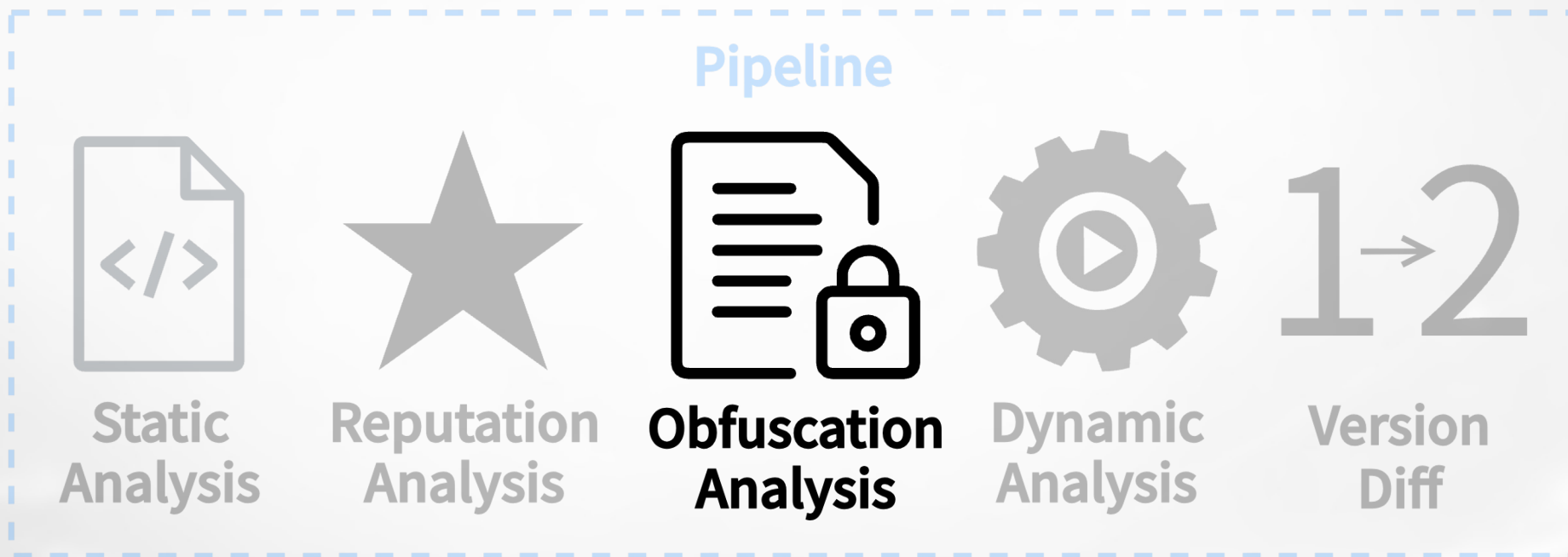
확장 프로그램 분석



확장이 통신하는 외부 도메인/IP를 대상으로
평판 데이터와 대조해 점수를 부여하는 **평판 기반 분석**

03. 프로젝트 진행

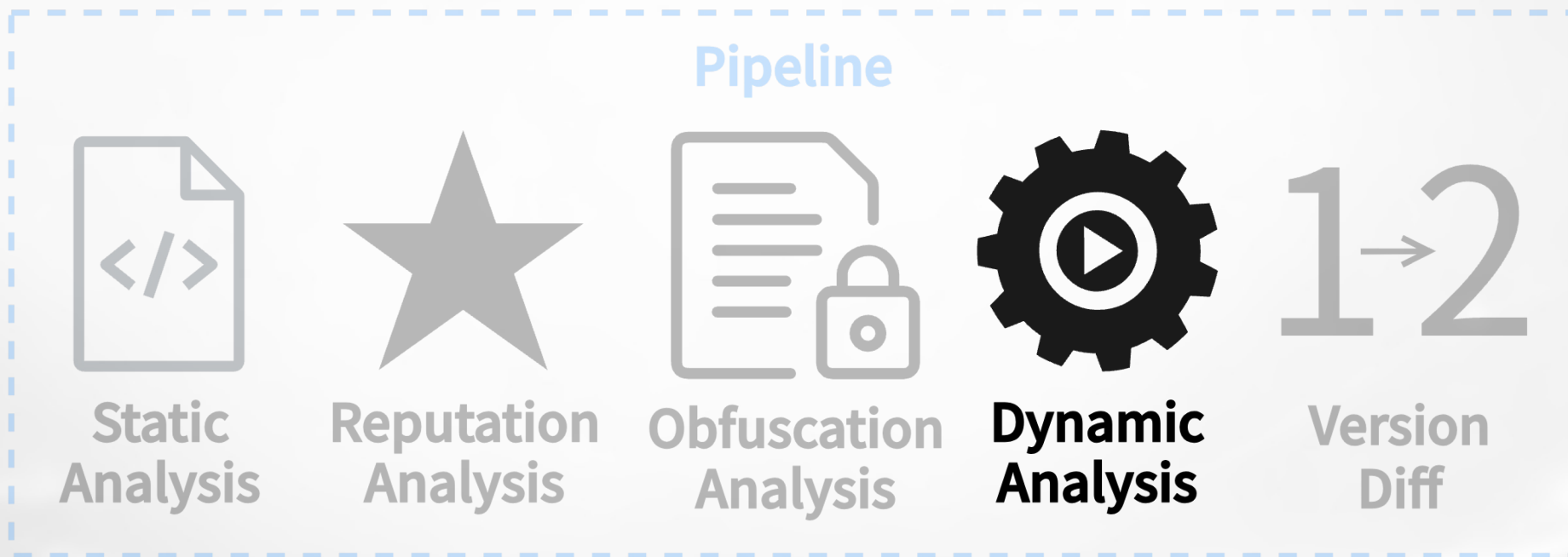
확장 프로그램 분석



정적 분석을 방해하는 난독화 요소를 라이브러리,
디코더 등의 패턴 기반으로 탐지하는 **난독화 분석**

03. 프로젝트 진행

확장 프로그램 분석



권한 및 코드 조합을 바탕으로 시나리오를 선정하고,
LLM이 시나리오를 수행하는 RAG 아키텍처 기반의 **동적 분석**

03. 프로젝트 진행

확장 프로그램 분석 - 동적 분석

시나리오 ID 관리

vectorDB에 적재되는 탐지 시나리오를 관리합니다.

등록된 시나리오

총 26개

기본적으로 26개의 시나리오를 제공하며,
커스텀 시나리오 등록 가능

시나리오들은
고유 ID를 통해 관리

등록된 시나리오

총 26개

jopbobkiihaohndkafaboogaokbekhao
browser_automation_remote_control

기본

확장 프로그램 분석 - 동적 분석

