

# 서버 자산 관리를 위한 서버 런타임 SBOM 솔루션



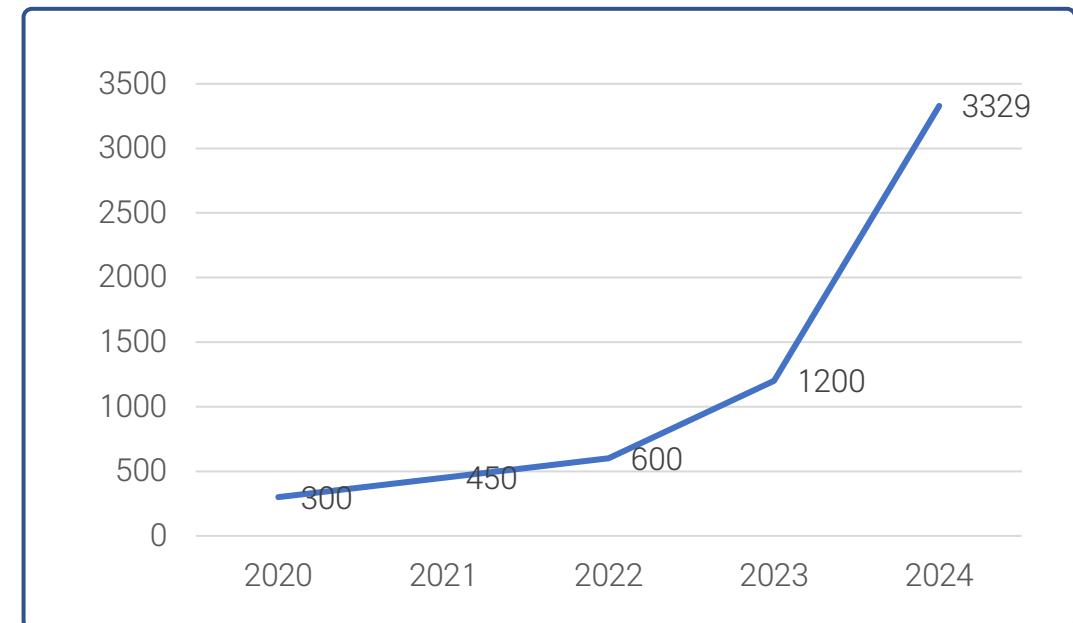
# 서버의 숨겨진 위협

① 오픈소스 활용의 보편화로, 서버의 보안 위협은 예측 불가능한 수준으로 증가했습니다

서버 생태계 주요 OSS 공격



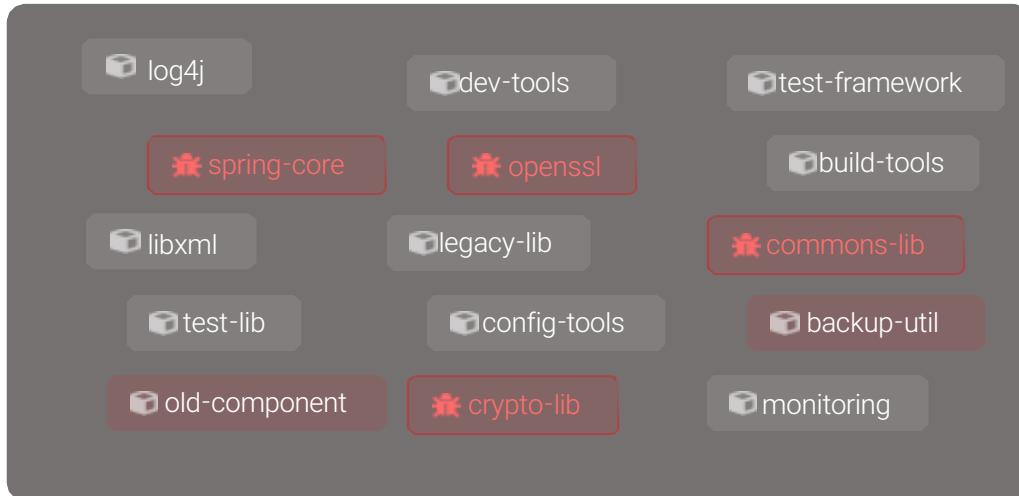
리눅스 생태계 CVE 증가



Log4j 사건이 발생했을 때 무엇이 가장 문제였습니까?

