컨테이너 이미지 취약점 분석 및 모니터링

OpenInfra & Cloud Native Days 2022

2022 . 11 . 01

제로원에이아이
윤명석

소개

윤명석

- 현) 제로원에이아이 AI Cloud 팀 / AI Cloud Engineer 연구원
- K8S, Container, DevOps - CKA

https://www.linkedin.com/in/myeong01

https://github.com/myeong01

컨테이너 이미지 취약점 분석 및 모니터링

무엇을 & 왜

언제

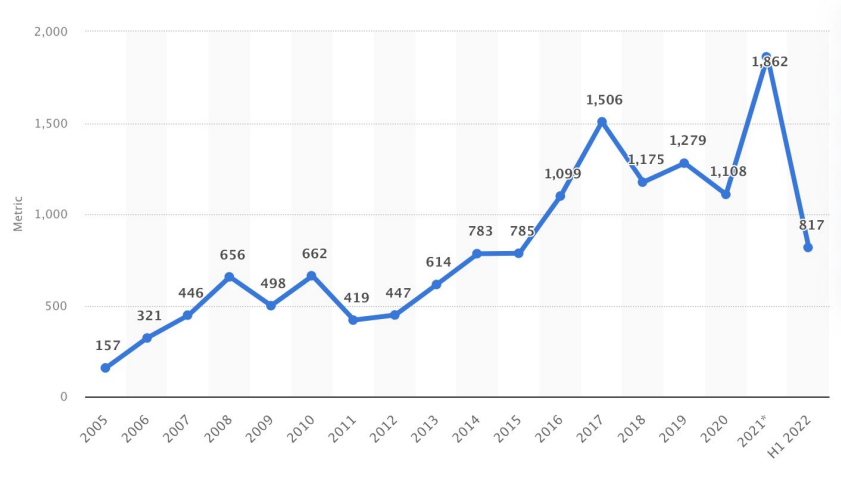
어떻게

무엇을 & 왜

보안

DevSecOps

증가하는 사이버 공격 건수



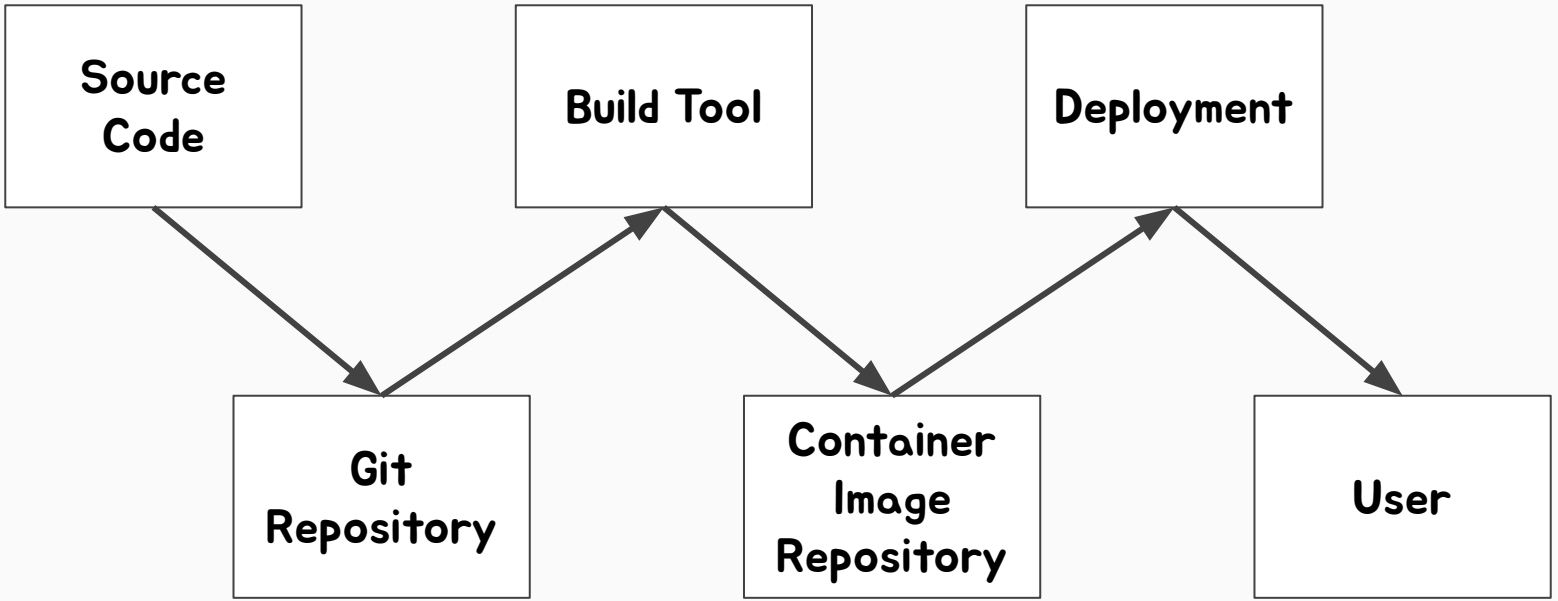
출처 : https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