1. Fingerprint 추출

분석 대상 확장 프로그램이 갖고 있는 권한 조합, 함수를 추출

```
{  
  "권한": a+b, c+b  
  "코드": 1, 4, 9  
}
```

03. 프로젝트 진행

확장 프로그램 분석 - 동적 분석

2. Vector DB에 저장된 시나리오와 비교

추출된 Fingerprint의 구조와 저장된 시나리오의 Fingerprint 구조를 비교

```
{  
  "권한": a+b, c+b  
  "코드": 1, 4, 9  
}
```

```
{  
  "권한": c+b  
  "코드": 4  
}
```

Vector DB :
이 시나리오 구조가 일치하네!!

확장 프로그램 분석 - 동적 분석

3. 반환된 시나리오가 가리키는 문서를 LLM에게 전달

특정 권한과 함수가 존재할 때 어떤 시나리오를 어떤 동작에 의해 발생시킬 수 있는지 정의된 Markdown 문서 반환

입력값 탈취

c+b 권한 조합에 4라는 코드 함수가 있는 경우 입력값 탈취가 발생할 수 있습니다.

1. 테스트용 웹페이지에 접근
2. 입력창에 정보 입력

확장 프로그램의 동작을 관찰하여 트리거된 악성 증거를 반환하세요.

