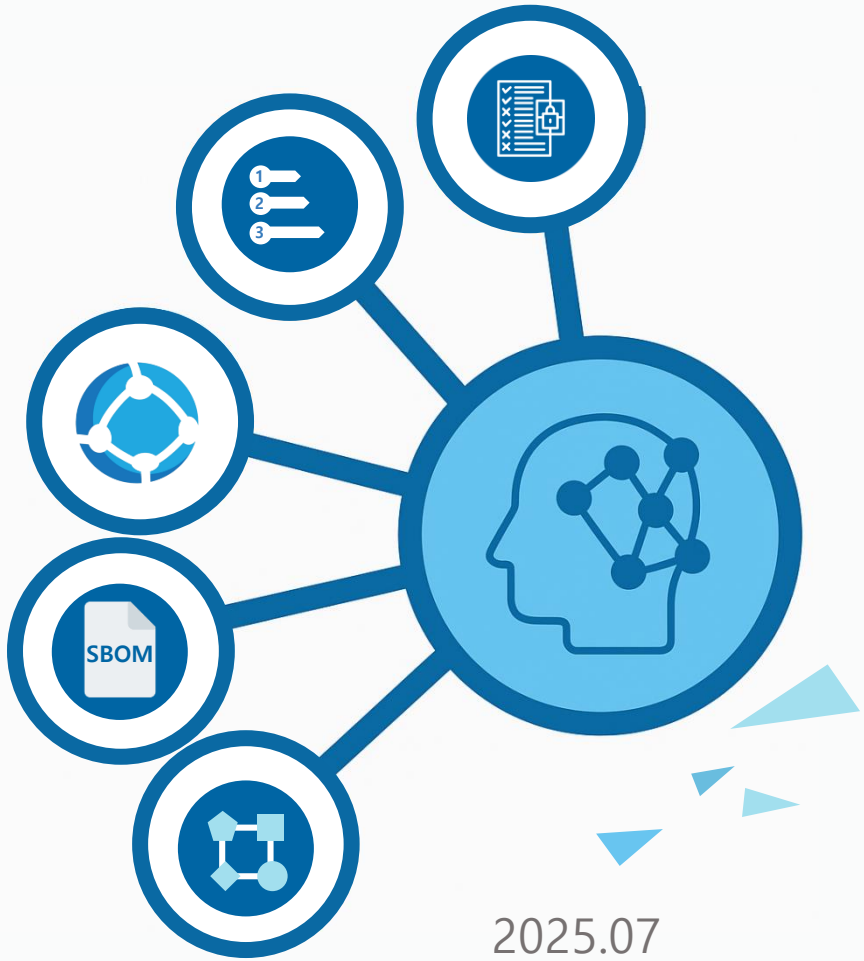


RedPenSoft

AI Agent를 응용한 오픈소스 취약점 관리 방안

XSCAN

2025.07

RedPenSoft

CONTENTS

AI Agent for Software Supply Chain Security

RedPenSoft

AI Agent를 응용한 오픈소스 취약점 관리 방안

Chapter I - 오픈소스 관리하기

통계로 확인하는 오픈소스 이슈

RedPenSoft

95%

전 세계 기업의 95%가 오픈소스 SW를 사용하고 있음

개발자의 90% 이상이 SW개발시 오픈소스 구성요소에 의존

오픈소스 프로젝트가 폐쇄형보다 코드 품질이 30% 높은 것으로 평가

World Metrics.org
2024 OSS Statistic Report

60%

10,000개 기업 대상 분석된 OSS 라이브러의 60%가 심각한 보안 취약점 내포

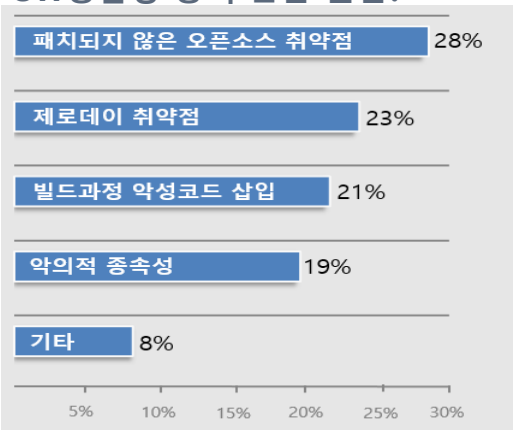
조직의 35%가 OSS 구성요소의 업데이트를 1년 이상 지연

OpenSSF
OPEN SOURCE SECURITY FOUNDATION
HARVARD UNIVERSITY

Census III of Free and Open Source Software, 2024/12

28%

SW공급망 공격 근본 원인?



Ponemon INSTITUTE
The State of Software Supply ChainSecurity Risks. 2024/05

여러분은 오픈소스의 취약점 위협으로부터 안전하다고 확신하십니까?

오픈소스 취약점 분포

RedPenSoft

미국 국립표준기술연구소 국가 취약점 데이터 베이스
National Vulnerability Database

- 2024년 약 4만 건, 누적 총 298,000건 이상의 CVE
- 이 중 상당수가 오픈소스 소프트웨어와 관련됨

Critical	13.7%	Medium	55%
High	33.5%	Low	4.3%

2025년 상반기 레드펜소프트 POC
32개 SW 기준

- 총 3, 369개 오픈소스 CVE 탐지
- 1개 SW 평균 105개 CVE, 그 중 10개 Critical

Critical	10.5%	Medium	50.8%
High	35.3%	Low	3.1%

여러분 기업은 어떤 오픈소스를 어느만큼 가지고 있나요?

현실에서 부딪히는 이슈

- [x] 대체 어디서부터 손을 대야 하나?
- [x] Critical CVE를 모두 제거해야 하나?
- [x] 어떤 버전으로 교체해야 하나?

놓치고 있는 이슈 : EOL

RedPenSoft

대표적인 EOL 사례

OpenSSL 1.0.2 : 2019년 12월 31일 EOL

수 많은 시스템(특히 IoT기기)에서 여전히 해당 버전사용
기업은 사용버전을 점검하고 반드시 업그레이드 필요

왜 소홀히 다뤄지는가?

