May.2024

SW공급망보안 가이드라인 1.0 해설

RedPenSoft

가이드라인 요약

집필참여

- 국가정보원, 과학기술정통부, 디지털플랫폼 정부 위원회
- 한국인터넷진흥원, 국내 정보보호 학계, SW공급망보안 포럼 등

발표취지

- SW 공급망에 침투하여 악성코드 삽입 등 SW 공급망 공격에 대한 우려 고조
- 기업의 의사 결정자 및 실무자들이 SW 공급망 보안 개념 쉽게 이해하고 활용 지원

핵심내용

- SW 공급망 위기 대응의 필요성, SW 공급망 위험 관리 방안
- 국내 SBOM 보안 실증 사업, 국가적 차원의 SW 공급망 보안 활성화 지원

기대효과

- 북한 등 고도화된 해킹 조직에 의한 기업의 SW 공급망 위협 완화
- SW 전체 라이프 사이클에서 SBOM 중심의 보안 관리체계 확산

핵심 내용

1장. 추진배경

- 초연결 사회가 도래되면서 SW 공급의 분업화로 책임이 복잡해지고, 제품 및 서비스 무결성에 대한 신뢰 하락
- 공급망 공격은 보안 취약점 및 악성코드를 악용한 것, 피해 광범위하고 지속적 특징
- 미국, 유럽 등은 SW 공급망 공격에 체계적으로 대응하기 위해 SBOM 도입 등 제도화
- 우리나라도 SW공급망 공격 대응 및 효과적인 보안 취약점 관리 방안으로 SBOM 기반 SW 공급망 보안 체계 마련이 필요함

2장. SW공급망 위험관리 방안

- 공급망 전체에서 사이버보안 위험을 관리하고 적절한 대응 정책 및 전략등을 개발하기 위한 체계적 프로세스(C-SCRM) 대두
- C-SCRM은 개발-구매-운영 및 유지보수 등 'SW 생명주기' 전체 에 결쳐 다양한 이해관계자 그룹이 함께 참여해야 함
- SW 공급망 참여자들은 SBOM을 통해서 보안 취약점, 공개 SW 라이선스 관리 가능
- SBOM은 SW를 개발하거나, 구매할 때 또는 시스템 운영에도 활용할 수 있음

SW 공급망 보안 가이드라인 v1.0

요약본

3장-1. SBOM기반 SW 공급망 보안 강화 방안

- [개발사 보안활동] SW 개발 생명주기 전반 걸친 위험 관리를 위해 SBOM 생성을 위한 필수 설비를 구축/활용→ 공개SW 및 상용 도구 활용하여 NVD 연계
- [공급사 보안활동] 타사 SW의 검증, 실행 파일 테스트를 통해 안전한 SW의 전달 및 신규 취약점 알림을 전파하고 취약점 대응 조치
- [운영사 보안활동] SW 제품의 구매 및 업그레이드시 제품과 구성요소의 무결성 검증, 인수한 제품과 SBOM 비교/ 확인 등 보안 활동 수행
- [SBOM 실증 결과] 소스코드, 바이너리, 의존성을 종합적으로 분석한 SBOM을 관리하여야 하며, 2개 이상의 도구를 이용한 교차 검증이 필요

3장-2. SBOM기반 SW 공급망 보안 강화 방안

- [테스트베드 지원] 중소기업이 효과적으로 이용할 수 있는 SBOM기반 SW 공급망 보안 관리체계 구현 : 디지털헬스 케어 보안 리빙랩(원주), 판교 공급망보안 테스트베드 등
- [NIS-SBOM] 정부/공공기관에 도입되는 SW 공급망 관리 체계를 구축하기 위해 국가정보원에서 NIS-SBOM 제정 : 기본 항목 최소화, 보안취약점 연동, 위험관리 효율화
- [발전 제언] ❶SW 공급망 보안 체계 구축을 위한 적극적 투자 필요 ❷기관 내 IT자산과 SW를 관리하고 보안 취약점을 지속 모니터링 할 수 있는 관리체계 필요 ❸ 안전한 SW 개발 환경 조성 위한 법적, 기술적 프레임워크 필요 ❹ SBOM을 기밀성 보장 및 안전한 공유를 위한 기술 연구 필요

Higlight & More

SW공급망 보안은 국가 사이버안보를 위한 핵심 의제

- SW 공급망 보안을 위해 국가의 사이버보안 관련 기관인 과기부 정통부 및 디지털플랫폼정부위원회가 국내 사이버 보안 가이드라인 관련 최초 공동 집필 참여
- 제로트러스트 가이드라인 1.0(2023. 06) 공표(과기부)와 더불어 사이버보안의 현대화를 위한 보안 정책 관련 현 정부 두번째 가이드라인