03. 프로젝트 진행

확장 프로그램 분석 - 동적 분석

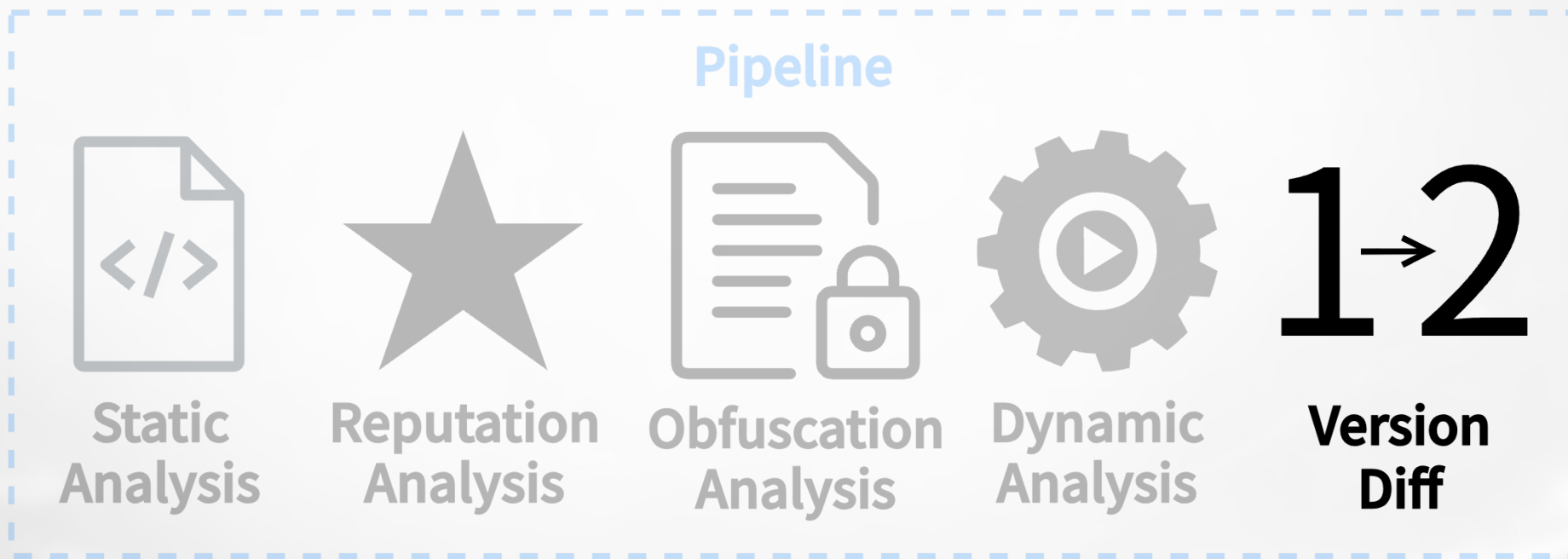
4. LLM이 실제 시나리오를 실행시켜 수집한 증거를 기반으로 위험도 반환

동적 분석	
위험도	CRITICAL
실제 관측된 네트워크 요청	18건
실제 관측된 스토리지 접근	135건
실제 관측된 메시지 이벤트	135건

CRITICAL

03. 프로젝트 진행

확장 프로그램 분석



만약 이미 존재하는 확장 프로그램이 업데이트되어 새로운 분석을
진행하는 경우 편리한 분석을 위해 제공되는 **버전 변경사항**

03. 프로젝트 진행

확장 프로그램 분석 - 버전 변경사항

조건부 분석 : 업데이트 기반 재분석 시 진행

버전 변경 사항

[자세한 변경 내용 보러가기](#)

v1.0.1 → v1.0.2 버전 간 변경 요약입니다.

매니페스트 변경 (manifest.json)

3 건

권한 추가: 0

권한 제거: 0

호스트 권한 추가: 1

호스트 권한 제거: 2

선택 권한 추가: 0

선택 권한 제거: 0

기타 필드 변경: 0

코드 변경 (manifest.json 외)

0 개 파일

파일 추가: 0

파일 제거: 0

파일 수정: 0

manifest.json 외 코드 변경 없음

03. 프로젝트 진행

확장 프로그램 분석 - 버전 변경사항

관리자의 수동 검토 과정의 분석 용이성 제공

v1.0.1 → v1.0.2 버전 간 전체 변경 내역입니다.

매니페스트 변경 3

코드 변경 파일 0

📄 매니페스트 변경 (manifest.json)

호스트 권한 (host_permissions)