# 서버 OSS 취약점 관리의 실상

## 설치된 소프트웨어



설치된 패키지: 1,500개  
취약점이 있는 패키지: 30개  
과잉탐지 CVE : 987  
대응 계획 : 수립 불가

## 실행 되는 소프트웨어



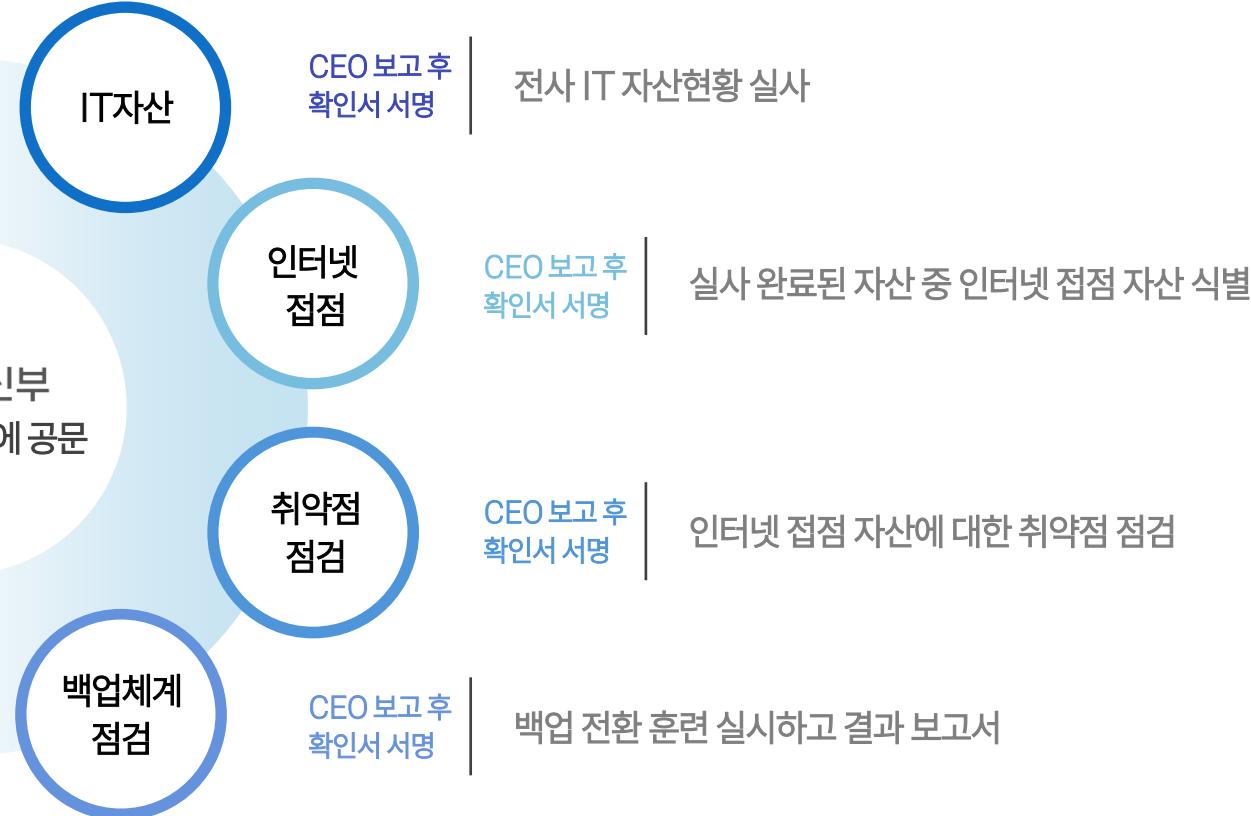
실행 되는 패키지: 30개  
취약점이 있는 패키지 : 4개  
초고도 위협 컴포넌트 : 1개  
대응 계획 : 패치 계획 수립

부정확한 위협 평가로 시간을 낭비하고 있지는 않습니까?