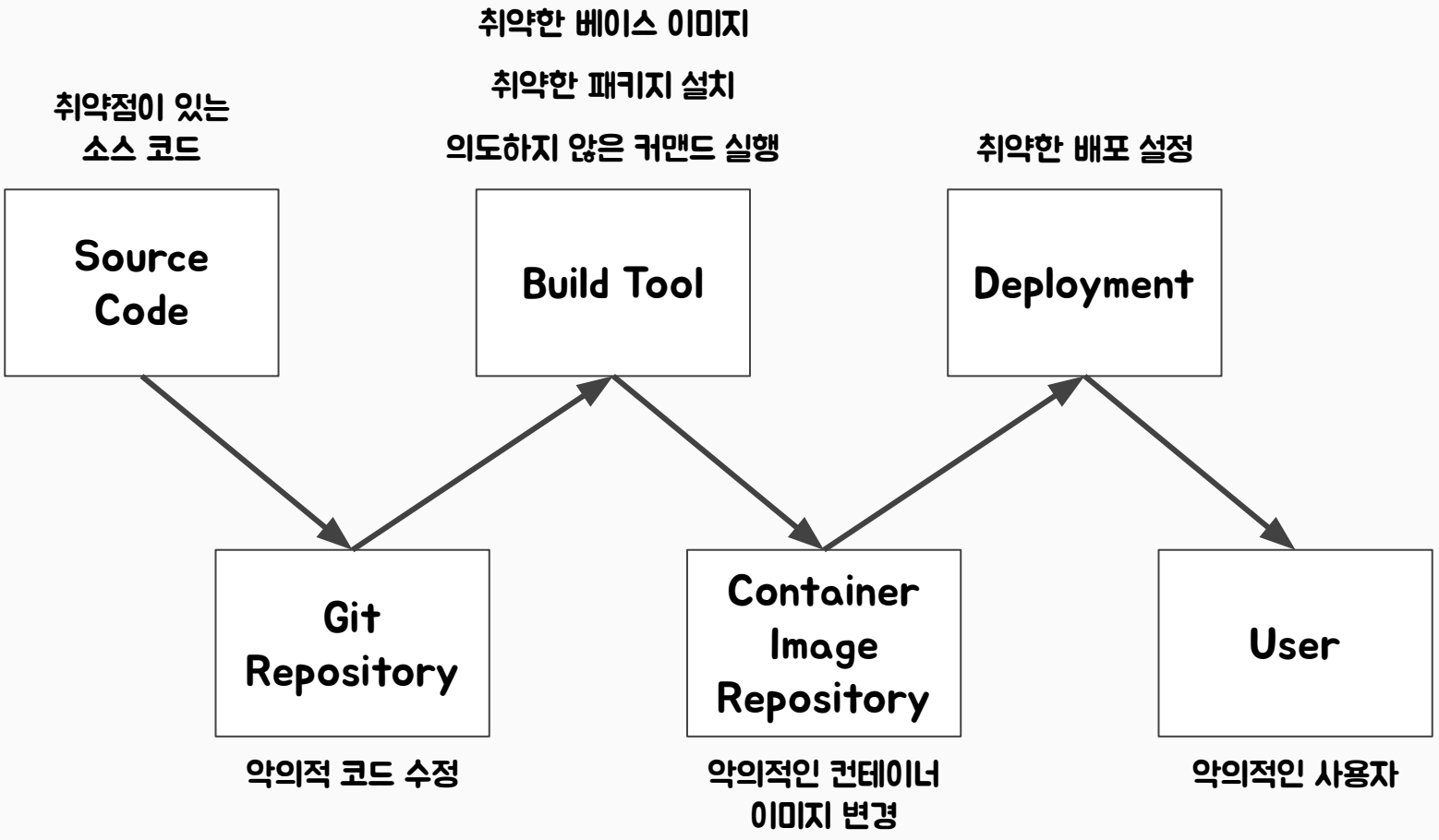
공급망 보안

공급망 보안

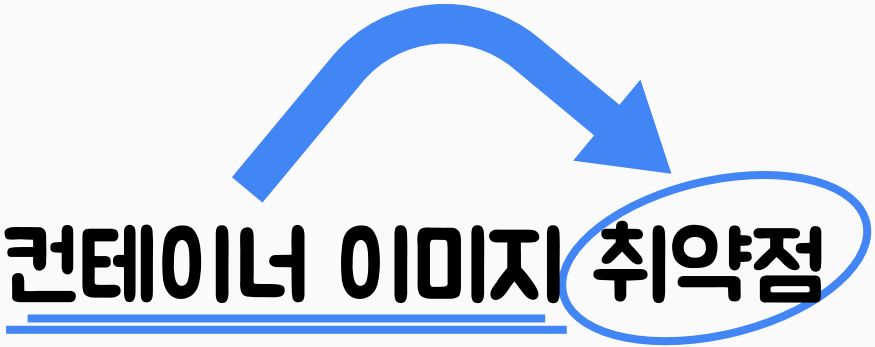
=

서비스 혹은 물건의 재료 수급부터
최종 고객에게 전달되기까지의 과정


Source Code
Build Tool
Deployment
Git Repository
Container Image Repository
User


취약한 베이스 이미지
취약한 패키지 설치
의도하지 않은 커맨드 실행
취약점이 있는
소스 코드
취약한 배포 설정
Source Code
Build Tool
Deployment
Git Repository
Container Image Repository
User
악의적 코드 수정
악의적인 컨테이너 이미지 변경
악의적인 사용자