"정부·공공기관의 정책결정자 및 기업의 경영진 등이 본 가이드라인을 통해서 SW 공급망 공격에 대한 경각심을 높이고 SW 공급망 보안에 대한 투자를 기획하고 실행하는 계기로 작용할 것"

SBOM기반의 SW공급망 보안위협 대응

- SBOM은 SW 위험 관리를 위한 기초 데이터가 됨
- 개발사 · 공급사 ·운영사 등 SW 생명주기에 있는 모든 주체에게 SBOM 기반의 SW 공급망 보안 활동 필요성 제기
- 특히 SW개발 생명주기에서의 보안 강화의 중요성을 강조
- NIS-SBOM의 제정 및 공표

"정부 디지털 플랫폼 사업 및 국가 핵심 기간망 사업 등의 추진시 SW 무결성 검증을 위한 SBOM의 제시 요청과 활용 적극화 될 것"

"SW Life Cycle, SBOM 사용주체, SW유형 등에 따른 SBOM도구의 선택기준과 활용방안 등이 시장에서 세분화 될 것"

아쉬운 점과 추후 발전방향

- 공개SW(오픈소스 SW)의 취약점 식별과 대응이 SW공급망 보안 강화의 전부인 것처럼 오해의 소지 있음
- 야생에서 발생하는 실제 SW 공금망 공격의 TTPs 연구에 기반하여 추가의 대응 기법 및 기술에 대한 논의가 필요함

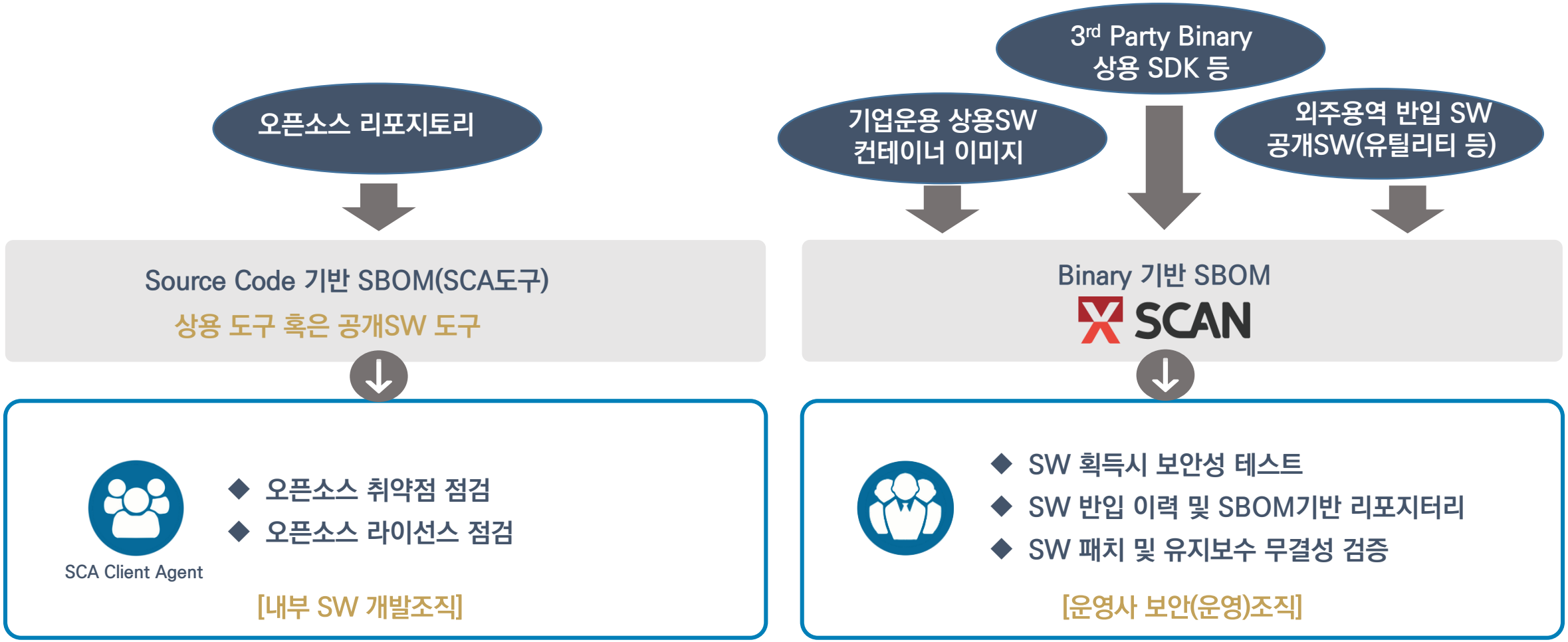
"가이드라인 v1.0 이후 지속적인 성숙 기대"