# 정부, 3만개 기업에 긴급 보안 점검 요청



2025.9.25  
과학기술정보통신부  
3만개 기업 CISO에 공문



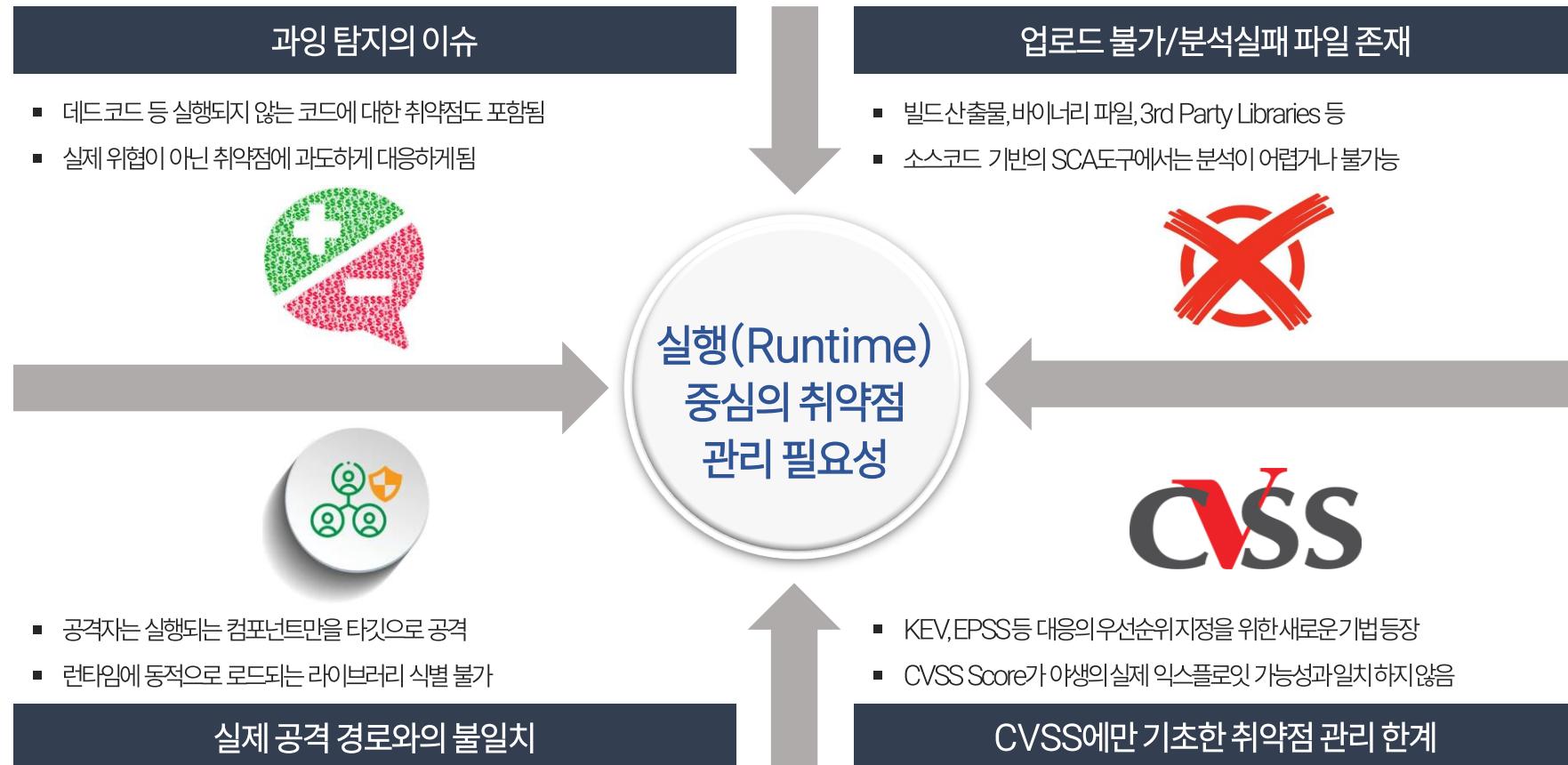
# 취약점 이슈 발생시 기업의 대응 예제

① 전문인력을 투입하여 4개월여만에 로그포제이가 포함된 서버 자산을 전부 알게 되었습니다



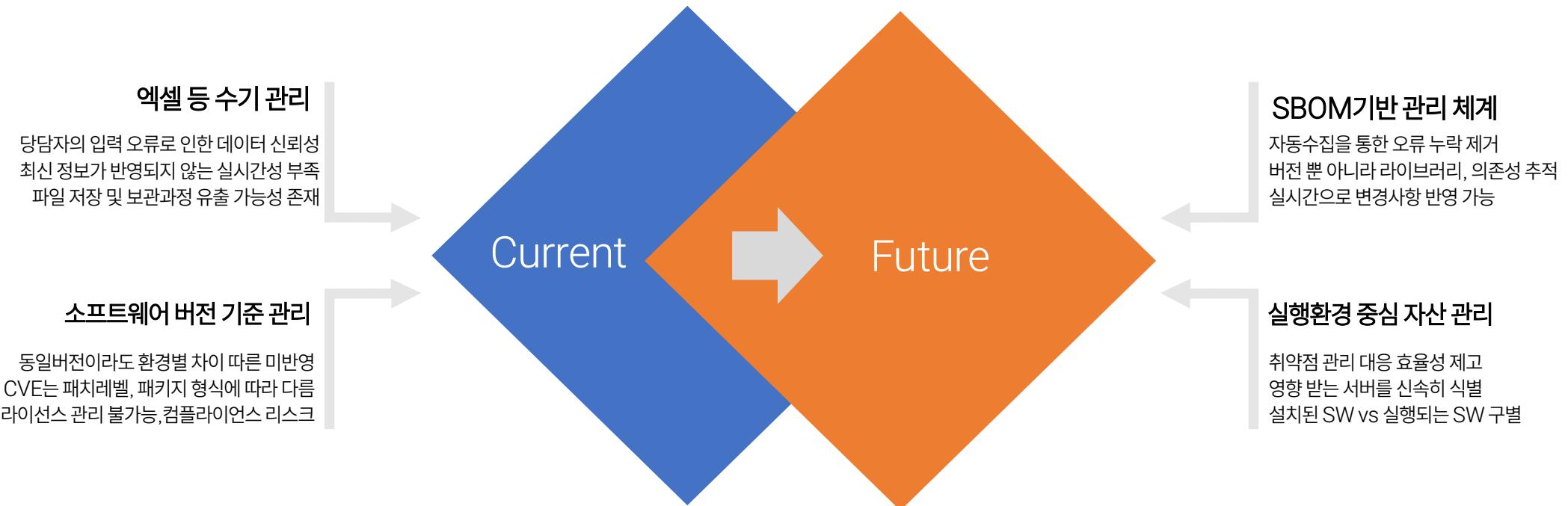
주요 취약점 이슈가 발생할 때마다 이 작업을 반복하시겠습니까?

# 기존 취약점 관리의 한계



제2의 Log4J 사건이 발생한다면 어떻게 대처하겠습니까?