+ <all_urls>

- http://*/*

- https://*/*

manifest.json 원본 diff

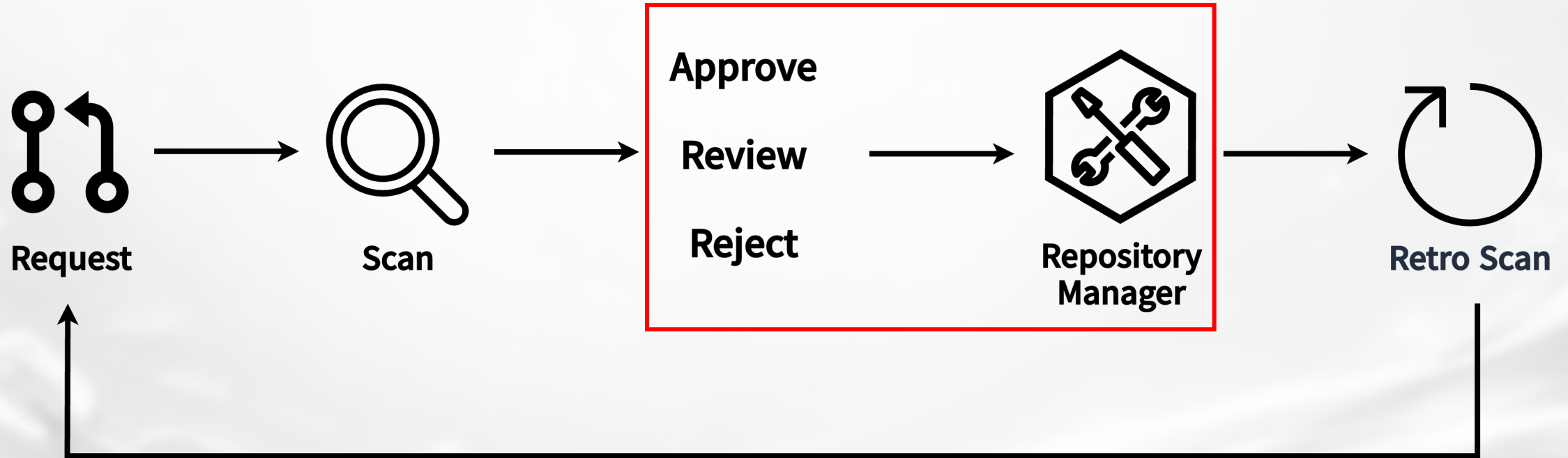
수정됨

```
@@ -23,8 +23,7 @@
23 23    ],
24 24
25 25    "host_permissions": [
26 -    "https://*/*",
27 -    "http://*/*"
26 +    "<all_urls>"
28 27    ],
29 28
30 29    "web_accessible_resources": [
```

03. 프로젝트 진행

확장 프로그램 분석

검사 결과에 따라 Repository Manager에 저장 / 담당자의 검토 / 자동 거부 가 결정



03. 프로젝트 진행

확장 프로그램 분석

Repository Manager에 저장 / 담당자의 검토 / 자동 거부

AI Final Decision Policy

정책 설정

심각도 결과에 따라 자동 승인 또는 자동 거부 여부만 설정합니다.

관리자 대시보드에서
분석 결과에 따라 확장 프로그램을
어떻게 처리할지 설정 가능

⚙ 기본 정책

Critical 자동 거부

critical 심각도가 포함된 분석 결과를 자동으로 거부합니다.



Low 자동 승인

low 심각도만 확인된 분석 결과를 자동으로 승인합니다.



자동 정책에 해당하지 않는 결과는 기존처럼 관리자 검토 상태로 유지됩니다.

03. 프로젝트 진행

확장 프로그램 분석

담당자의 검토 대상으로 처리된 확장 프로그램은 관리자 대시보드에서 수동 검토 가능

관리자 대시보드

시스템 상태 및 리포지토리 활동을 실시간으로 모니터링합니다.

User Access

정책 설정

Report Download

Refresh Data

승인 대기중인 앱

Nexus review 폴더에 있는 검토 대상만 표시합니다.

APP NAME	BROWSER	VERSION	ACTIONS
2026-06-20			
Google Translate 오후 04:07	Chrome	2.0.16	승인 거부
2026-06-12			
Mouse Tooltip Translator - PDF & Netflix Youtube dual subs 오전 01:42	Chrome	0.1.230	승인 거부
원격 권한 제어 오후 04:31	Chrome	1.0.2	승인 거부
원격 권한 제어 오후 04:18	Chrome	1.0.1	승인 거부

거부 프로그램 목록



DeepL: translate and write with AI

Chrome · 1.87.0 · 2026. 6. 9. 오후 7:34:39

애플리케이션 > 승인 대기

승인 대기 앱 상세 분석

원격 권한 제어 PENDING

× 반려

✓ 최종 승인

앱 기본 정보



Title
원격 권한 제어

신청 일시

2026-06-12T16:31:58+09:00

카테고리

Chrome Extension

브라우저

Chrome

버전

1.0.2

확장 ID

원격 권한 제어

보안 및 정적 분석 리포트

2 critical

5 high

11 medium

3 low

분석 요약

Risk signals or analysis uncertainty require human review before approval.