컨테이너 이미지 취약점


컨테이너 이미지 취약점

컨테이너 이미지

=

컴퓨팅 시스템에서 컨테이너를 생성할 수 있는 실행 코드와 해당 코드를 동작시키기 위한 파일들이 포함된 정적 파일

컨테이너 이미지

=

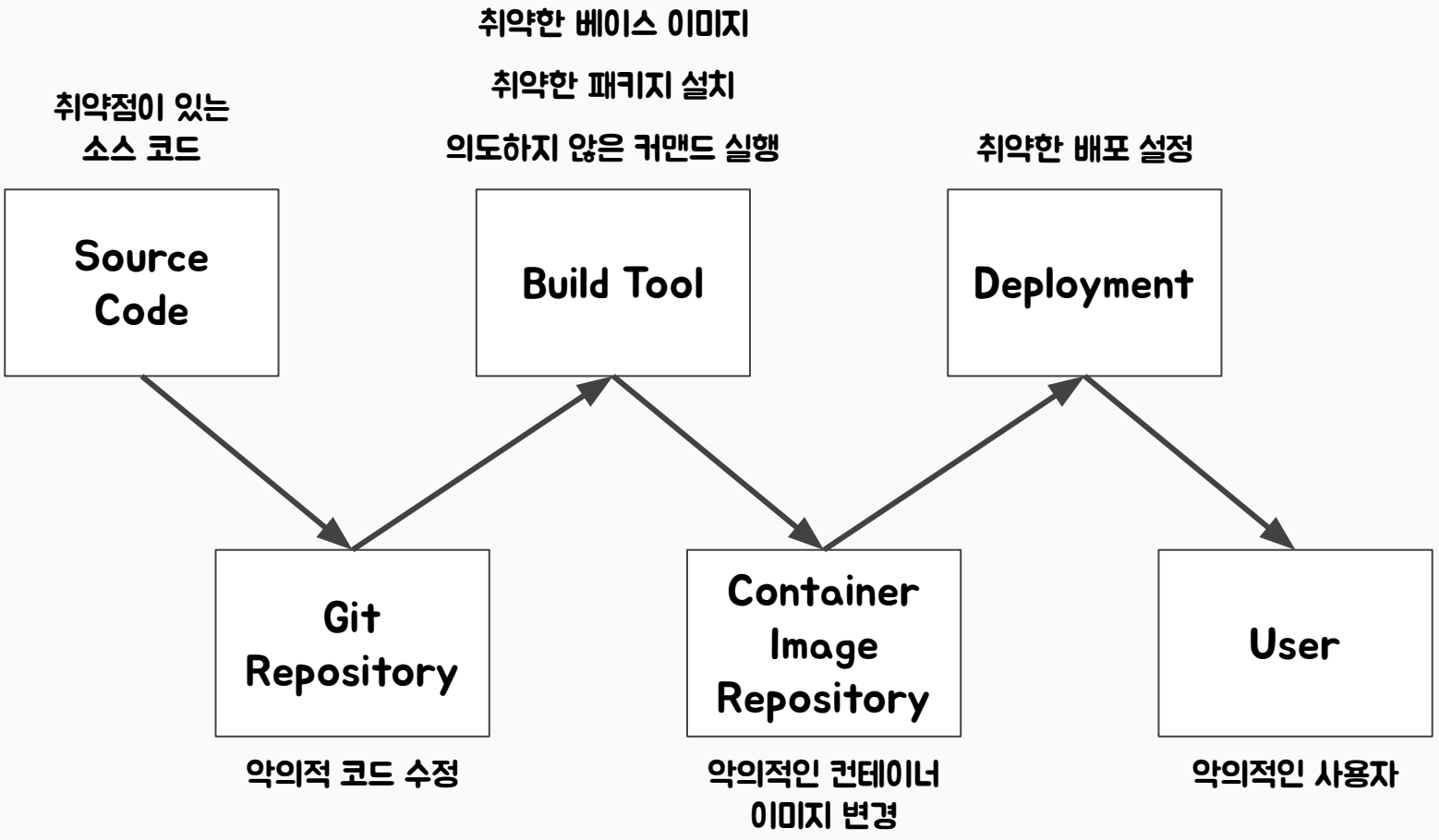
컴퓨팅 시스템에서 컨테이너를 생성할 수 있는

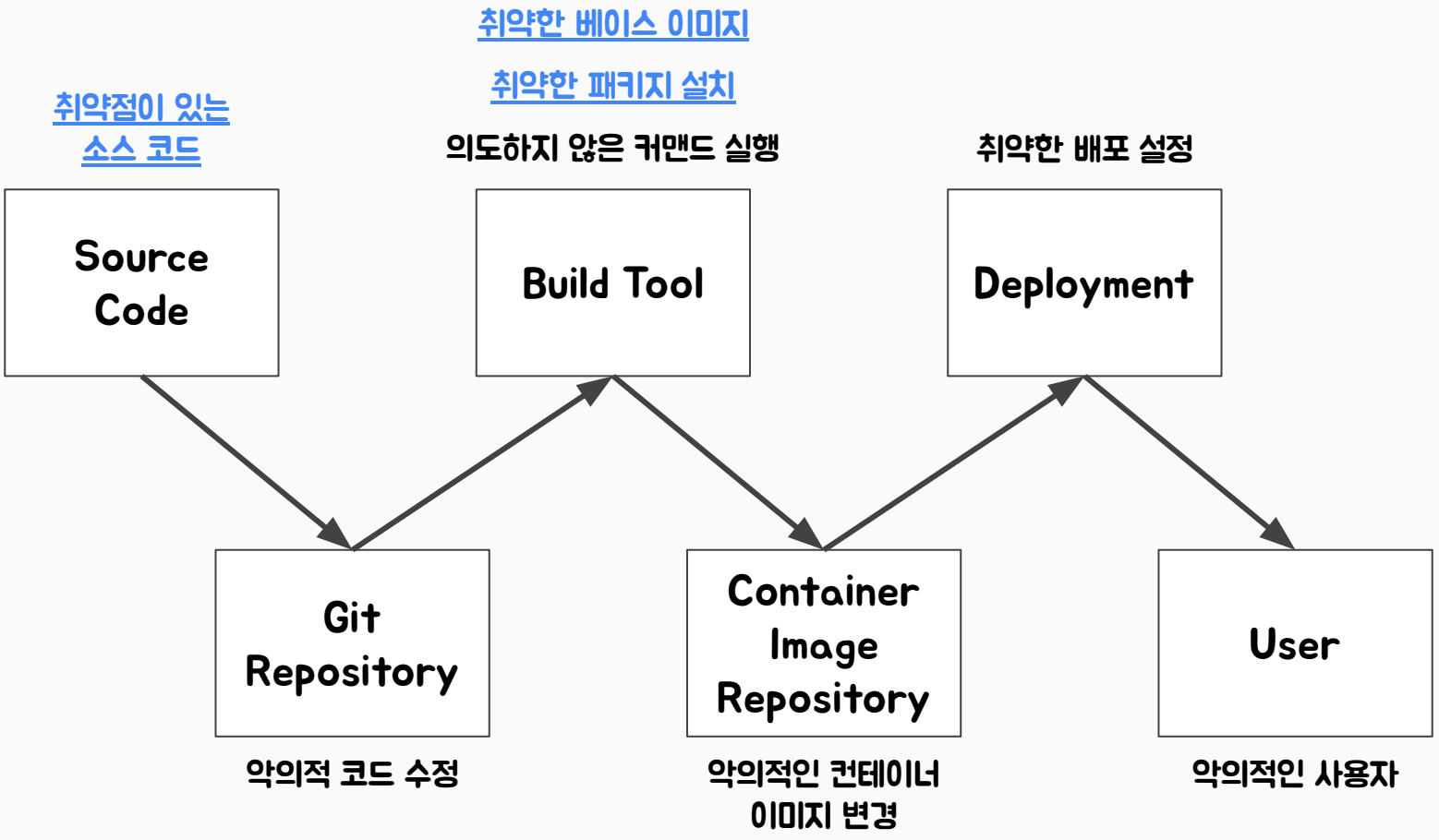
실행 코드와 해당 코드를 동작시키기 위한

파일들이 포함된 정적 파일

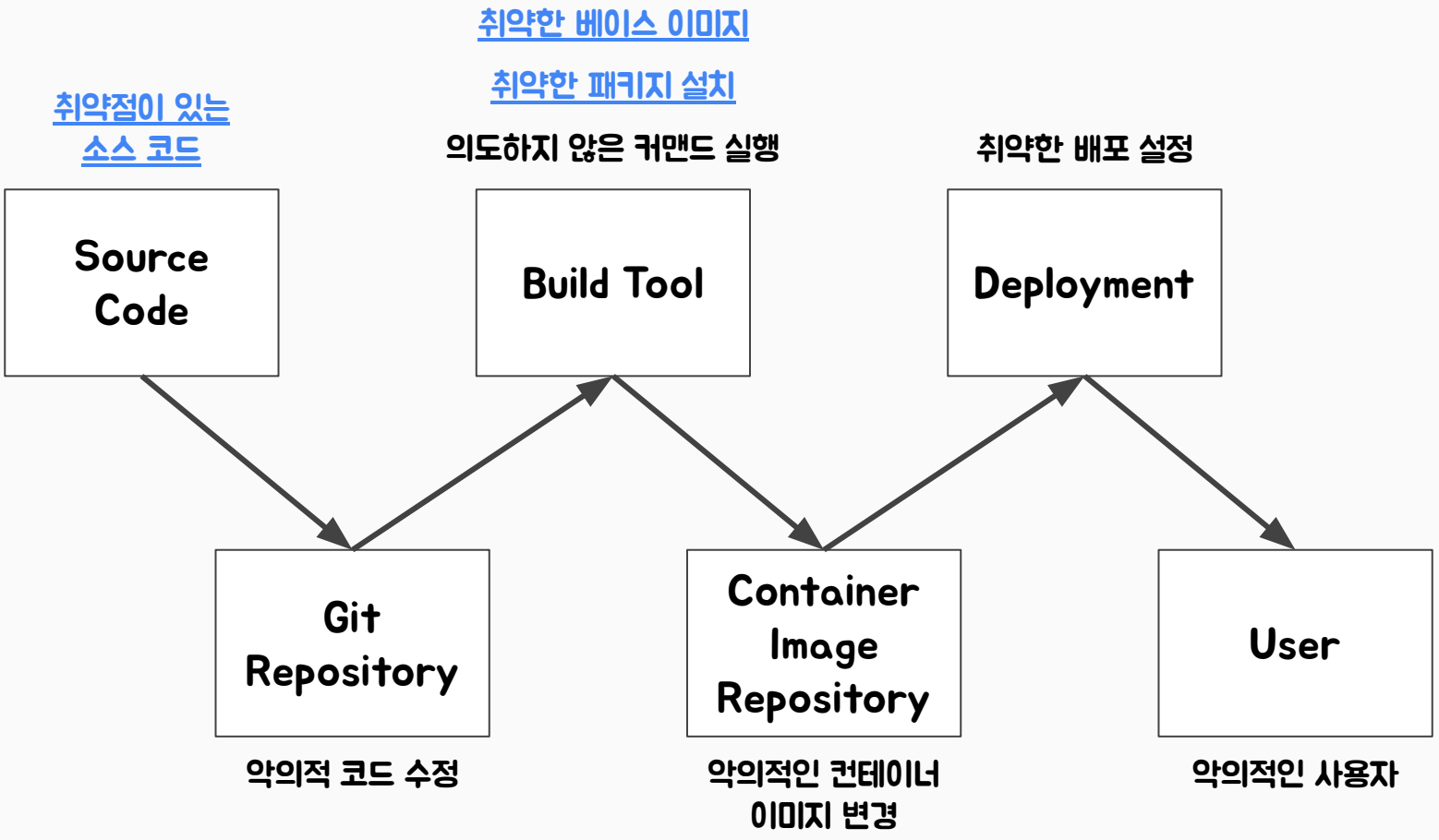
OS 패키지,
프로그래밍 언어 패키지,
설정 파일

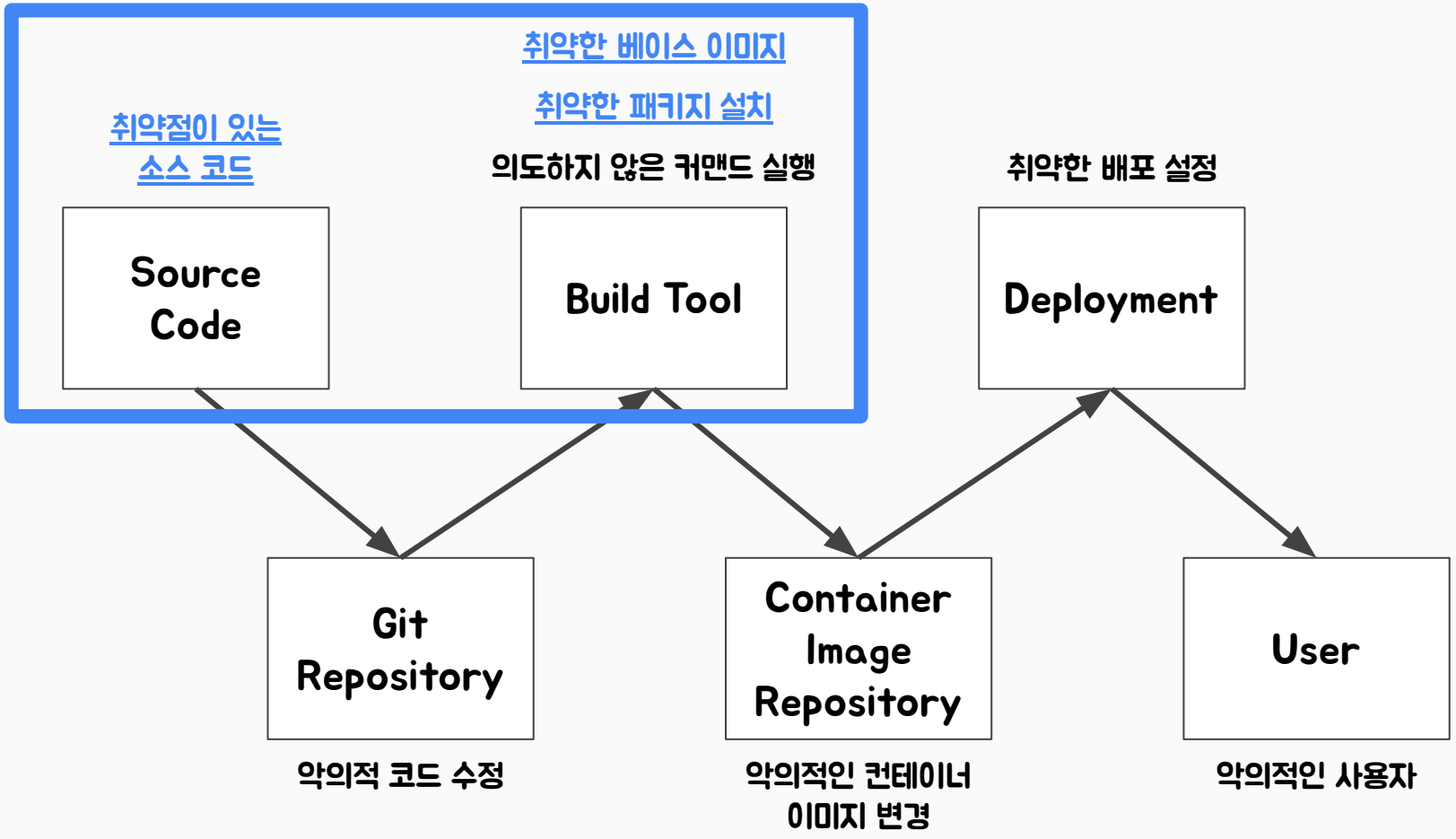
OS 패키지,
프로그래밍 언어 패키지,
실행 파일