# 기존 취약점 관리의 한계

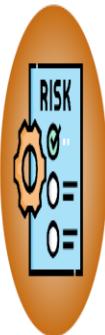


# 정부의 컴플라이언스 강화 방향

2025년 금감원의 디지털·IT 감독 검사 방향

✓ IT기술 활용에 따른 잠재적 리스크에 대한 점검을 강화하고 금융 사이버 복원력을 제고

## IT리스크 분석결과, 고위험권을 집중 검사



- ① 제3자 IT리스크: 중요 연계서비스에 대한 관리 실태 및 IT비상대책 수립·운용 적정성 등
- ② 보안통제 사각지대: 망분리 규제 완화 및 오픈소스SW 활용 등에 따른 보안 취약점 관리 실태 등
- ③ IT실태평가: IT감사 등 5개 부문 전반을 점검하되, 상시감시에서 확인된 핵심 취약부문은 집중 점검



보안통제의 사각지대에 있는 기업 내부 IT 자산에 대한  
오픈소스 취약점의 상시 점검 체계를 구축할 것을 지적

국가망 보안체계(N2SF) 보안 통제 항목 (제6장 정보자산 중)

## 보안통제 항목

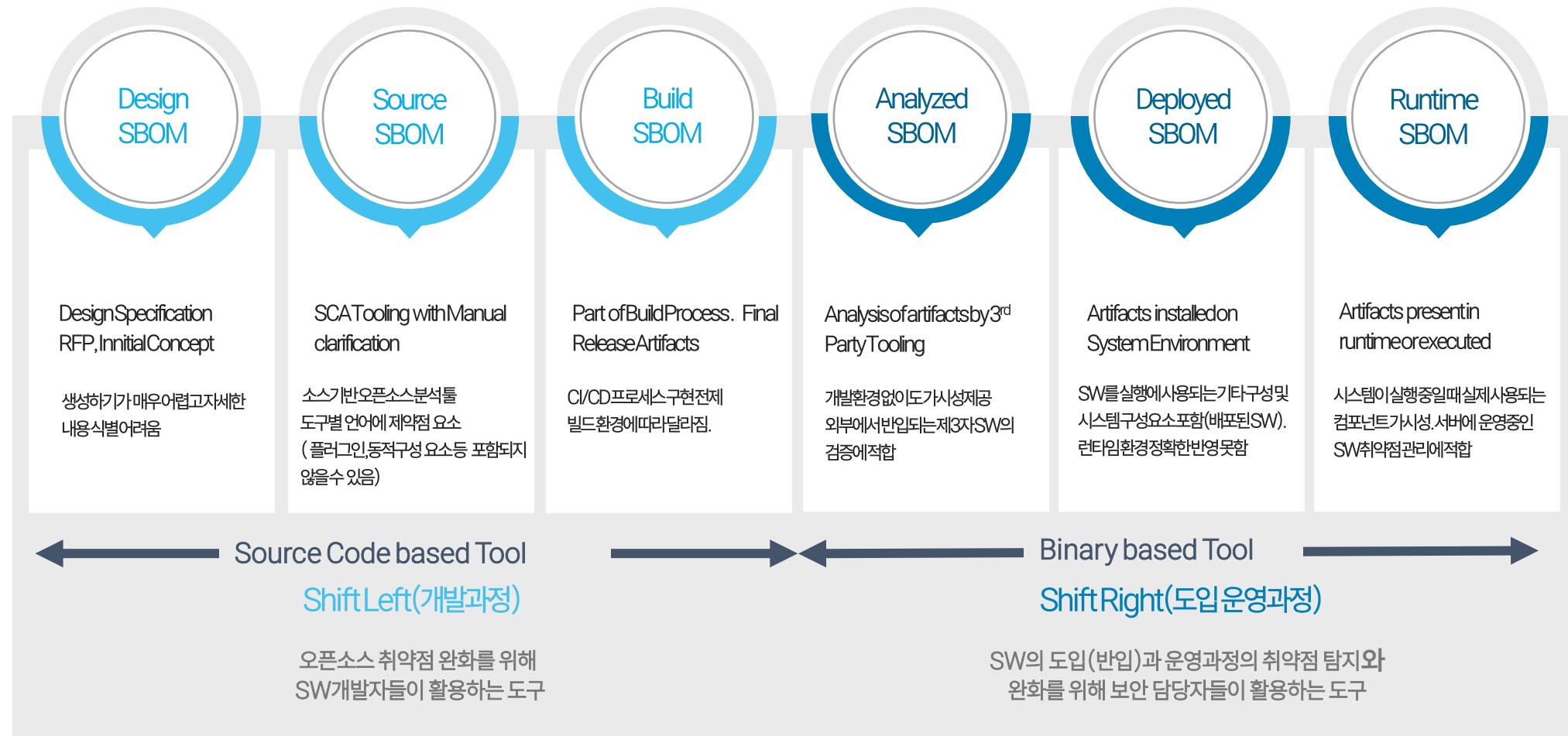
NNSF ID	보안통제 설명	
NNSF-IN-1	C S	정보시스템 구성요소 최신상태 유지 정보시스템 내의 모든 구성요소가 포함되도록 정보시스템 구성 요소 목록을 작성하고 정기적으로 검토 및 최신 상태로 업데이트 한다.
NNSF-IN-2	C S	구성요소 목록 현행화 정보시스템 구성 요소 설치, 제거, 또는 정보시스템 업데이트 시 목록을 갱신한다.
NNSF-IN-3		구성요소 목록 자동관리 자동화된 메커니즘을 통해 정보시스템 구성요소 목록의 최신성, 완전성, 정확성, 기용성을 유지한다.
NNSF-IN-4	C S O	비인가 구성요소 식별 정보시스템 내 비인가 하드웨어, 소프트웨어 및 펌웨어 구성 요소를 검사하여 식별한다.