"SW공급망 보안 강화를 위한 제도화 및 세부적인 정부지원 방안 등이 논의 및 마련 될 것"

SBOM 기준 가이드라인의 준수

운영자(고객사)입장의 SW공급망 보안 가이드라인v1.0을 준수하기

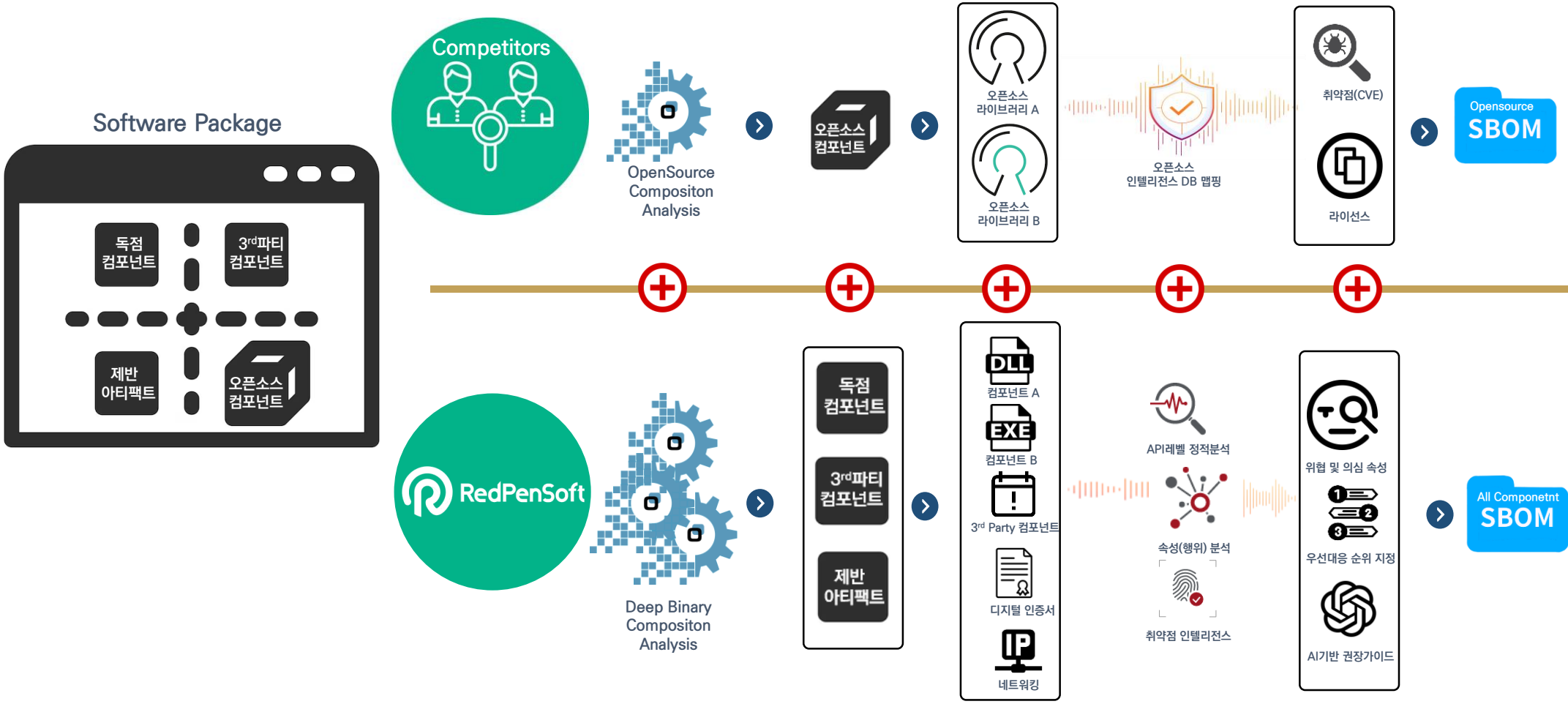
내부 SW개발팀을 가지고 있는 경우와,보안 운영 조직만 보유하고 있는 경우가 다릅니다.



XSCAN 차별점 *01*

공격자의 관점(전술·기술·프로세스)에서 대응방안을 모색했습니다.

오픈소스 분석은 공급망 공격 대응의 일부분일 뿐입니다. 엑스스캔은 소프트웨어를 폭파 수준에 이르까지 완전 분해했습니다.