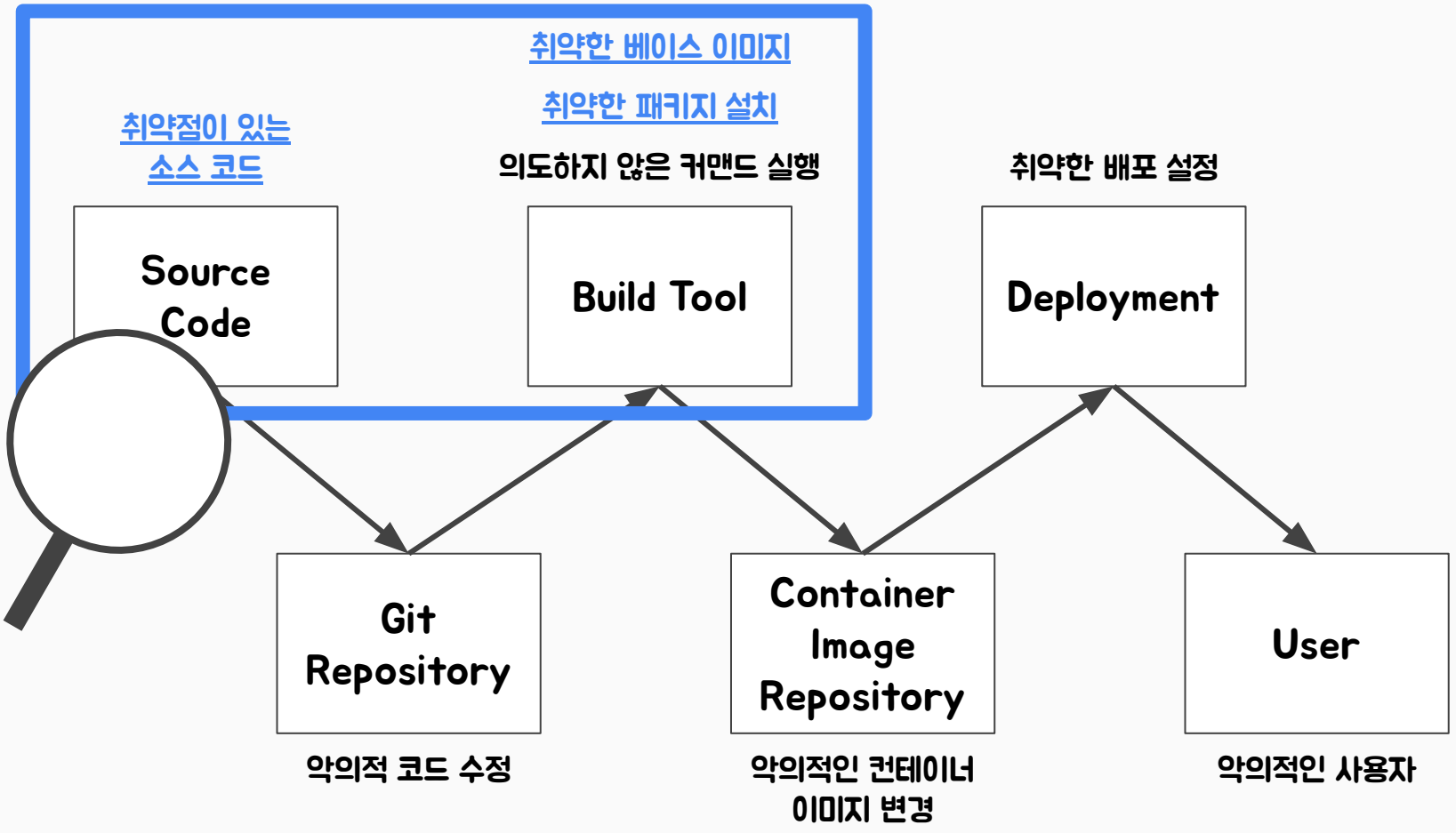

취약한 베이스 이미지
취약한 패키지 설치
의도하지 않은 커맨드 실행
취약점이 있는
소스 코드
취약한 배포 설정
Source Code
Build Tool
Deployment
Git Repository
Container Image Repository
User
악의적 코드 수정
악의적인 컨테이너 이미지 변경
악의적인 사용자

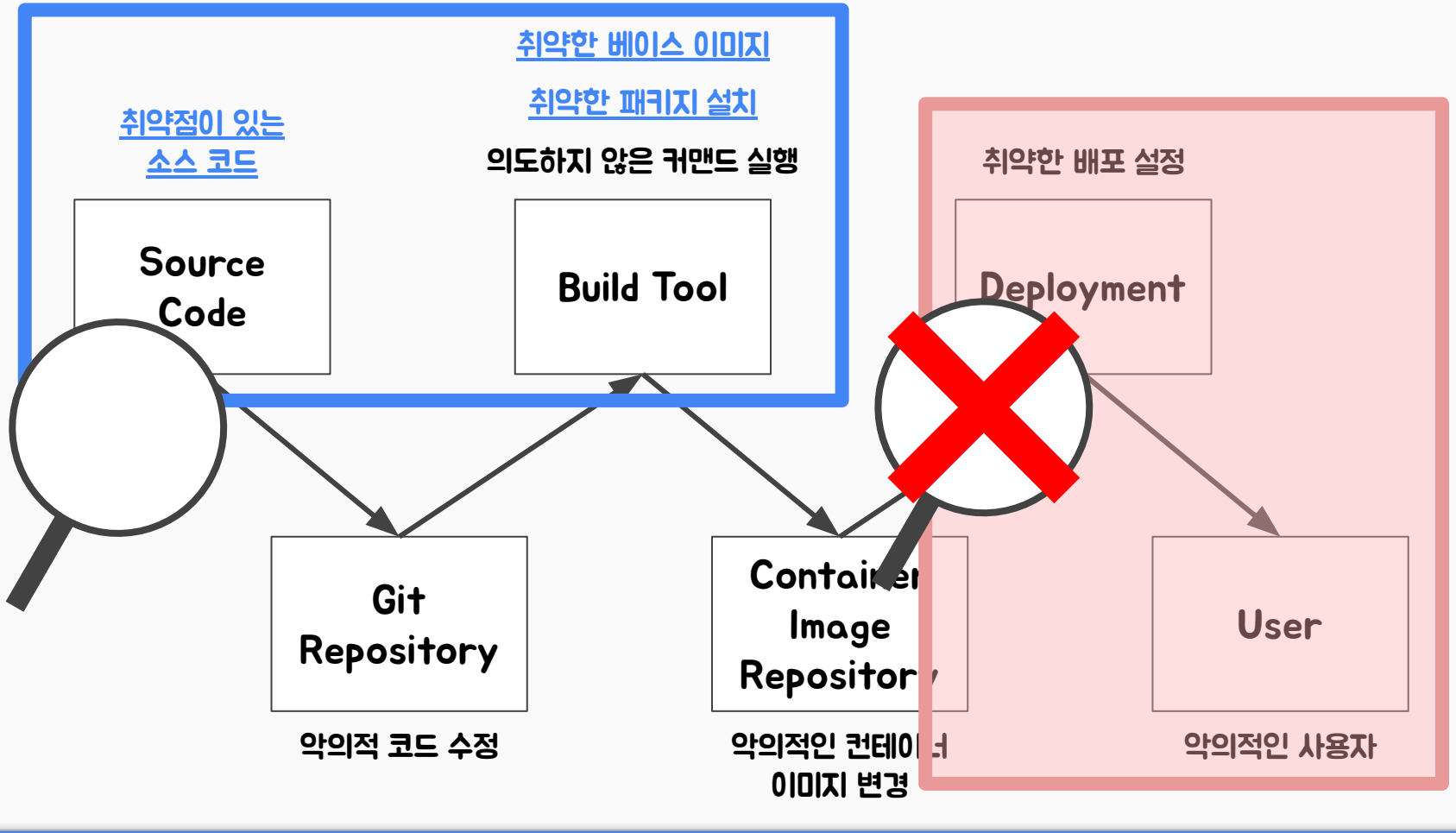

취약한 베이스 이미지
취약한 패키지 설치
취약점이 있는
소스 코드
의도하지 않은 커맨드 실행
취약한 배포 설정
Source Code
Build Tool
Deployment
Git Repository
Container Image Repository
User
악의적 코드 수정
악의적인 컨테이너 이미지 변경
악의적인 사용자