PDF 내 보내기

JSON 다 운로드

판정

검토 필요

위험도

CRITICAL

점수

0.93 / 1.0

권장 조치

승인 전 사람이 검토

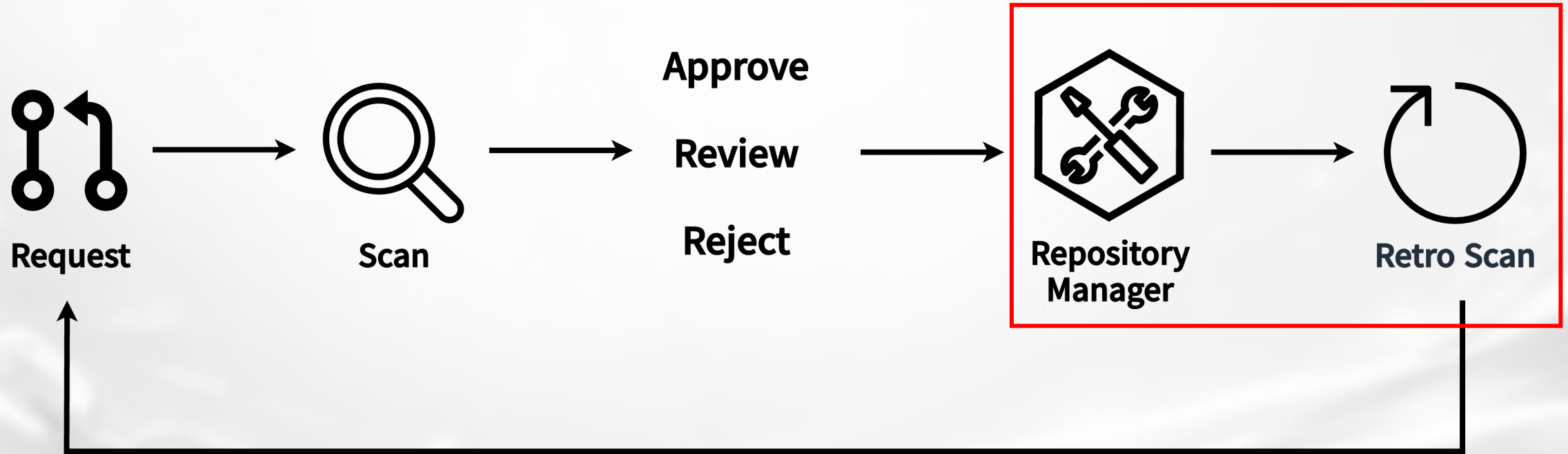
! 주요 위험 근거

확장 프로그램 코드에서 외부 통신 또는 URL 이동과 관련된 정적 신호가 발견되었습니다.

03. 프로젝트 진행

확장 프로그램 분석

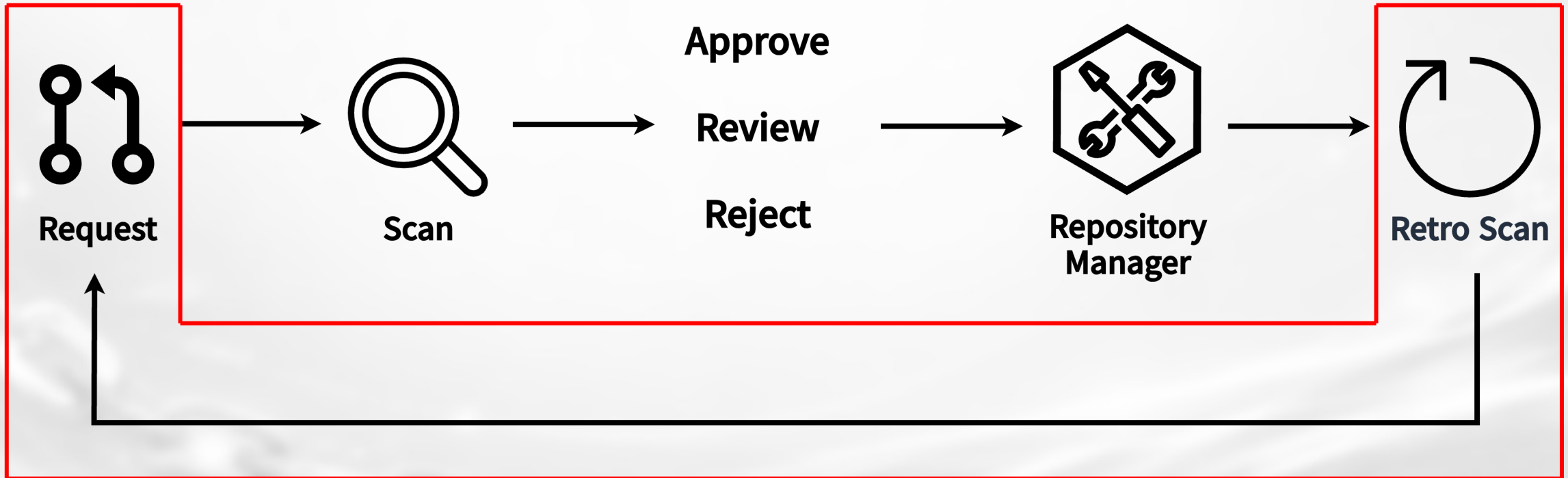
저장된 확장 프로그램이 업데이트되거나 평판에 문제가 발생했는지 주기적으로 점검