설치/제거/업데이트되는 정보자산의 구성요소에 대하여 자동화된  
메커니즘을 통해 중앙 저장소에 목록화 및 현행화 필요성 제기

# 6 Types of SBOM

① CISA는 SW 생명 주기 및 데이터 원천에 따라 6개의 SBOM Type 규정



# 레드펜소프트 솔루션



- 외부에서도 입 및 반입하는 모든 유형 SW
- 보안 기반 반입 체계 및 무결성 검증 지원

Real-time Updates  
AI Agent 등 모든 기능 활용



- SW 개발 환경 연동하여 바이너리 파일 및 3rd Party 검증
- 기업 내부망 운용 중인 모든 유형의 SW 지원

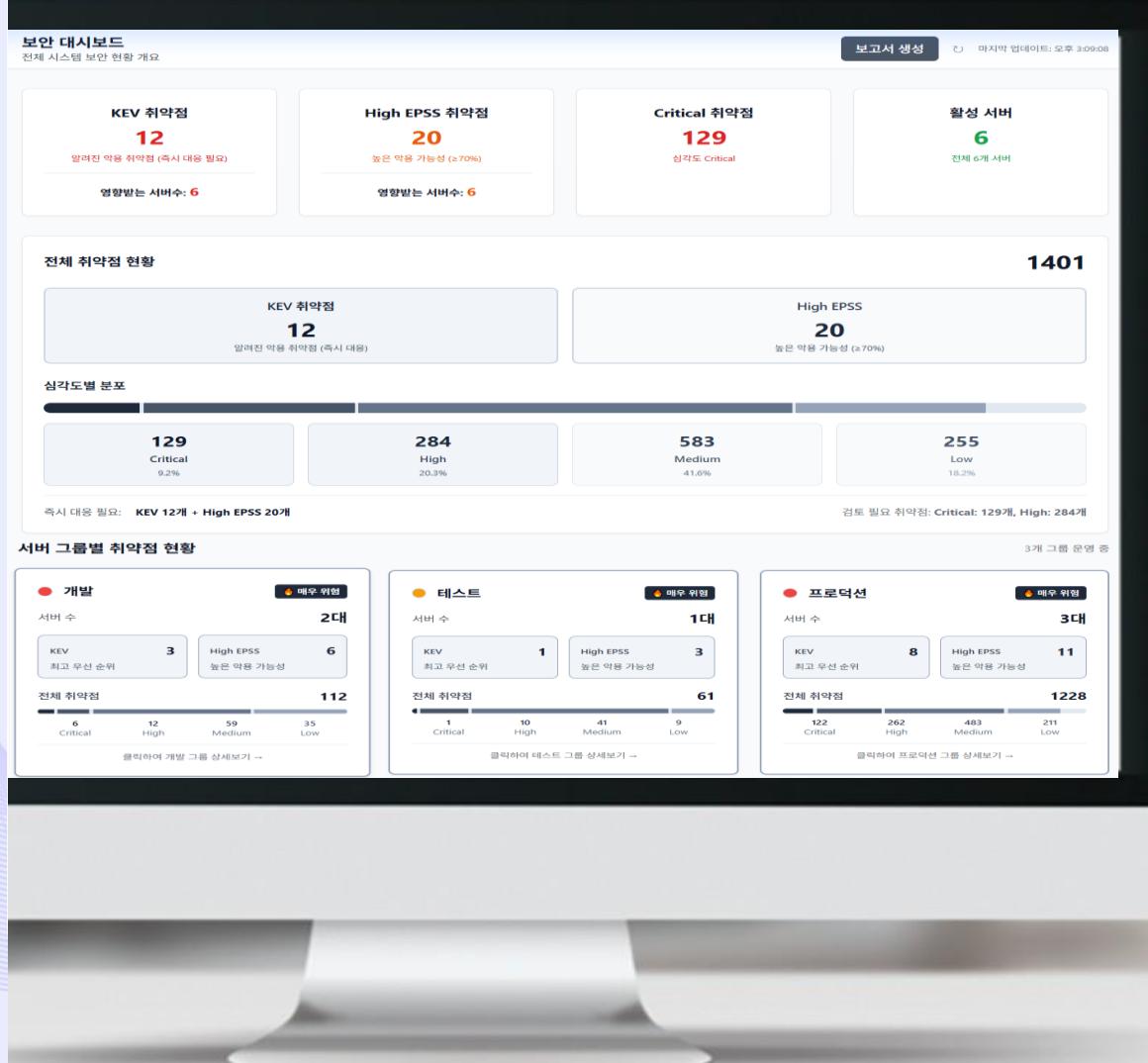
DB Update/1Month  
Relay Server 연동, AI Agent 기능 지원