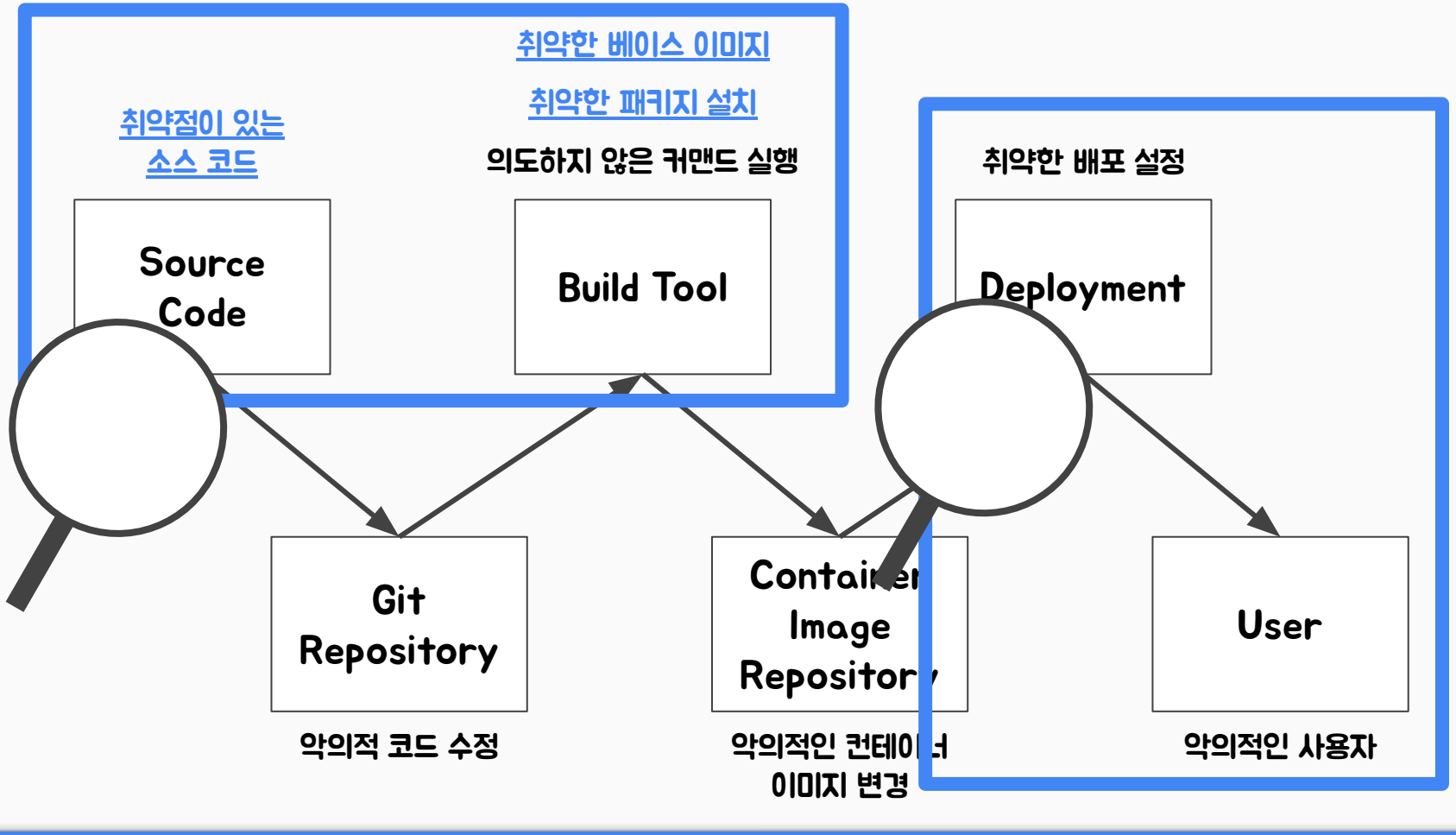
왜 모니터링을?


취약한 베이스 이미지
취약한 패키지 설치
취약점이 있는
소스 코드
의도하지 않은 커맨드 실행
취약한 배포 설정
Source Code
Build Tool
Deployment
Git Repository
Container Image Repository
User
악의적 코드 수정
악의적인 컨테이너 이미지 변경
악의적인 사용자


취약한 베이스 이미지
취약한 패키지 설치
취약점이 있는
소스 코드
의도하지 않은 커맨드 실행
취약한 배포 설정
Source Code
Build Tool
Deployment
Git Repository
Container Image Repository
User
악의적 코드 수정
악의적인 컨테이너 이미지 변경
악의적인 사용자


취약한 베이스 이미지
취약한 패키지 설치
취약점이 있는
소스 코드
의도하지 않은 커맨드 실행
취약한 배포 설정
Source
Code
Build Tool
Deployment
Git
Repository
Container
Image
Repository
User
악의적 코드 수정
악의적인 컨테이너
이미지 변경
악의적인 사용자


취약한 베이스 이미지
취약한 패키지 설치
취약점이 있는
소스 코드
의도하지 않은 커맨드 실행
취약한 배포 설정
Source
Code
Build Tool
Deployment
Git
Repository
Image
User
악의적 코드 수정
악의적인 사용자
이미지 변경


취약한 베이스 이미지
취약한 패키지 설치
취약점이 있는
소스 코드
의도하지 않은 커맨드 실행
취약한 배포 설정
Source
Code
Build Tool
Deployment
Git
Repository
Container
Image
Repository
User
악의적 코드 수정
악의적인 컨테이너
이미지 변경
악의적인 사용자

모든 취약점 ?