03. 프로젝트 진행

확장 프로그램 분석

Retro Scan에서 재검사가 필요하다 판단된 확장 프로그램은 다시 분석 요청 전송



03. 프로젝트 진행

관리자 대시보드

관리자 대시보드를 통해 사용자 권한 및 정책 설정 가능

User Access

Approve signup requests and toggle user permissions.

Signup Requests

No pending signup requests.

Users

test

Roles: user

Roles & permissions

admin

Roles: admin

Roles & permissions

Chrome Enterprise Policy Catalog

Chrome 정책 카탈로그

5종 표준 Chrome 관리 정책을 입력 → 미리보기 → .bat 다운로드. 사용자 PC에서 관리자 권한으로 실행하면 레지스트리에 정책이 등록됩니다.

정책 타입

선택

강제 설치 (Forcelist)

지정 확장을 자동 설치하고 사용자가 제거할 수 없게 한다.

레지스트리 경로

모든 정책이 등록되는 루트:

HKLM\Software\Policies\Google\Chrome

이 정책은 ExtensionInstallForcelist 키로 등록됩니다.

<> 입력 JSON

정책 타입을 바꾸면 예시 JSON으로 자동 채워집니다. 자유롭게 수정하세요.

```
{
  "entries": [
    {
      "extension_id": "aaaaaaaaaaaaaaaaaaaaaaaaaaaaa"
    }
  ]
}
```

실행 주의

- 다운로드한 .bat는 Windows에서 관리자 권한이 필요합니다.
- 실행 시 사용자 PC의 Chrome 정책이 즉시 변경됩니다
— 테스트 머신에서만 실행.
- 적용 후 Chrome 재시작 필요.

04. 프로젝트 결론

시연 영상

Nexus Repository - 대시보드

http://localhost:8000

Gemini에게 물어보기

Administrator

검색어를 입력하세요...

Suppressor Enterprise Edition

대시보드

홈

앱 탐색

라이브러리

시나리오 관리

관리자 대시보드

대시보드

저장소의 상태를 한눈에 파악하고 확장 프로그램의 라이프사이클을 관리하세요. 시스템이 최적의 상태로 작동 중입니다.

STORAGE OVERVIEW

전체 저장소 사용량

242 MB / 931 GB

0% 사용 중

남은 용량: 931 GB

사용 가능한 확장 프로그램 수

0

검증 완료 항목

0

현재 저장소 목록

전체 보기

안전 검사가 완료된 항목이 없습니다.

Upload

Help

Logout

업로드 페이지로 이동하여
확장 프로그램 업로드

Nexus Repository - 대시보드

Gemini에게 물어보기

http://localhost:8000

ES3

대시보드

앱 탐색

라이브러리

시나리오 관리

Administrator

검색어를 입력하세요...

Suppressor

Enterprise Edition

홈

앱 탐색

라이브러리

시나리오 관리

관리자 대시보드

대시보드

저장소의 상태를 한눈에 파악하고 확장 프로그램의 라이프사이클을 관리하세요. 시스템이 최적의 상태로 작동 중입니다.

STORAGE OVERVIEW

전체 저장소 사용량

242 MB / 931 GB

0% 사용 중

남은 용량: 931 GB

사용 가능한 확장 프로그램 수

0

검증 완료 항목

0

현재 저장소 목록

안전 검사가 완료된 항목이 없습니다.