- 서버에 설치된 SW 및 실제 실행되는 SW 감지
- 보안 관점 현실적인 SW 취약점 대응 지원

DB Update/1Month

# 엑스스캔 서버 런타임



- 기업의 내부 서버 자산 대상
- 실행 중인 소프트웨어 명세와 취약점 수집



- Deployed SBOM과 Runtime SBOM 생성
- 서버별 SBOM Repository System 구축

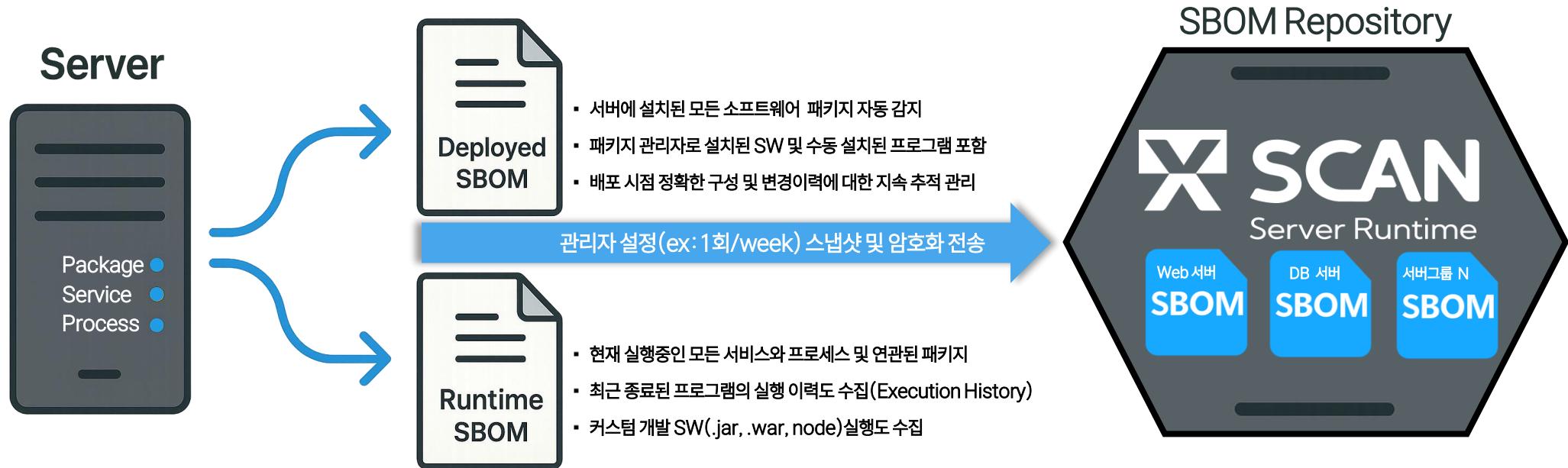


- 오픈소스 취약점과 라이선스 이슈 대응
- 규제 및 감독기관 컴프라이언스 준수

# 주요 특징



# 아키텍쳐 및 데이터 플로우



# Deployed SBOM & Runtime SBOM

① 시장의 주요 취약점 관리도구들은 대부분 Deployed SBOM 수준에 머물러 있습니다

## Deployed SBOM

설치된 패키지 기준

### 잠재위험 표면

비활성화 서비스의 권한상승/DLL 하이재킹 등  
초고도 해킹기법을 응용한 공격 가능성은 있음

### 설치자산 관리 관점

운영환경에 전혀 사용하지 않는 불필요한(방치된)SW를  
식별하여 제거함으로써 잠재위험 제거 및 규제 준수

## Runtime SBOM

실행되는 프로세스·컴포넌트 기반

### 실제 공격 표면

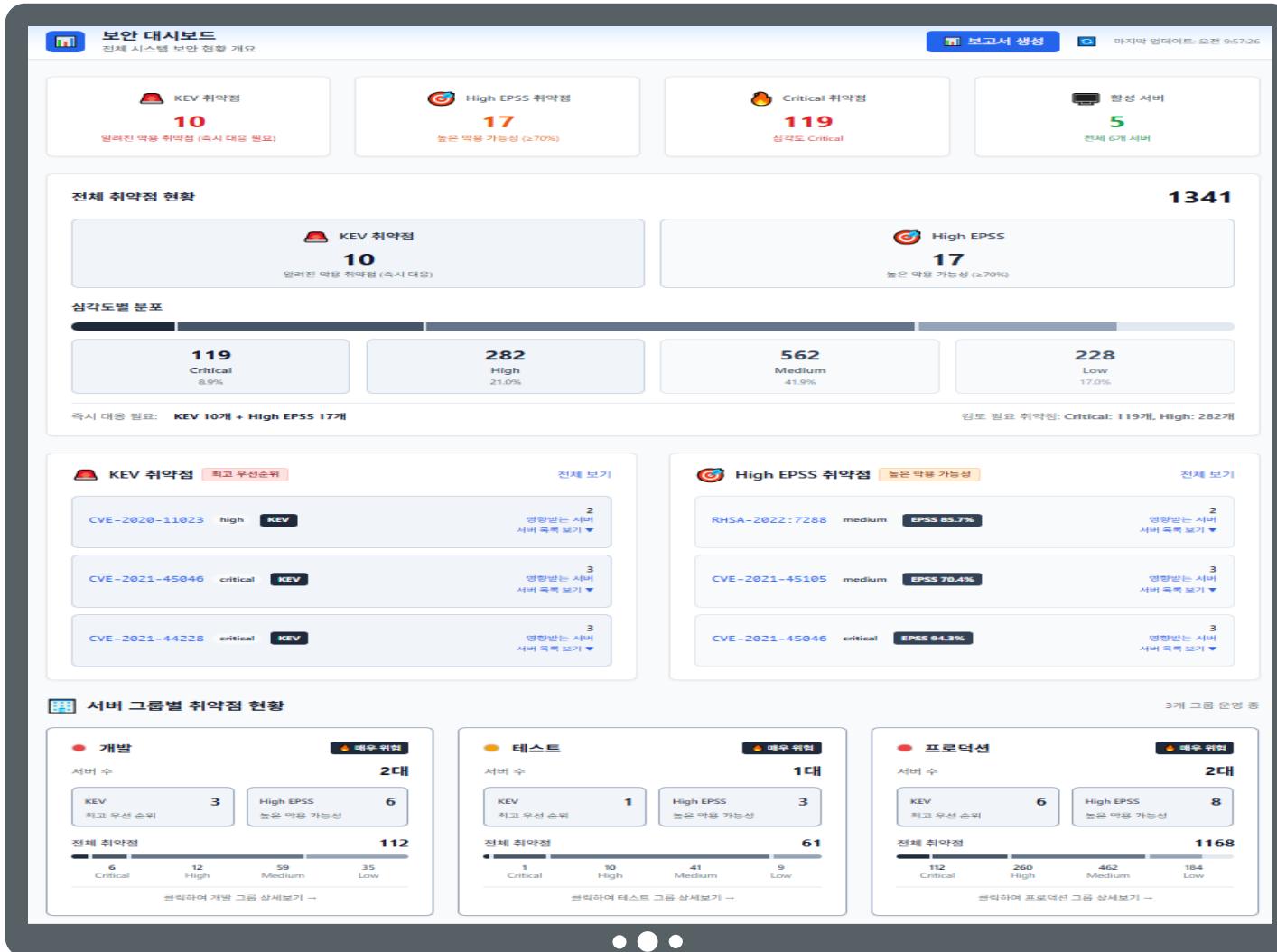
공격자의 1차 공격 표면으로 직접 네트워크 및  
로컬에서 취약점을 악용한 익스플로잇 가능