매일 업데이트되는 취약점들

컨테이너 이미지


LOG4J

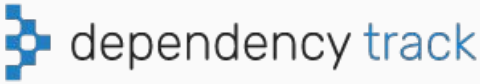
언제

컨테이너 이미지가 사용되는 동안 언제나

어떻게

컨테이너 이미지 취약점 스캔과 지속적인 추적과 관리

컨테이너
이미지 스캔



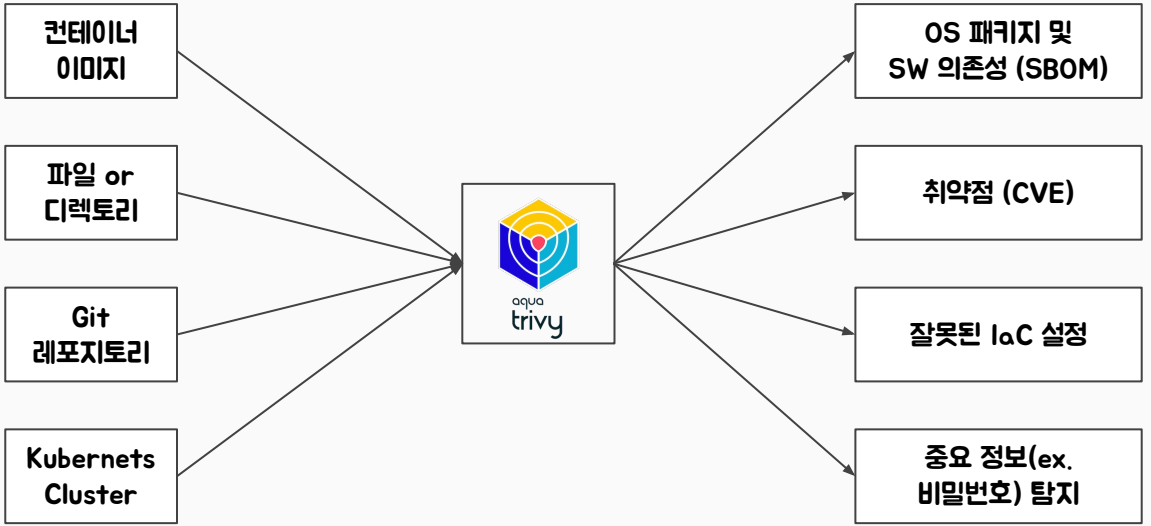
취약점
추적 및 관리

AI Secu

취약점
관리 자동화

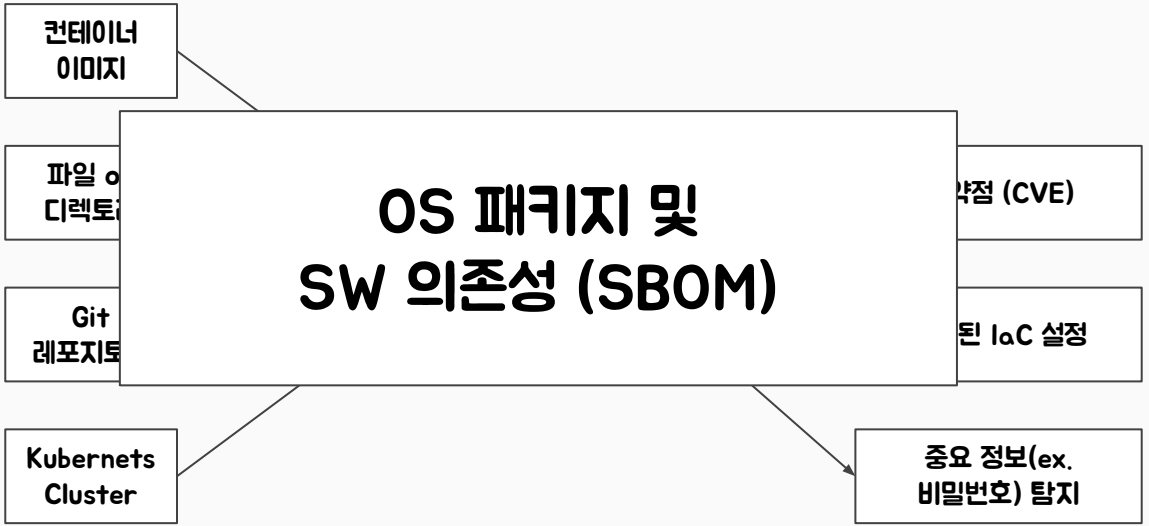
컨테이너 이미지 스캔

Github : https://github.com/aquasecurity/trivy
간단 설명 : 광범위한 보안 취약점 스캐너 오픈소스



컨테이너 이미지 스캔

Github : https://github.com/aquasecurity/trivy
간단 설명 : 광범위한 보안 취약점 스캐너 오픈소스



Software Bill of Materials (SBOM)

소프트웨어 개발과 실 운영에 있어 사용되는 모든 구성요소를 정리해놓은 명세서

NTIA 에서 인정한 SBOM 형식

출처 : https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

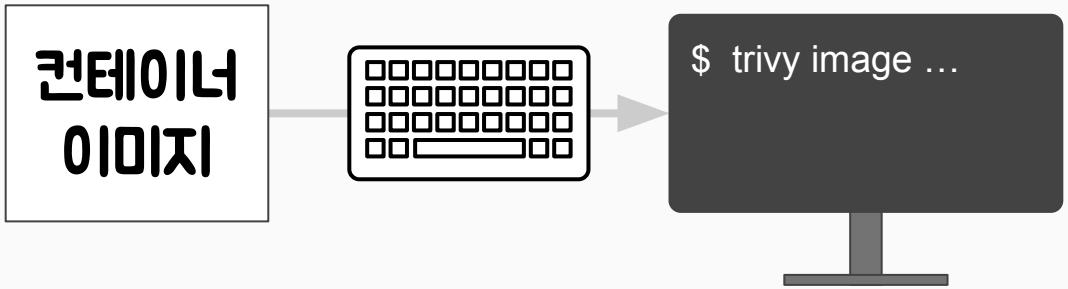
데모


zerooneai@ZeroOneAIs-MacBook-Pro:~
zerooneai@ZeroOneAIs-MacBook-Pro

GOOD

컨테이너 이미지 취약점과 구성 요소 스캔

1 회성 스캔

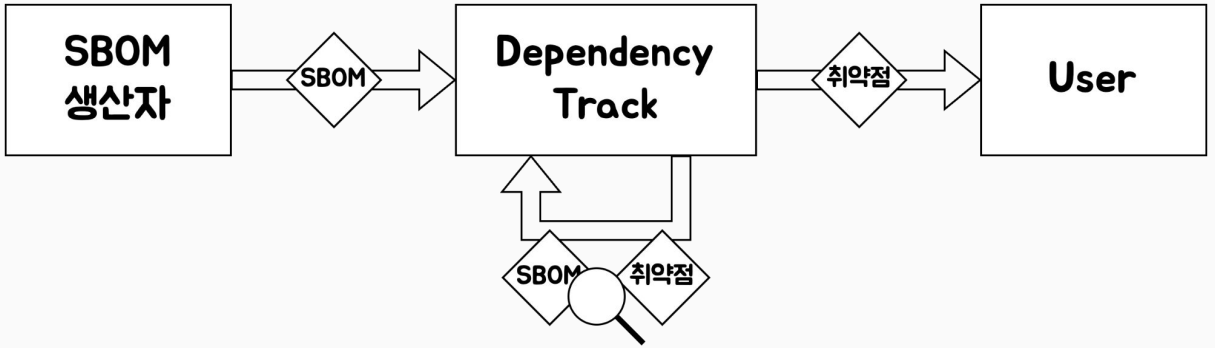


반복

dependency track

Github : https://github.com/DependencyTrack/dependency-track
간단 설명 : 구성 Component 분석 및 관리 오픈소스