보안 보다는 운영 관점의 문제로 인식

기능이 종료된다는 운영의 문제로만 인식, 그러나 더
이상 패치를 지원하지 않기에 심각한 보안 리스크 유발

EOL 소프트웨어 관리의 중요성

공격자의 주요 타겟 및 라이선스 이슈

신규 취약점에 영구히 노출되며,컴플라언스 위반
가능성도 존재함. FDA SBOM 제출시 관리 방안 필수

EOL 상태의 자동 감지 체계

개발팀만의 문제가 아닌 조직 정책으로

전문 도구를 통해 OSS의 공식지원 여부, 보안 패
치 지원여부에 대한 지속 점검 및 관리체계 필요

RedPenSoft

AI Agent를 이용한 오픈소스 취약점 관리 방안

Chapter II – 혼돈에서 벗어나기

새로운 접근 : KEV

RedPenSoft

What?

Known Exploited Vulnerabilities

- 알려진 악용된 취약점
- CVSS 기준 대응이 실제 위협과 연결성이 약하다는 한계 탈피
- 현재 실제로 야생에서 악용되고 있음이 증명된 취약점(CVE)
- 전 세계 기업의 60%가 일주일에 평균 1개의 KEV를 가짐[Bitsight Report, 2024]
- 일반적으로 공식 패치가 있어야 등록 가능

Who?

- 미국 국토안보부(DHS)의 CISA가 관장, 각종 정보 제공기관과 협력하여 갱신됨
- KEV Catalog List로 유지관리 하며, 주로 해당 취약점이 발견된 제품의 CWE 동시 기재
- 2021년 11월 부터 시작, 2023년 187건, 2024년 185건, 2025년 6월 24일 기준 1,367개
- FDA 의 SBOM 제출시 기재 권고 사항

How?

Must Patch List

- 행정지침 'BOD 22-01' (Reducing the Significant Risk of KEVs)
- 미국 연방 정부 기관은 정해진 기간 내에 취약점에 대한 패치 또는 완화 조치를 취하고 완료를 보고 해야 함
- 일반적으로 2주~3주 Due Date 제시됨
- KEV로 인한 연방 정부 기관의 공격 표면이 79% 감소 효과

새로운 접근 : EPSS

RedPenSoft

What?

Exploit Prediction Scoring System

- 취약점 악용 가능성 예측
- CVE가 30일 이내 악용될 확률을 예측하는 확률 기반 점수 시스템(0.0001~1)
- Technical Data, Intelligence, Metadata&Disclosure Context, Software Context 등 약 1,400개 이상의 속성을 바탕으로 학습된 기반 모델
- KEV가 현재 위협이라면, EPSS는 미래 위협에 집중

Who?

FIRST

- Forum of Incident Response and Security Team(국제 사이버 보안 사고 대응 조직)
- 보안 대응조직간의 글로벌 협업을 촉진하고, 정보 공유 및 CVSS 등 공통 표준 개발을 주도
- 조직의 보안 우선 대응 순위를 효율적으로 지원하고자 머신러닝 기반 스코어링 시스템 개발(2019년 최초, 2023년 v3)

Why?

Prioritization

- CVSS만 보면 모두 위험한 것처럼 보임 : 실제 악용 가능성은 낮은 경우 많음
- SIEM, SOAR등과 연동하여 자동 필터링·분류·우선순위 부여 활용
- 리스크 기반 보안 대응 전략
- KEV와 병행 활용을 추천
  - KEV : 즉시 대응
  - EPSS ≥0.7 : 선제적 대응 검토

취약점 관리를 위한 필수 : VEX

RedPenSoft

What?

Vulnerability Exploitabilty eXchange

- 특정 취약점이 악용 가능한지 여부를 명시하는 기계판독 가능한 표준 문서 형식(NTIA 제안)
- CVE가 있다고 무조건 위험한 것이 아니다(Justification) 는 사실을 공식적으로 전달하는 목적
- Affeted, Not Affected, Fixed, Under Investigation 4가지 상태
- 불필요한 패치를 최소화 하기 위한 조치

When?

- SW개발사 : 제품에 영향을 주지 않는 취약점을 VEX로 공식 입장
- SW 도입·운영사 : 특정 SW의 취약점(특히 KEV, HEV)에 대해 SW개발사에 VEX 요청
- 기업내부 보안팀의 요청으로 개발자(팀)가 발행할 수도 있음
- 점차적으로 고객사의 요청으로 인한 SW 개발사의 VEX 발행이 일반화될 것으로 예측

How?

Justification

- eXchange (상호 의견 교환)을 하기 위해서 이해관계자들이 참여할 수 있는 플랫폼이 필요
- 'Not Affected'의 상태를 NTIA표준에서는 5가지 정당한 사유(Justification)으로 제시, 그외 CycloneDX VEX, CSAF 등 표준
- SBOM과 VEX는 독립적으로도 존재 가능하나 함께 활용하는 것을 권장함

그래도 부족한 것

새로운 접근

- XSCAN에 KEV,HEV 맵핑 완료
- XSCAN에 VEX 구현(25,Q3예정)