### 보안 운영 대응 관점

취약점 관리 최우선 대상으로 KEV/EPSS 등  
초고도 취약점에 대한 패치업데이트 실행

&

# 주요기능 : 대시보드



기업 내부 서버의 취약점 현황을 직관적으로 확인하고 취약점 완화 조치를 위한 보안 관점 우선 대응 순위를 지정할 수 있습니다!

## KEV Known Exploited Vulnerability 알려진 악용된 취약점(현재)

- 미국의 CISA가 관리하는 Must Patch List
- 악용되고 있음이 증명된 취약점, 2024년 185개
- 법으로 연방정부 기관은 반드시 패치하고 보고 조치

## EPSS Exploit Prediction Scoring System 취약점의 악용 가능성 예측 시스템(미래)

- FIRST(국제사이버보안사고대응조직)가 제정
- 30일 이내 악용될 가능성에 대한 머신러닝 기반 예측
- 조직의 보안 우선 대응 순위를 효율적으로 지원

# 주요기능 : 서버 기본 현황

서버 기본 정보      패키지 (1548)      서비스 (298)      실행중 프로세스 (387)      실행되었던 프로세스 (50)      네트워크 정보

시스템 정보

운영체제 Rocky Linux 9.6 (Blue Onyx) Red Hat Family	서버 정보 hskang-rocky9-dev Database Server	CPU 8 코어 Intel	메모리 15.33 GB 사용: 7.74 GB	아키텍처 x86_64 Red Hat/CentOS/Fedora
가상화 환경 VMware Virtual Platform cpu:8,mem:15701MB	CPU 모델 Intel(R) Core(TM) Ultra 7 265K Intel	디스크 사용량 92.85 GB / 95.55 GB 사용률: 97.18%	네트워크 192.168.18.138 ens160, docker0	

패키지 현황

설치된 패키지

설치된 패키지 타입 분포

1548 설치됨

Library: 440	Other: 896	System: 95	Kernel: 22	Python: 68
Ruby: 1	Java: 8	Go: 5	NPM: 13	

총 설치된 패키지 1548

실행 중인 패키지

실행 중인 패키지 타입 분포

206 실행됨

Other: 97	Library: 12	System: 12	Python: 64	Java: 7	NPM: 13
Kernel: 1					

실행 중인 패키지 206

각 서버별 시스템 기본 정보 및 서버에서 어떤 소프트웨어(패키지)가 실행되는지 비활성(미 사용)패키지는 무엇인지 확인할 수 있습니다!

# 주요기능 : 변화도 추적

런타임 SBOM 버전 비교

이전 버전: 250925.0628 현재 버전: 250926.0628.9

패키지 변경 서비스 변경 프로세스 변경 네트워크 변경 변경 대시보드

전체 취약 있음 안전 CRITICAL+ HIGH+ MEDIUM+ LOW+ KEV EPSS≥70% EPSS≥90%

installed-packages 검색...