전체 보기

Upload

Help

Logout

업로드 페이지로 이동하여
확장 프로그램 업로드

47/55

기대 효과

3가지
보안 공백을
해결

1

정상과 악성의
부정확한 기준

2

플랫폼 심사의
한계점

3

사용자가 인지하기
어려운 자동 업데이트

기대 효과

3가지 보안 공백을 해결

1

정상과 악성의
부정확한 기준

코드 흐름을
기반으로 분석

2

플랫폼 심사의
한계점

정적, 동적, 난독화 등
다양한 관점으로 분석

3

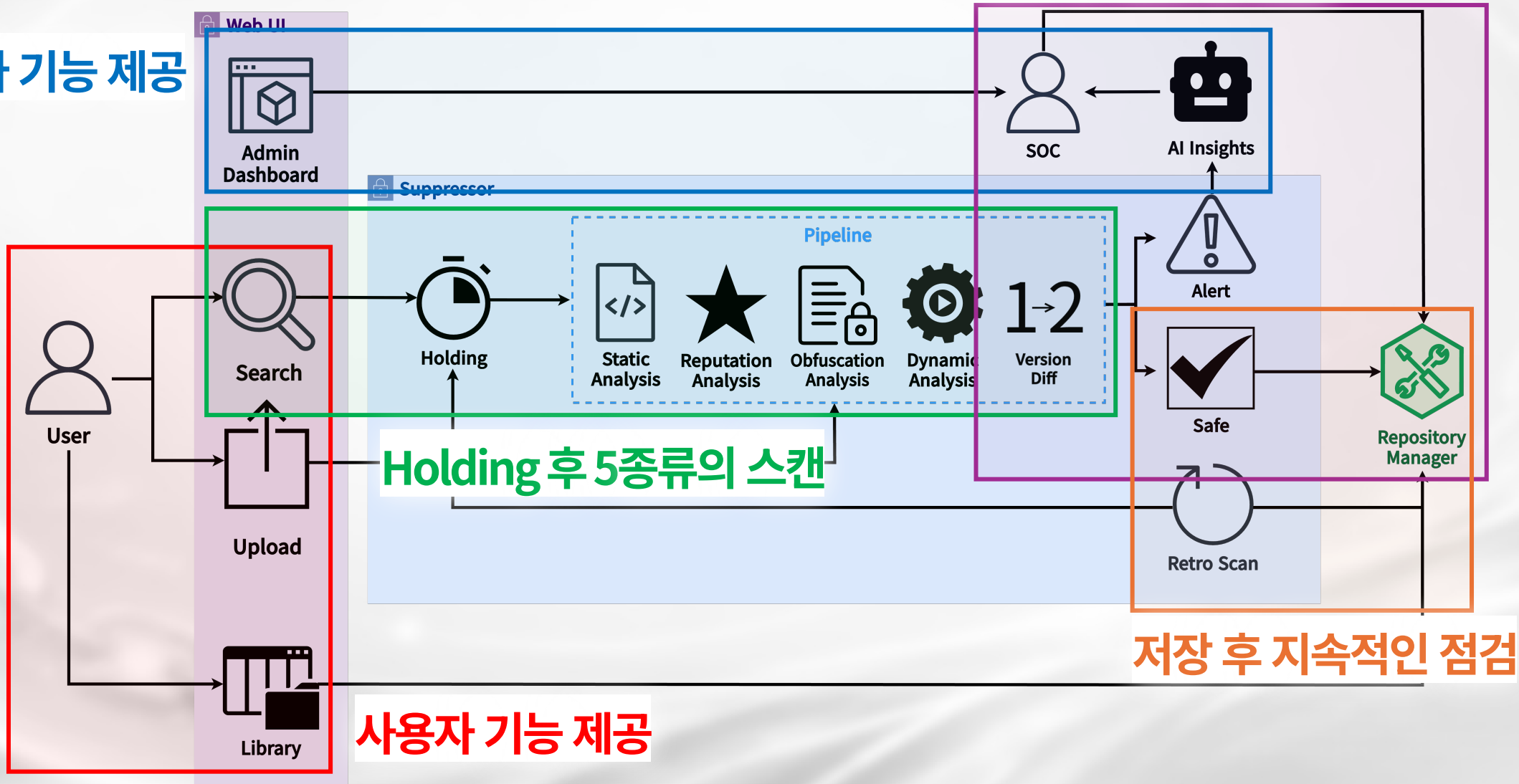
사용자가 인지하기
어려운 자동 업데이트

점검 없이
업데이트 불가능

04. 프로젝트 결론

최종 시스템 구조