취약점 추적 및 관리



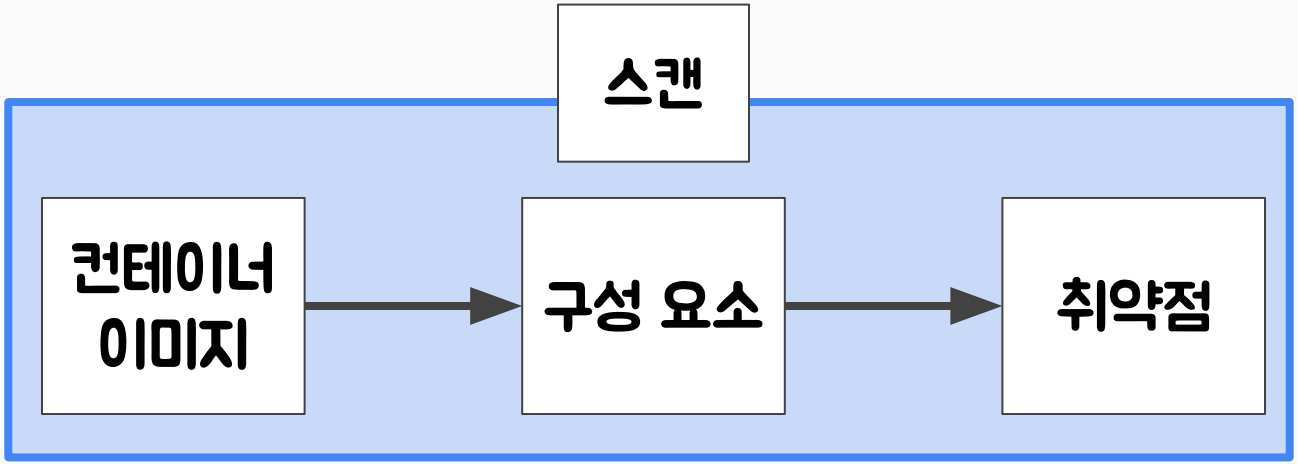
컨테이너 이미지 취약점

=

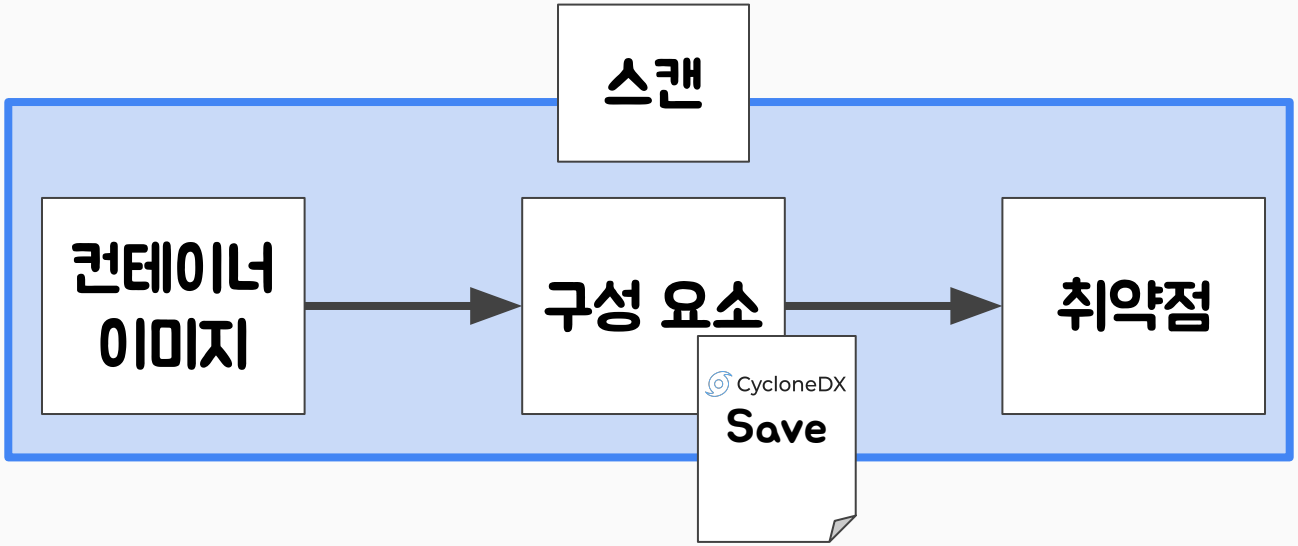
컨테이너 이미지의 구성 요소들의 취약점

CycloneDX

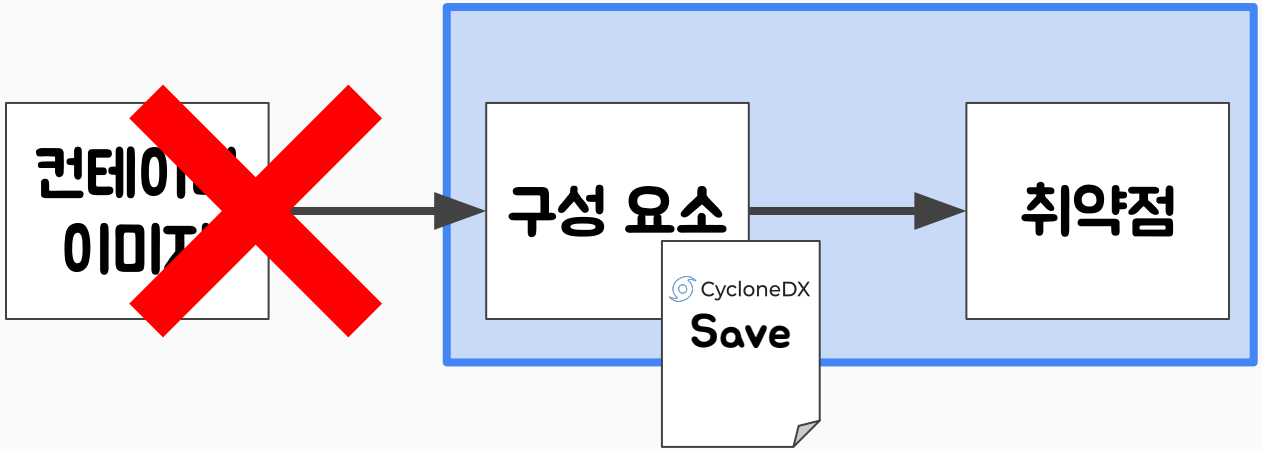
컨테이너 이미지의 구성 요소들의 목록



반복

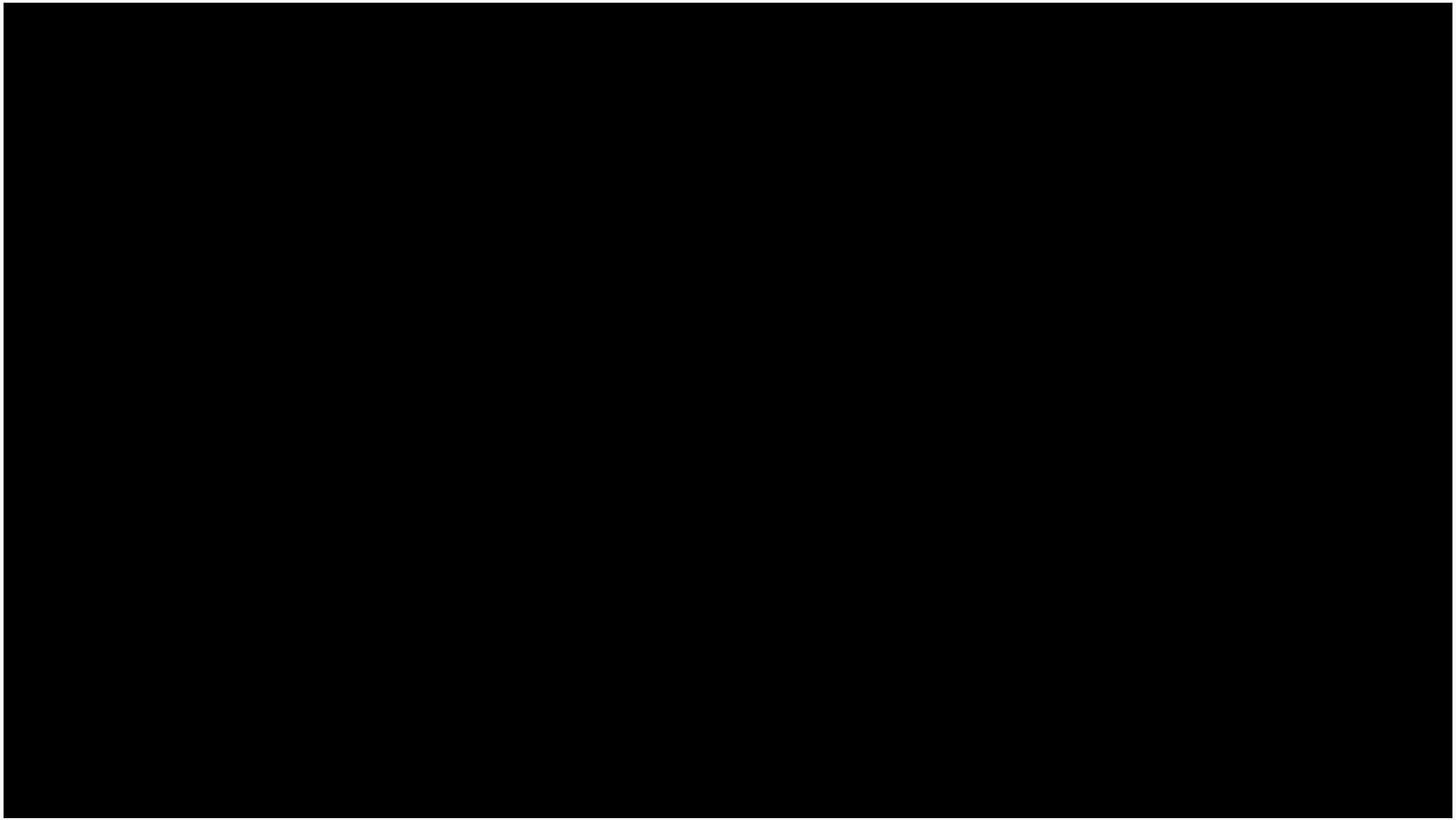


반복

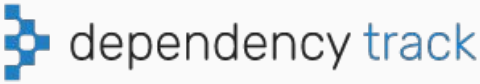


반복

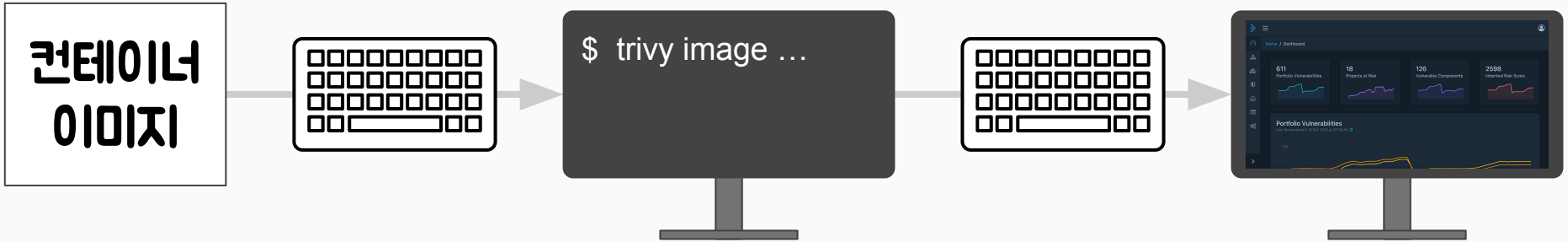
데모



컨테이너
이미지 스캔



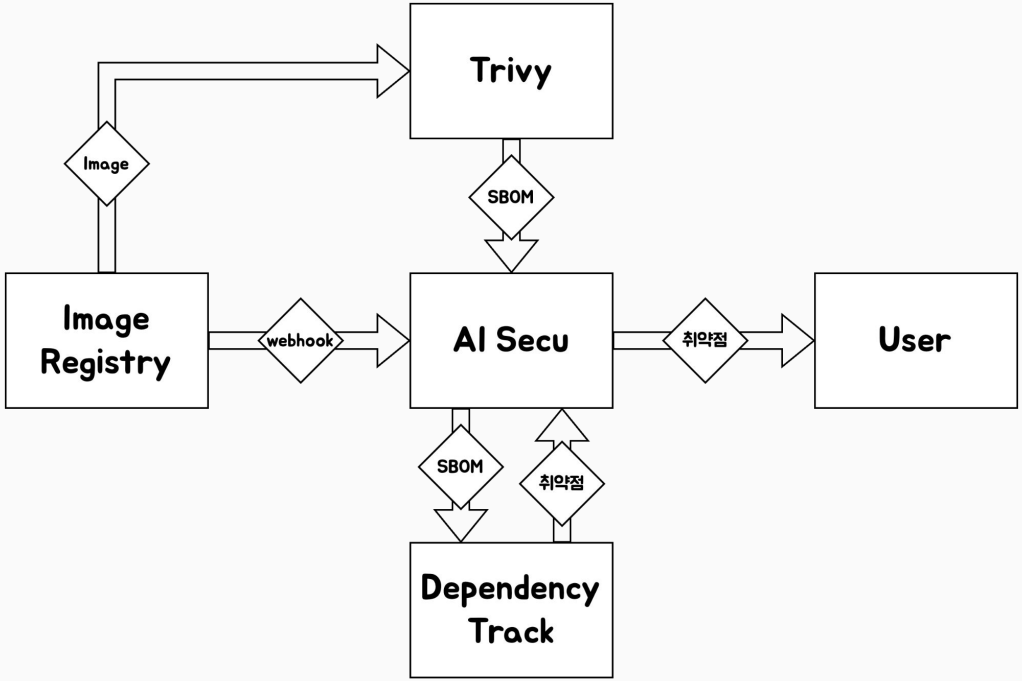
취약점
추적 및 관리


컨테이너
이미지
$ trivy image …
Portfolio Vulnerabilities

Github : https://github.com/ZeroOneAI/AISecu
간단 설명 : 컨테이너 이미지 자동 관리 오픈소스

AI Secu

취약점
관리 자동화



현재

Docker Hub 만 지원