그래도 부족한 것

- 기업별 SW자산의 실제 악용 가능성
- 접근성, 방어체계 등 리스크 평가

AI Agent 연계

- 맥락(Context)기반 취약점 관리
- 노이즈 필터링, 대응방안 가이드

혼돈에서 벗어나기

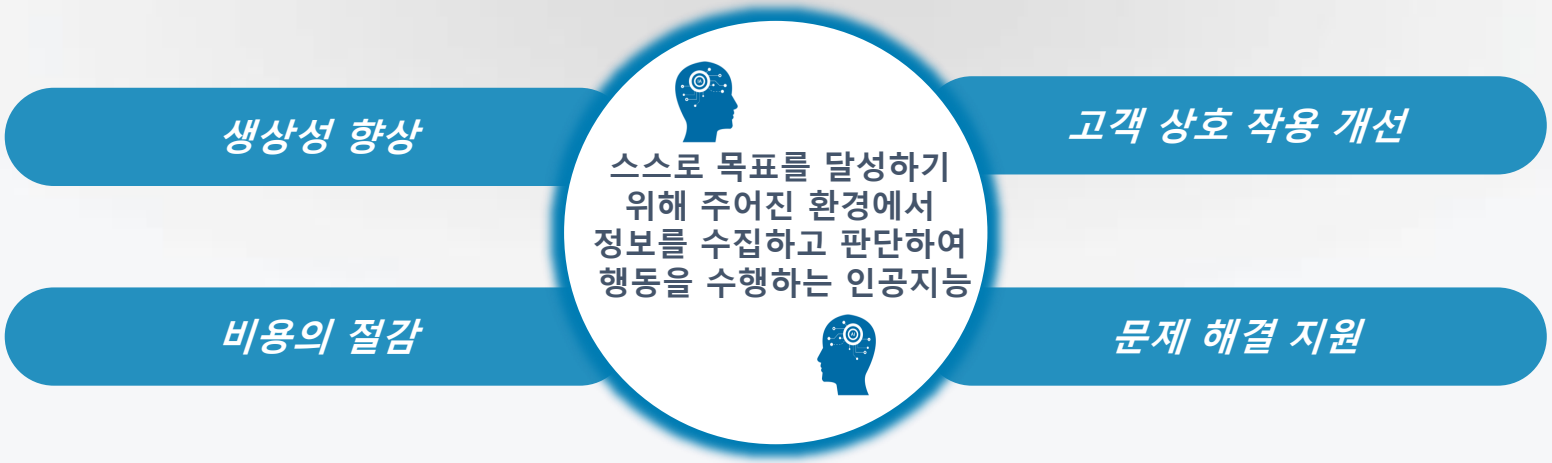
- 차세대 오픈소스 취약점 관리 도구
- SW공급망 보안 관리 전 영역 확대

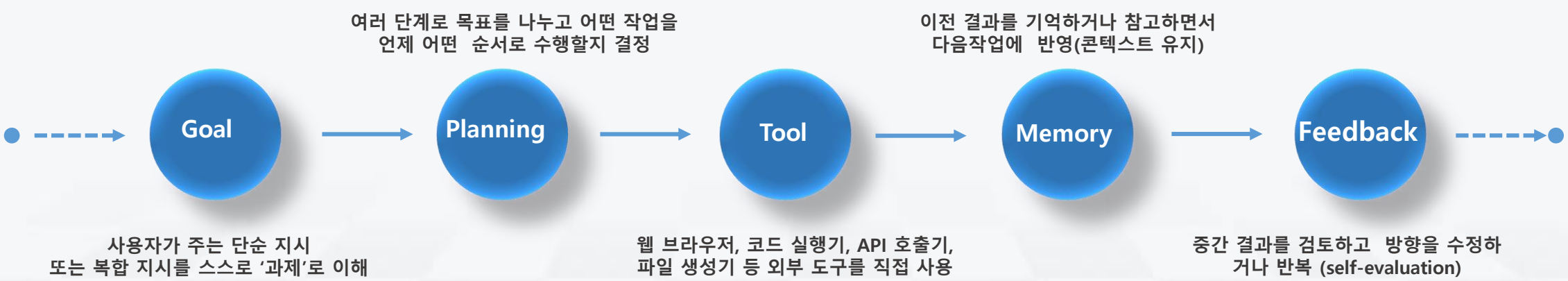
RedPenSoft

AI Agent를 이용한 오픈소스 취약점 관리 방안

Chapter III – AI Agent 응용하기

AI Agent?


생상성 향상
고객 상호 작용 개선
스스로 목표를 달성하기 위해 주어진 환경에서 정보를 수집하고 판단하여 행동을 수행하는 인공지능
비용의 절감
문제 해결 지원


여러 단계로 목표를 나누고 어떤 작업을 언제 어떤 순서로 수행할지 결정
이전 결과를 기억하거나 참고하면서 다음작업에 반영(콘텍스트 유지)
Goal
Planning
Tool
Memory
Feedback
사용자가 주는 단순 지시 또는 복합 지시를 스스로 '과제'로 이해
웹 브라우저, 코드 실행기, API 호출기, 파일 생성기 등 외부 도구를 직접 사용
중간 결과를 검토하고 방향을 수정하거나 반복 (self-evaluation)