총 1532개 항목

← 이전 버전 (제거됨)  
5개 항목

- ...0fc4e35e4ec970eed0348ed65d1d59d26234260 Standalone exec... Package
- ...8ed65d1d59d26234260/server/out/server-main.js Standalone script... Package
- ...ec970eed0348ed65d1d59d26234260/server/node Standalone executable detect... Package 2개 취약점 XSCAN 분석(2개 컴포넌트)
- ...s/node\_modules/typescript/lib/typingsInstaller.js Standalone script executed ... Library XSCAN 분석(1개 컴포넌트)
- ...ions/node\_modules/typescript/lib/typesMap.json Standalone script executed ... Library XSCAN 분석(0개 컴포넌트)

○ 변화없는 항목 (1522개)

- libgcc v11.5.0 GCC version 11 shared support library  
공급업체: Rocky Enterprise Software Foundation 라이선스: GPLv3+ and GPLv3+ with exceptions and GPLv2+ with exceptions and LGPLv2+ and BSD
- fonts-filesystem v2.0.5 Directories used by font packages  
공급업체: Rocky Enterprise Software Foundation 라이선스: MIT

...r-0b554a0d285c4e0dbeec34c61fd30984071f47c0 Standalone exec... Database

...34c61fd30984071f47c0/server/out/server-main.js Standalone script... Database

...85c4e0dbeec34c61fd30984071f47c0/server/node Standalone executable detect... Database 2개 취약점 XSCAN 분석(2개 컴포넌트)

...s/node\_modules/typescript/lib/typingsInstaller.js Standalone script executed ... Library XSCAN 분석(1개 컴포넌트)

...ions/node\_modules/typescript/lib/typesMap.json Standalone script executed ... Library XSCAN 분석(0개 컴포넌트)

서버에서 실행되는 패키지/서비스/프로세스/  
네트워크 노드의 변경(제거/추가 등) 되는  
모든 내역을 추적합니다!

# 주요기능 : 네트워크 정보

The screenshot displays a network monitoring interface with the following sections:

- Top Navigation:** 서버 기본 정보, 패키지 (1548), 서비스 (298), 실행 중 프로세스 (387), 실행되었던 프로세스 (50), and 네트워크 정보 (selected).
- Network Filter:** 네트워크, 전체, 리스닝, 아웃바운드 (selected), and 인바운드.
- Outbound Connections:** 총 5개 항목 (네트워크 필터: outbound).
  - node PID: 4074694: Service (4개 취약점, 3개)
  - node PID: 4074766: Service (4개 취약점, 3개)
  - node PID: 4085460 포트: tcp:5000: Service (4개 취약점, 3개)
  - ora\_ireg\_free PID: 2676: Service (1개)
- System Information:** 시스템 정보: Service Type: 기타, Outbound Count: 1, Risk Level: low.
- Network Summary:** 네트워크 정보: 인바운드 연결 0개, 아웃바운드 연결 1개.
- Connected Packages:** 연결된 패키지 (1개): oracle-database-free-23ai v1.0 Oracle 23ai Free Database. 공급업체: (none) 라이선스: Oracle Corporation.

SW 실행과 관련된 네트워크 리스닝, 아웃바운드, 인바운드 및 해당 네트워크 프로세스에 관련된 취약점을 파악할 수 있습니다!

# 주요기능 : Oracle 제품의 취약점 분석

취약점 상세 정보 CRITICAL K-EV

연결된 패키지: [standalone:/opt/oracle/middleware/wlserver/server/lib/weblogic-launcher.jar](#)

**CVE-2020-14882**

K-EV 94.5%

Oracle Critical Patch Update에서 수정된 취약점입니다. CPU 날짜: 2020-10-16

데이터 소스: [Oracle CPU](#)

관련 ID:  
CVE-2020-14882

담겨진 컴포넌트 정보

**weblogic** v12.2.1.4.0 신뢰도: 99% [standalone:/opt/oracle/middleware/wlserver/server/lib/we...](#)

순위 #1

매칭 방법: Identifier Matching

매칭 항목: 1개

언어 분포:

■ 정보 없음

사용 가능한 패치 버전: 1개 (상용 패치 포함)

상용 소프트웨어 패치:  
1763514094

CPU 발행일: 2020-10-16

💡 CVE-2020-14882를 해결하는 패치 버전입니다.

리눅서 서버에 설치된 상용SW인 Oracle 제품군(DB, Weblogic, Java등)에 대한 취약점 분석 지원

# 도입효과

**완전한가시성** | 서버에 설치된 모든 SW 목록 제공

**라이선스관리** | 상용SW 및 OSS 라이선스 추적

**비용최적화** | 불필요한 SW 식별로 비용 절감

**감사대응자동화** | 상부기관의 SW 취약점 감사 등

**SW리스크관리** | 법적분쟁, SW 리콜 등 위험 감소

**비용절감** | 고비용의 외부 컨설팅 비용 절감



**인시던트대응** | 영향받은(는) 시스템 범위 신속파악

**우선순위지정** | 취약점 완화를 위한 패치 우선순위

**구성및변경추적** | 서버 간 구성차이 및 변경 추적

**취약점식별** | 신규 설치 SW의 취약점 사전식별

**공격경로분석** | 해킹 시 영향받은 프로세스와 파일 추적

**실시간위협탐지** | 승인되지 않은 프로그램 실행 감지

# Building a Relialble Software Value Chain



경기도 과천시 과천대로7나길9, DX타워 4층  
TEL. 02-2219-2585

Copyright 2025. Redpensoft Co., Ltd. All Rights Reserved.

독고준 팀장  
[Jun.dockko@redpensoft.com](mailto:Jun.dockko@redpensoft.com)

[www.redpensoft.com](http://www.redpensoft.com)