정해진 취약점 스캐너와 취약점
관리 소프트웨어만 사용 가능

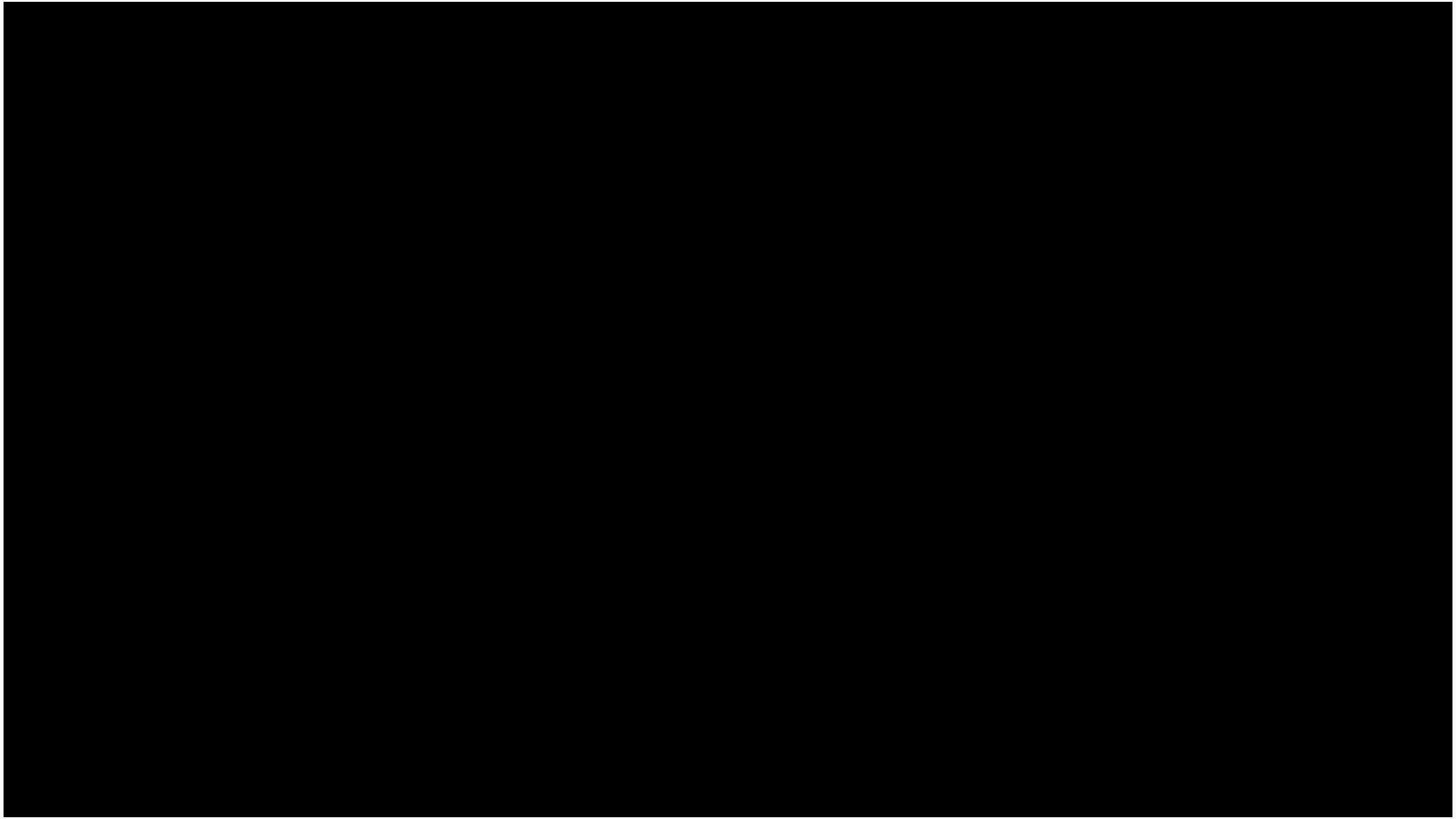
목표

ECR, Harbor 등 다양한
이미지 레지스트리 지원

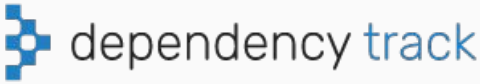
사용자 커스텀 스캐너와 취약점
관리 소프트웨어 적용 가능

https://github.com/ZeroOneAI/AISecu

데모



컨테이너
이미지 스캔

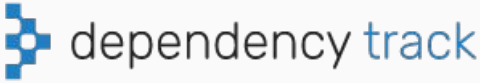


취약점
추적 및 관리

AI Secu

취약점
관리 자동화

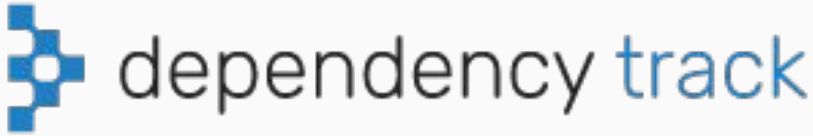
컨테이너 이미지 스캔



취약점
추적 및 관리

AI Secu

취약점
관리 자동화



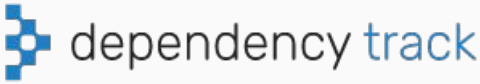
AI Secu

컨테이너
이미지 스캔

취약점
추적 및 관리

취약점
관리 자동화

컨테이너
이미지 스캔



취약점
추적 및 관리

AI Secu

취약점
관리 자동화

매일 새로운 취약점이 발견되는 세상 속에서

우리는 우리의 취약점을

효과적으로 관리할 줄 알아야한다.

감사합니다