SW공급망 보안에 AI Agent 응용하기

RedPenSoft

기존 SW공급망
보안 도구의 한계점

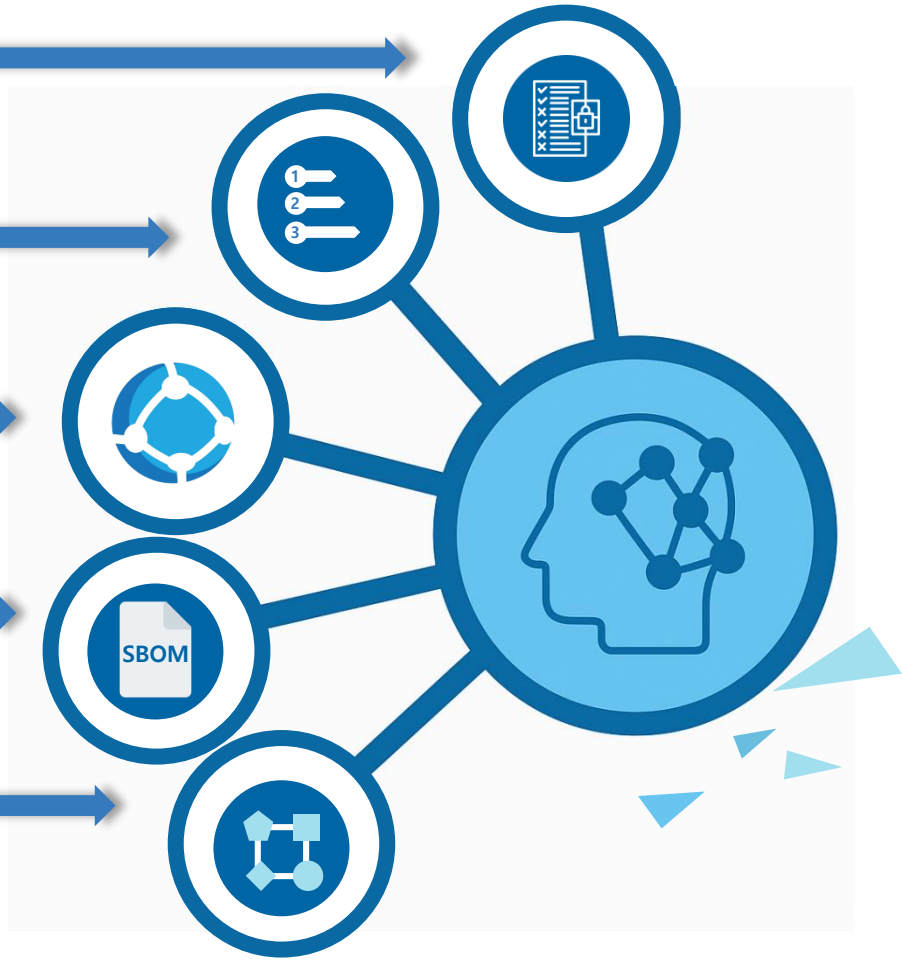
오픈소스 취약점 대응 및 가이드 제공

SW공급망 보안 대응의 우선순위 지정

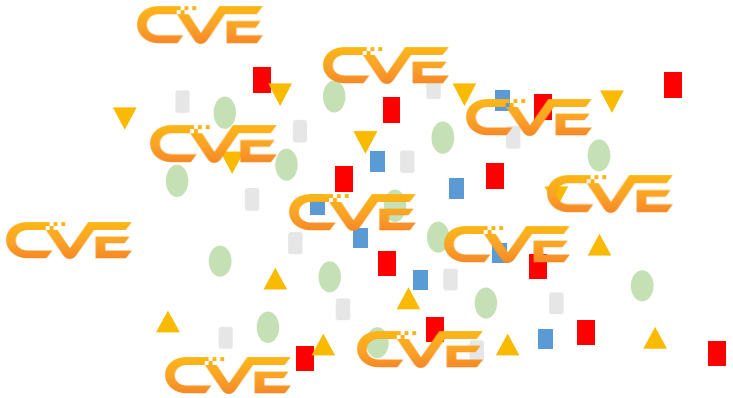
이해관계자와의 자동화 커뮤니케이션

SBOM 비교분석 등 관리 자동화

문제해결을 위한 워크플로우 지원



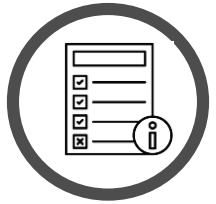
오픈소스 분석 : AI Agent 활용 Flow



최우선 조치가 필요한 고위험 라이브러리

해당 라이브러리에 대한 상세 분석

업그레이드 방법론에 대한 단계별 가이드



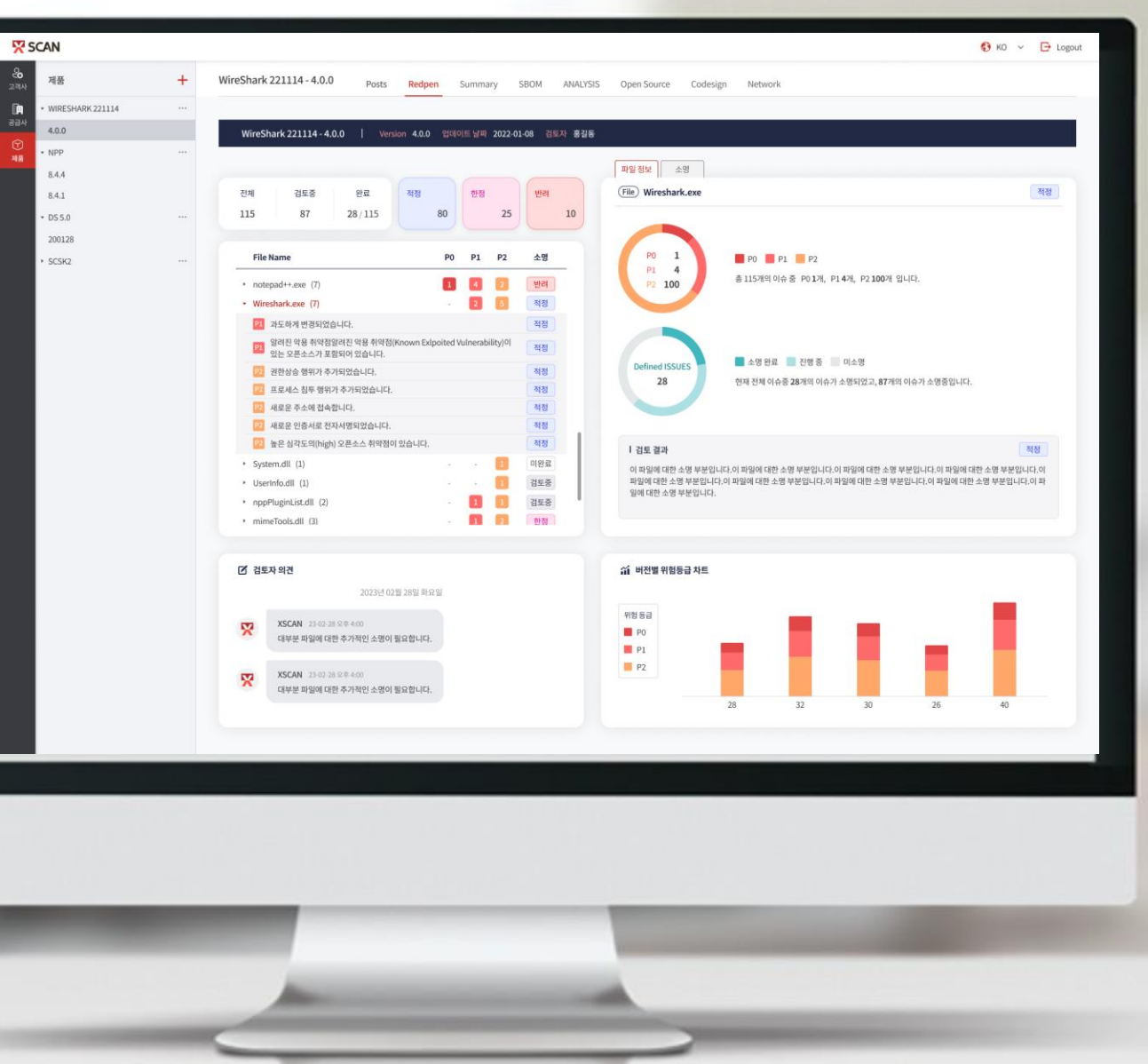
RedPenSoft

AI Agent를 이용한 오픈소스 취약점 관리 방안

Chapter IV –엑스스캔으로 관리하기 XSCAN

엑스스캔

RedPenSoft



- 오픈소스 취약점 등 SW공급망 보안
- SW 구성 컴포넌트에 대한 SBOM
- AI Agent에 기반한 맥락 기반 대응

모든 파일 포맷 지원

RedPenSoft

모든 코드, 모든 포맷, 모든 플랫폼을 위한 SBOM 생성 지원

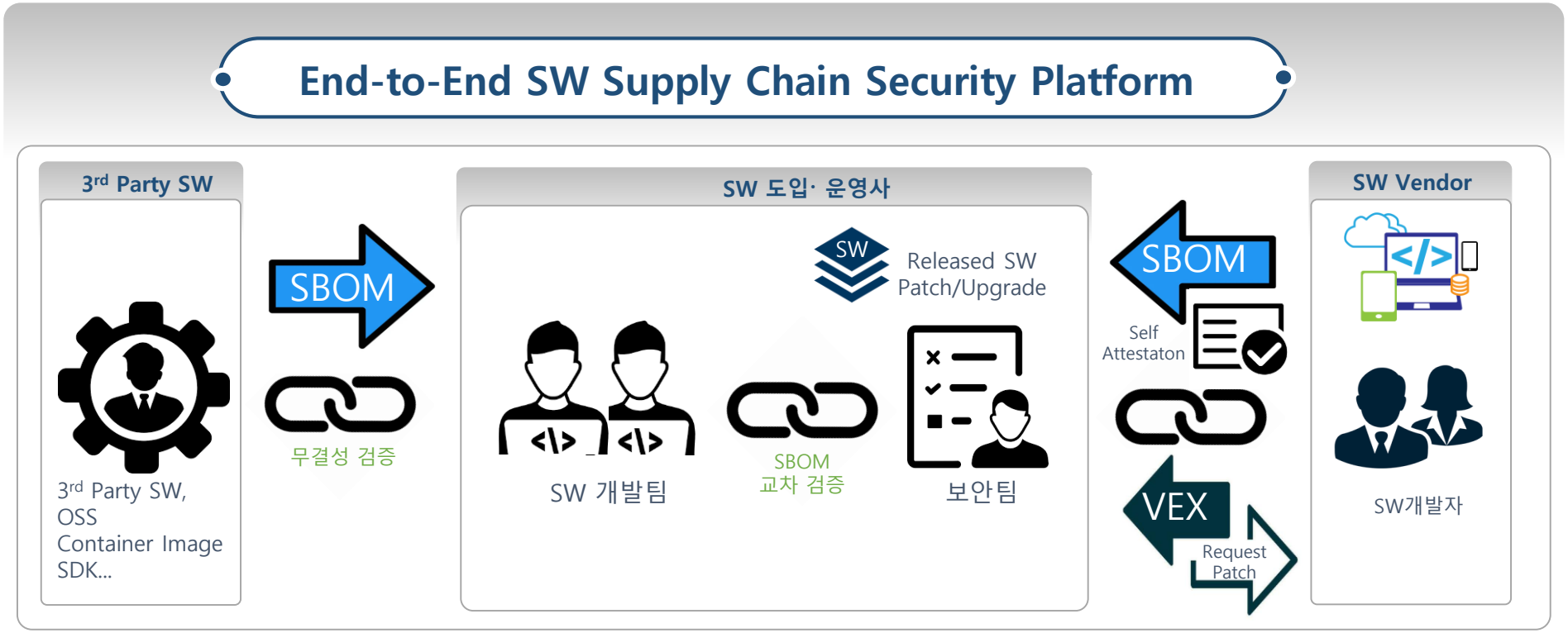
Programming Laguages	File Systems	Binary Formats	Firmware Formats	Installation Formats	Compressin/ Archive Formats
C C++ C# Go Java JavaScript TypeScript Kotlin Python Ruby PHP Rust R Dart	Docker Android Sparse Cramfs Ext2/3/4 ISO JFFS2 Minix RomFS Squashfs UBIFS Yaffs2 WIM	Native binaries (ELF, PE, Mach-O) Java binaryies (APK, Java class, dex/odex, aar, jar, war) Linux kernel Base64 bFLT ipa	Intel Hex SREC uboot RedBoot Aris firmware Juniper firmware Kosmos firmware QNX firmware VxWorks firmware	MSI Deb RPM InstallShield InnoSetup	7z Ar Arj bzip2 cab cpio gzip lrzip lzip lzma lzop rar rzip tar upx xar xz z zip lz4 zst