XSCAN 차별점 *02*

야생의 실제 공격은 특정 컴포넌트의 바꿔치기를 주 공격기법으로 하고 있었습니다

엑스스캔은 이전 버전 대비 변화되는 패치의 형상 관리가 그 해답임을 찾았습니다

XSCAN 차별점 *03*

너무나 많은 오픈소스 취약점이 탐지되어 난감할 수 있습니다

엑스스캔은 우선 해결해야 할 취약점에 집중할 수 있도록 Pinpoint합니다

KEV

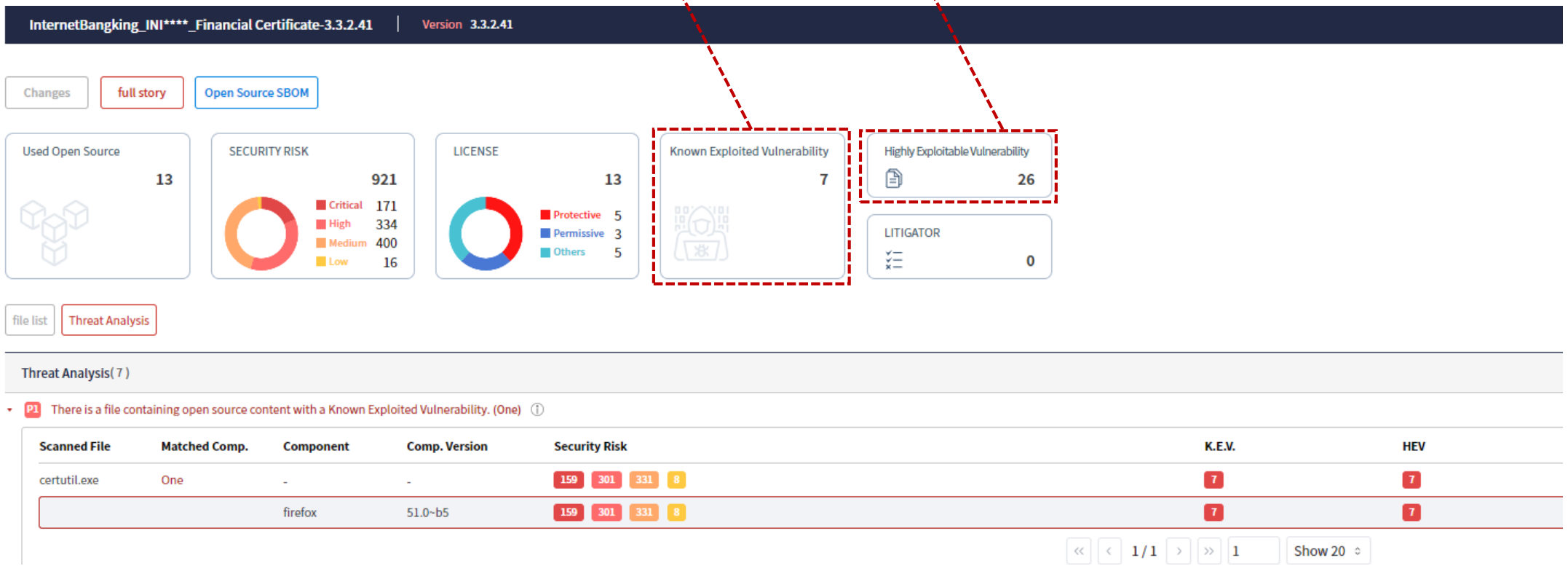
· Known Exploited Vulnerabilty로 미국의 CISA에서 관리하는 Must Patch CVE List

· 이러한 취약점을 가진 SW는 내부로 반입하면 심각한 위협을 초래할 수 있다

HEV

· Higly Exploitable Vulneability로 FIRST(국제사이버사고대응포럼)의 EPSS 맵핑

· 30일 이내 익스플로잇 될 가능성이 70% 이상인 취약점



XSCAN Business Area

모두가 왼쪽(Shift Left)만을 이야기할때...

우리는 오른쪽(Shift Right)을 바라보았습니다.

SW가 침해될 수 있다는 제로트러스트 관점에서, 수요자가 SW의 무결성을 검증해야 합니다.

공급자 관점의 공급망 보안 대응

SAST/DAST/SCA Tools etc

수요자 관점의 공급망 보안 대응

XSCAN

SW벤더의 개발자가▪
오픈소스 분석도구 등을 ▪
개발 단말 및 SaaS환경에서 ▪
SW개발 라이프 사이클시에▪
안전하고 고품질의SW개발을 위해서 ▪
소스코드 기반 자동화된 분석 기법 ▪

5W 1H

▪ 기업의 보안 담당자가
▪ 레드펜소프트의 엑스스캔을
▪ 클라우드 SaaS 환경에서
▪ SW의 획득 및 패치 유지보수시에
▪ SW공급망 공격을 방어하기 위해서
▪ 바이너리 기반 자동화된 분석 기법

Thanks