관리자 기능 제공



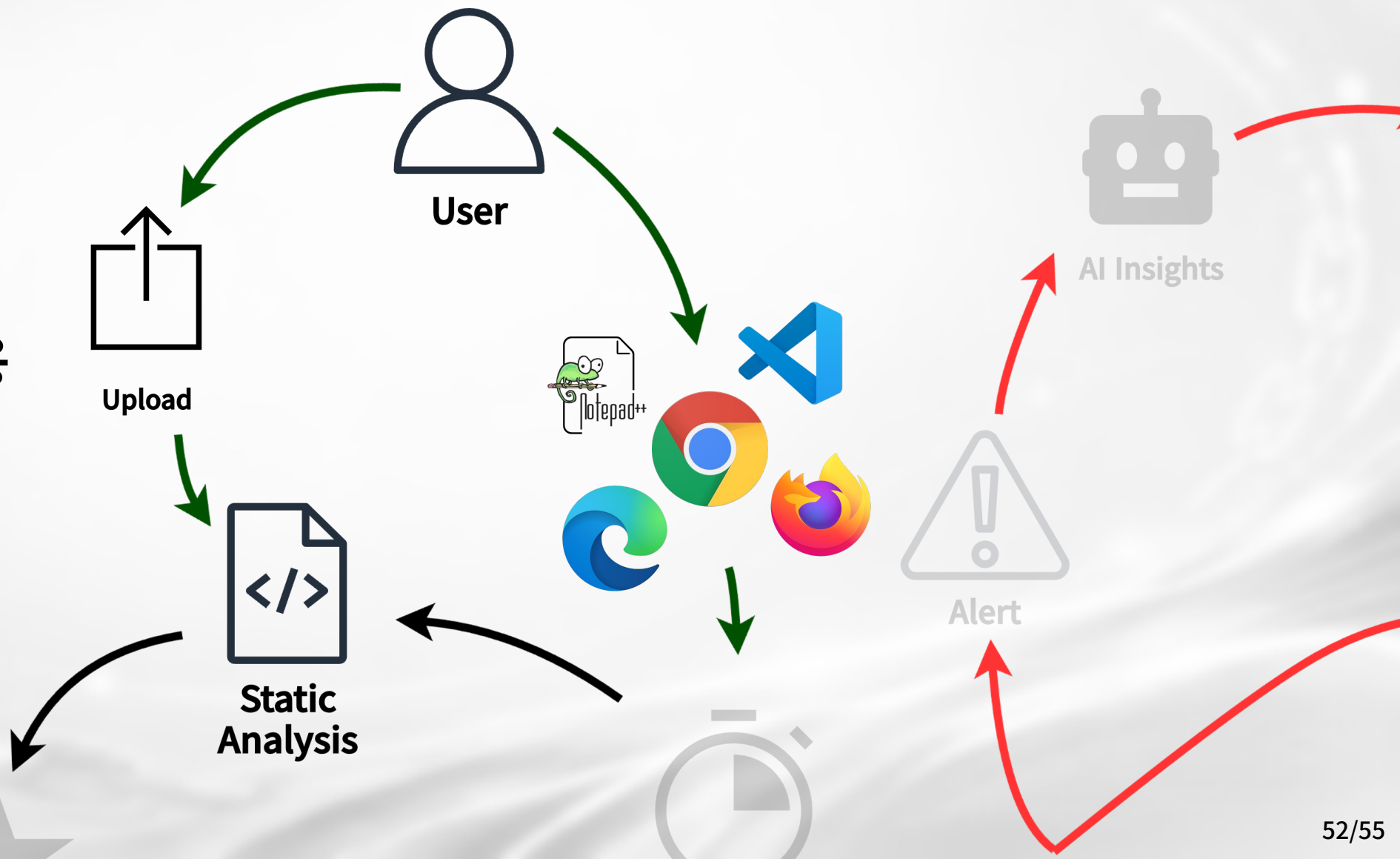
최종 시스템 구조



향후 계획

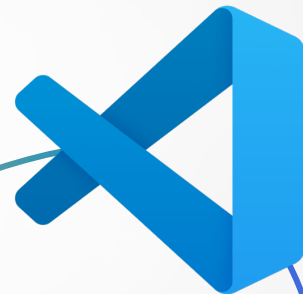
확장성

순환 구조를
유지하며 전체
파이프라인 활용



04. 프로젝트 결론

향후 계획

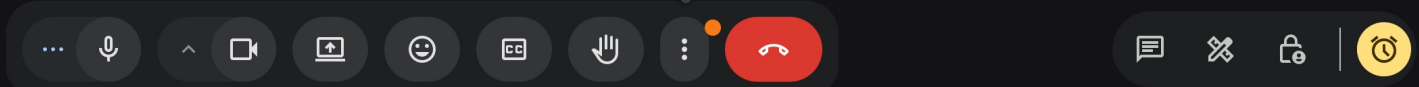


팀원들이 다함께 프로젝트를 **장기간 사이드 프로젝트**로 지속시킬 예정

Q & A

8:43 오후 | CCIT 온라인 미팅 ①

5



2026-1 정보보안SW융합전공

업데이트 기반 확장 프로그램 공급망 보안 시스템 설계

곽민경, 박혜수, 심재훈, 윤주혁, 정재성(PM)