End-to-End 공급망 보안 플랫폼

RedPenSoft

SW개발·도입· 운영 과정의 모든 이해 관계자 참여 가능한 플랫폼



오픈소스 분석 : 3 Level Drill Down

RedPenSoft

SW구성 요소에 활용된 오픈소스의 취약점과 라이선스 이슈 등을 분석

변경 내용 | 전체 내용 | CVE 검색 AI

Used Open Source	SECURITY RISK	LICENSE	Known Exploited Vulnerability	Highly Exploitable Vulnerability	LITIGATOR
64	80	27	1	1	1
	Critical 8, High 34, Medium 35, Low 3	Protective 13, Permissive 5, Other 9			

CVSS 기준 취약점 | 라이선스 이슈 | 법적분쟁 가능성

파일 리스트 | 위험도 리스트

파일 리스트(113)

Scanned File	Count	Component	Version
LCTUtilities.dll	2	-	-
		openssl	1.1.1b
		zlib	1.2.13
libcrypto-1_1-x64.dll	1	-	-
libssl-1_1-x64.dll	1	-	-
libcrypto-1_1-x64.dll	1	-	-
libssl-1_1-x64.dll	1	-	-
Planetkit64.dll	1	-	-
DuiLib_u_x64.dll	2	-	-
ElsaContentKit.dll	3	-	-
zlib1.dll	1	-	-

CLICK

AI 분석

CVE-2022-2068은 OpenSSL의 c_rehash 스크립트에서 발생하는 취약점으로, 이 스크립트가 쉘 메타문자를 적절히 처리하지 않아 명령어 주입이 가능하게 되는 문제입니다. 이로 인해 공격자는 스크립트의 권한으로 임의의 명령어를 실행할 수 있습니다. 이 취약점은 OpenSSL 3.0.0부터 3.0.3, 1.1.1부터 1.1.1o, 1.0.2부터 1.0.2ze 버전에 영향을 미치며, OpenSSL 3.0.4, 1.1.1p, 1.0.2zf에서 수정되었습니다.

다음은 이 취약점으로 인해 발생할 수 있는 위협과 대응책을 요약한 표입니다.

위협 요약

위협 요소	설명
기밀성 손상	공격자가 민감한 데이터를 탈취할 수 있음
무결성 손상	공격자가 시스템 파일이나 데이터를 변조할 수 있음
가용성 손상	공격자가 시스템을 중단시키거나 서비스 거부 상태로 만들 수 있음

대응책 및 요청 사항

대응책	설명
소프트웨어 업데이트	OpenSSL을 최신 버전(3.0.4, 1.1.1p, 1.0.2zf)으로 업데이트
c_rehash 스크립트 사용 중지	c_rehash 스크립트 대신 OpenSSL rehash 명령어 사용
시스템 모니터링 강화	비정상적인 명령 실행을 탐지하기 위한 로그 모니터링 및 경고 시스템 설정

공급업체 요청 사항	설명
패치 제공	취약점이 수정된 패치를 신속히 제공
보안 공지	취약점에 대한 상세 정보와 대응 방법을 포함한 보안 공지 발행
고객 지원	취약점 대응에 대한 고객 지원 및 가이드 제공

이와 같은 조치를 통해 CVE-2022-2068 취약점으로 인한 위협을 최소화할 수 있습니다. 고객은 소프트웨어를 최신 버전으로 유지하고, 공급업체의 보안 공지를 주기적으로 확인하여 시스템을 안전하게 보호해야 합니다.

오픈소스 분석 : KEV, HEV 맵핑

RedPenSoft

> 반드시, 그리고 긴급히 대응해야 하는 오픈소스 취약점 맵핑

CVSS = Start point

CISA Known Exploited Vulnerabilities Catalog

KEV

Must Patch List

EPSS

HEV

Highly Exploitable Vulnerability

인터넷뱅킹 필수설치 SW의 KEV, EPSS 맵핑 예제

오픈소스 분석 : AI Agent 활용 예시

RedPenSoft

취약점 분포

400
전체 취약점

- Critical: 36
- High: 164
- Medium: 192
- Low: 8

고위험 취약점

Critical 취약점	36개
High 취약점	164개
조치 가능한 취약점	337개

최우선 조치 필요

thunderbird 91.13.0 → 128.8.0-1.fc42
313개 취약점 해결

즉시 조치 방법 보기 >

thunderbird

현재: 91.13.0 | 권장: 128.8.0-1.fc42 | 순위 #1

AI 심층 분석 결과

AI 권장: 업그레이드 | 83% 취약점 감소 가능 | 예상 작업: 3 시간

권장 근거: 현재 사용 중인 Thunderbird 91.13.0 버전은 지원이 종료(EOL)되었으며, 313개의 취약점(22개는 심각)을 포함하여 매우 높은 위험 점수를 가지고 있습니다. 권장 버전인 128.8.0-1.fc42는 현재 활성 ESR 버전으로, 업그레이드 시 위험 점수가 크게 감소하며 지속적인 보안 지원을 받을 수 있습니다. 보안 위험을 최소화하고 안정적인 사용을 위해 즉시 권장 버전으로 업그레이드하는 것이 강력히 권장됩니다.

버전 비교 | 마이그레이션 | 대안 라이브러리

패치 적용 시 개선 효과

83%	86%	64%
전체 취약점 감소율	Critical 감소율	소프트웨어 위험도 기여도

라이브러리 정보

이름	thunderbird
설명	무료 오픈소스 이메일 클라이언트, 개인 정보 관리자 (캘린더, 주소록), RSS 피드 리더, 채팅 클라이언트, 뉴스 클라이언트.
현재 버전	91.13.0
권장 버전	128.8.0-1.fc42
위험도 순위	#1
카테고리	tool
메인테이너	MZLA Technologies Corporation (Mozilla Foundation 자회사)
라이선스	Mozilla Public License 2.0

현재 버전: 91.13.0

100%
위험도

수명 주기 정보

EOL 상태	EOL까지 남은 일수
종료	1일 전 EOL

취약점 분포

Critical:	22	High:	131
Medium:	157	Low:	3

총 취약점: 313개

권장 버전: 128.8.0-1.fc42

65%
위험도

수명 주기 정보

EOL 상태	EOL까지 남은 일수
활성 (ESR)	정보 없음

취약점 분포

Critical:	3	High:	22
Medium:	28	Low:	0

총 취약점: 53개

관련 자료 | 공식 문서 | 보안 권고 | 개발 도구 | 커뮤니티

- Thunderbird 공식 웹사이트
- Thunderbird 128.0 Release Notes
- Mozilla Security Advisories for Thunderbird
- Mozilla Public License Version 2.0 (MPL-2.0)

버전 비교 | 마이그레이션 | 대안 라이브러리

예상 작업 시간
3 시간

필요 기술
소프트웨어 설치 및 제거, 파일 시스템 탐색, 기본적인 문제 해결 능력

마이그레이션 복잡도
보통

마이그레이션 단계

1. **현재 프로필 백업**
   Thunderbird를 종료하고 프로필 디렉토리를 안전한 위치에 백업합니다. 이는 마이그레이션 실패 시 데이터를 복구하는 데 필수적입니다.
   예상 시간: 0.5 시간
2. **권장 버전 다운로드 및 설치**
   Thunderbird 공식 웹사이트 또는 신뢰할 수 있는 배포 채널에서 권장 버전(128.x ESR) 설치 파일을 다운로드하여 설치합니다. 기존 버전에 덮어쓰거나 별도의 위치에 설치할 수 있습니다.
   예상 시간: 0.5 시간
3. **프로필 마이그레이션 확인**
   새 버전의 Thunderbird를 실행하여 기존 프로필 데이터(계정 설정, 메일, 주소록 등)가 올바르게 마이그레이션되었는지 확인합니다. 대부분 자동 진행됩니다.
   예상 시간: 0.2 시간
4. **확장 기능 호환성 확인 및 업데이트**
   설치된 확장 기능(Add-ons)이 새 버전과 호환되는지 확인하고, 필요한 경우 업데이트하거나 대체 확장 기능을 찾습니다. 일부 확장 기능은 더 이상 지원되지 않거나 내장 기능으로 대체되었을 수 있습니다.
   예상 시간: 1 시간
5. **기능 및 설정 검토**
   새 버전의 변경된 UI 및 설정을 검토하고 필요에 따라 조정합니다. 주요 버전 업그레이드 시 사용자 인터페이스에 변화가 있을 수 있습니다.
   예상 시간: 0.5 시간

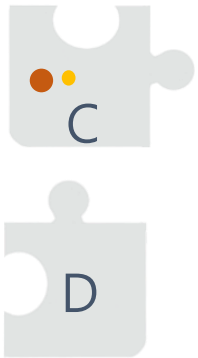
엑스스캔 차별점 : 변화도 비교 추적

RedPenSoft

"이전 버전 대비 변화도를 AI 기반으로 추적하여 컴포넌트 레벨의 의심 및 위협 요인 판별

Version 1

"과거 버전은 A, B,C 의 컴포넌트로 구성되어 있으며 어떠한 의심 및 위협 행위도 없었다 "



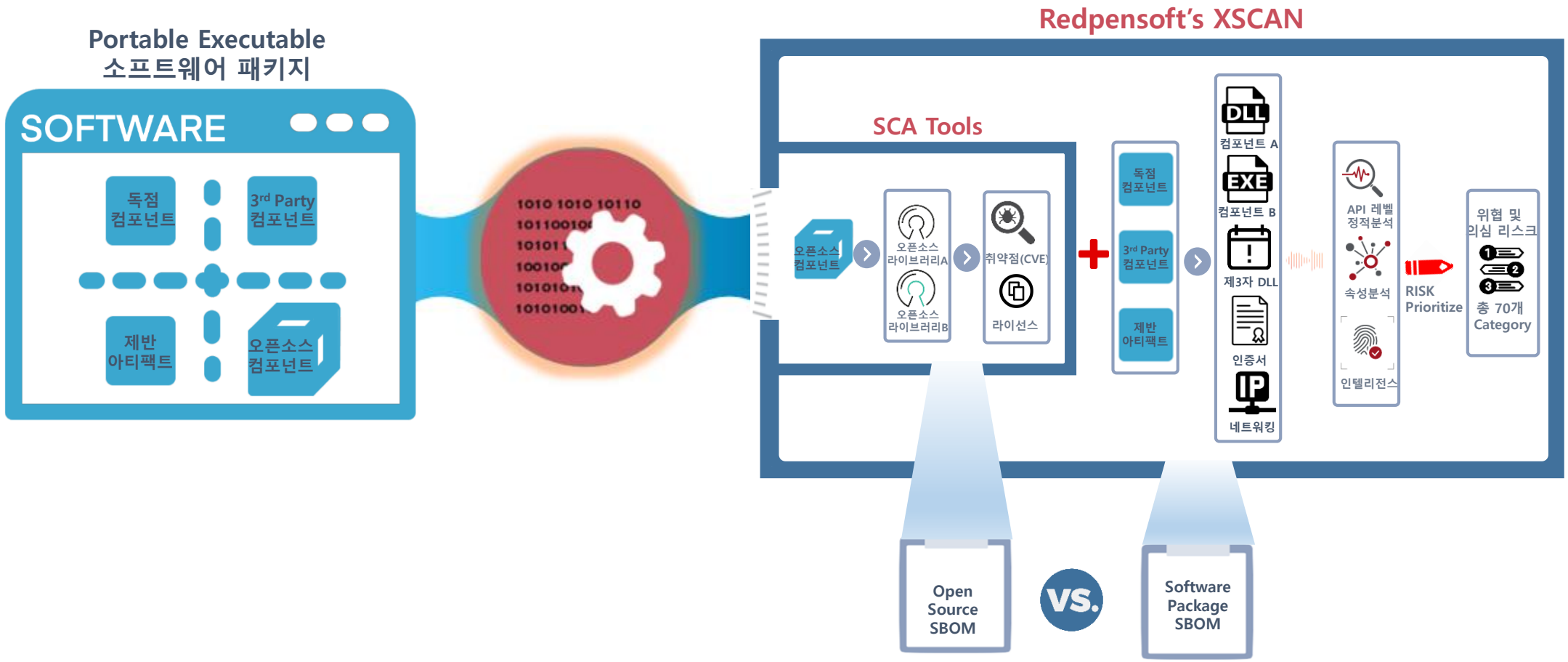
Version 2

"기능과 보안 강화 목적의 D컴포넌트가 새로 추가되었고, C컴포넌트에도 일부 변화가 생겼다"

엑스스캔 차별점 : PE파일 특화분석

RedPenSoft

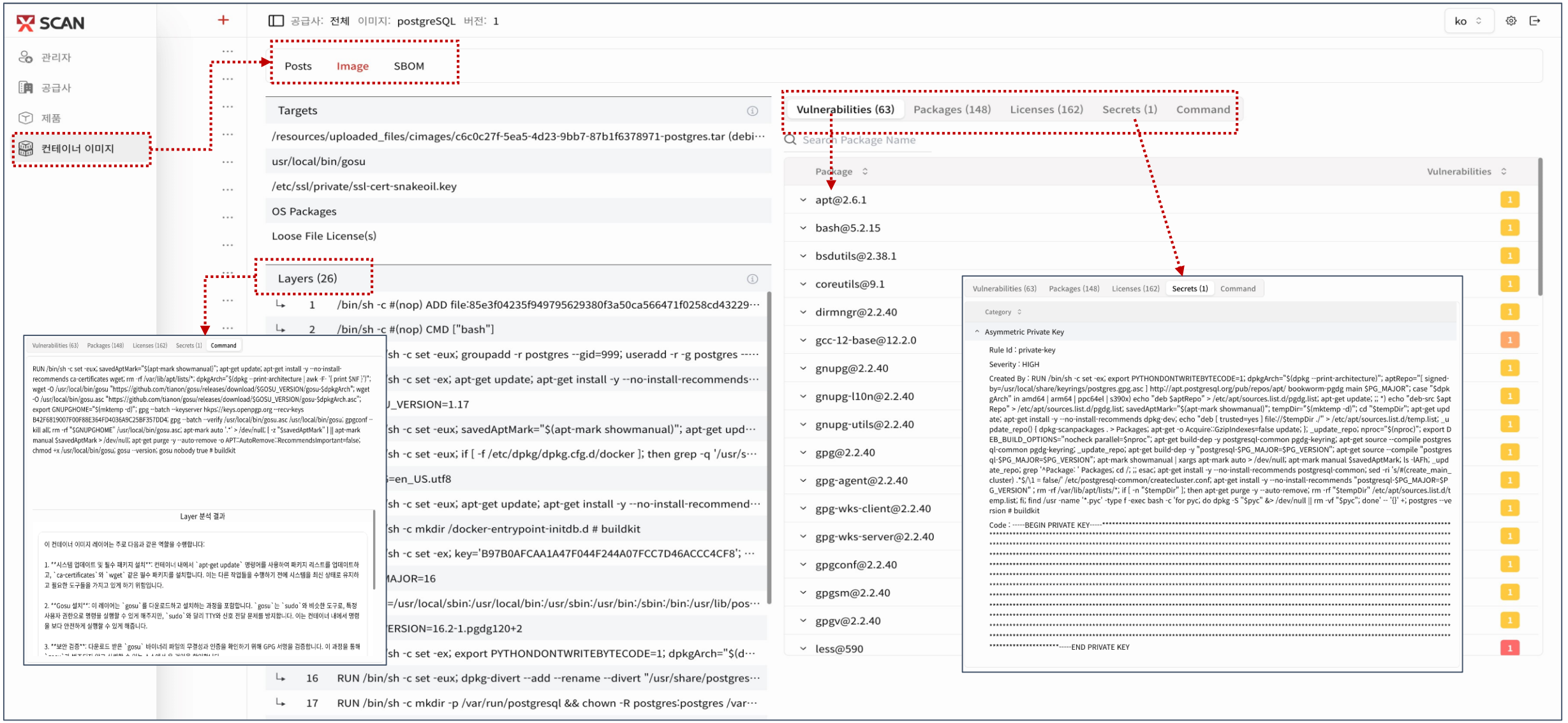
❝단말 SW는 공격자들이 가장 선호하는 타겟, 도입·운영되는 모든 PE파일 완벽 분해



엑스스캔 차별점 : 컨테이너 이미지 분석

RedPenSoft

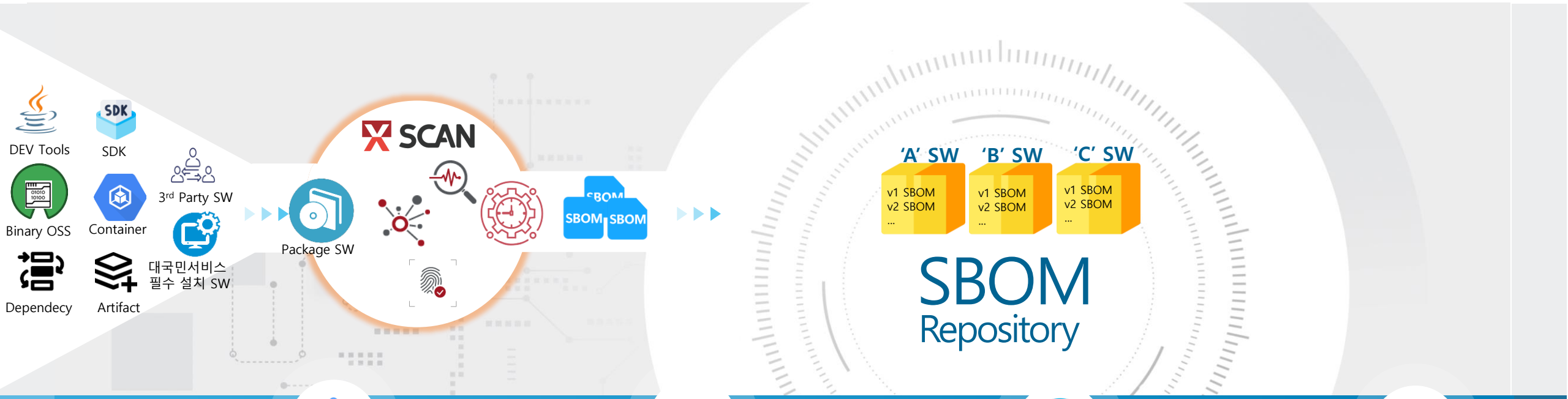
컨테이너 이미지의 레이어, 취약점과 숨겨진 비밀(Secret)을 제시



엑스스캔 도입효과

RedPenSoft

보안 관점의 오픈소스 취약점 대응 및 SW별 SBOM 리포지토리 구축



01 SW 개발 과정 리스크 관리

- SW 개발시 활용되는 모든 오픈소스 컴포넌트 검증
- 특히 SaaS 기반 등 서비스를 위한 컨테이너 이미지 및 3rd Party SW
- 개발자(팀)이 놓칠 수 있는 제반 아티팩트 등에 대해 교차 검증

02 도입 및 운영 리스크관리

- 반입 SW 내 오픈소스 취약점 및 License 이슈 관리 자동화
- 공급사 벤더와의 커뮤니케이션 및 취약점 조치 이력 DB화
- 제2의 로그포제이 발생시 빠른 대처

03 SW 투명성 및 신뢰성 확보

- 기존 버전 기준 SW 관리를 SW 컴포넌트 단위로 리포지토리화
- 납품 ·운영 과정에서 고객사에서 SBOM 요구시 신뢰성 있는 조치
- 취약점 및 리스크 대응 순위에 대한 상호 커뮤니케이션

04 보안 사고 시 증적 제공

- 특정 구성요소가 있는 모든 SW 확인하여 사고 영향 범위 분석
- 구성요소의 출처와 변경 내용에 대한 추적으로 유사 문제 예방
- 사고 발생시 규제 당국이나 고객에 증적 자료 제출

XSCAN POC Proposal

- 오픈소스 취약점! 잘 관리하고 계십니까?
- SW공급망 공격! 안전하다고 자신할 수 있습니까?
- 새로운 서비스! 구축 혹은 도입을 준비하십니까?

01 기업의 인프라에 아무것도
설치되는 것이 없습니다.

02 대상 SW를 업로드 후
리포트를 보시면 됩니다.

03 POC에 소요되는 시간은
딱 하루면 됩니다.

지금 바로 XSCAN POC 서비스를 신청하세요

Your Voice Matters!

ikchan@redpensoft.com

RedPenSoft

Make Trusted Software Value Chain