

X SCAN

SBOM기반 SW 무결성 검증

2024.02

CONTENTS

-  1. 급증하는 SW공급망 공격
-  2. 표준기술로 자리잡은 SBOM
-  3. XSAN 소개
-  4. 도입사례 & FAQ



소프트웨어의 생산 및 전달과정 해커의 악의적인 공격, 제로데이 취약점

Q1

- 파일선 저장소 종속성 혼란 공격
- 노르웨이 선박사 DNV Ship Manager
- 포티넷 FortiOS 제로데이 취약점
- 원격모니터링 AnyDesk
- 파일전송 솔루션 Go Anywhere MTF
- 대용량 파일전송 AsperaFaspex
- 비밀번호 관리 전문 LastPass
- 브라우저 확장 프로그램
- 국내 파일전송 솔루션 취약점
- 국내 공동인증서 전자서명 프로그램

Q2

- 온라인 화상회의 솔루션 3CX
- Mobile App 제3자 SDK(TDI Play)
- 메세징앱 Tencent QQ,
- 화면녹화 앱 iRcoder
- 보안장비 포티가드
- 이메일보안 게이트웨이 Barracuda
- 파일전송솔루션 MOVEit
- 웹메일서버 RoundeCube
- 암호관리 및 SSO솔루션 ADSelfService
- 국내 네트워크접근제어 솔루션

Q3

- 전자메일 Outlook
- 전자행정 서비스 E-Office
- 마이크로소프트 M365
- ID및 Access 관리 Jump Cloud
- 모바일보안 솔루션 EPMM
- NPM 저장소 악성 Package
- 암호호화 솔루션 Cobra DocGuard,
- GUI설계솔루션 QT,
- 파일보관 솔루션 WinRaR,
- IT인프라 관리 Zoho Manage Engine,
- Rust 저장소 Creats 타이포스쿼팅 공격

Q4

- 위키소프트웨어 Atlassian Confluence
- CI/CD 파이프라인 TeamCity
- ID 및 Access 관리 Okta
- 협업관리소프트웨어Zimbra
- 국내 공동인증서 프로그램
- ITSM전문 솔루션 SysAid
- 방화벽 Zyxel
- 멀티미디어 솔루션 Cyberlink

WHO?

금융 및 스파이 활동 목적의
국가 후원 해킹그룹이 배후
2023년은 북한과 중국이 주도



HOW?

업데이트 바꿔치기
제로데이 취약점
손상된 인증서 악용
오픈소스 취약점



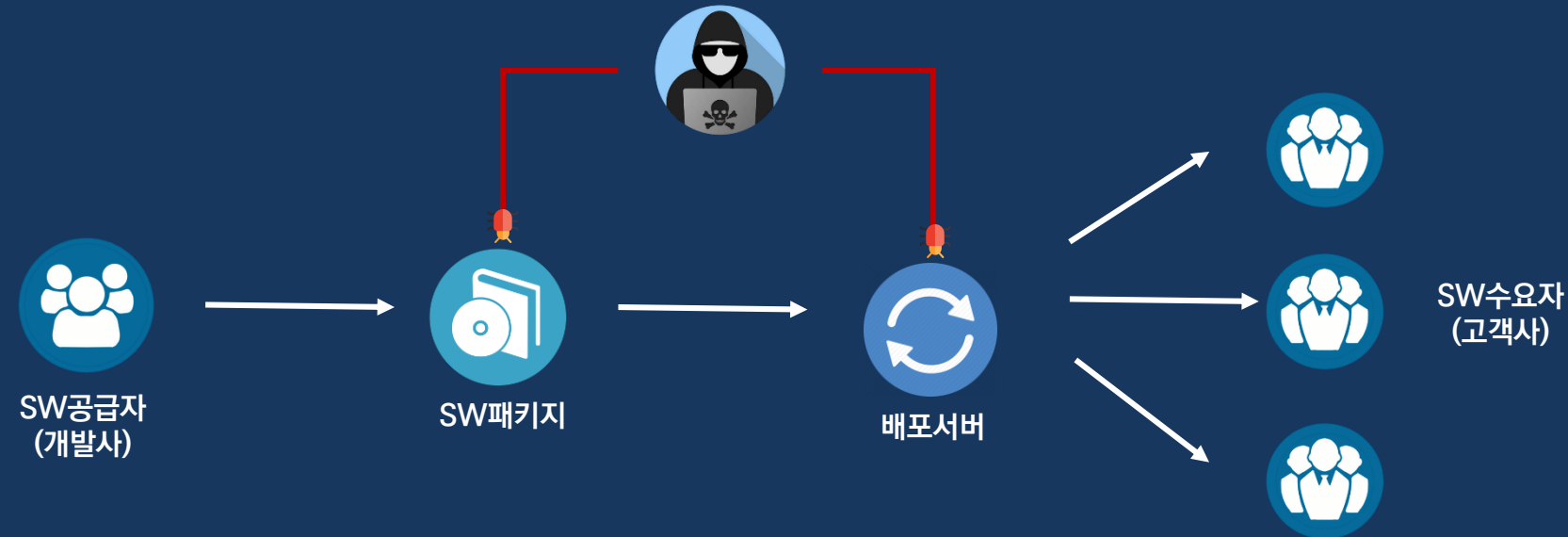
WHAT?

보안전용 단말 SW
파일관리 및 전송 SW
IT인프라 관리 SW





공격자가 소프트웨어 제작 및 업데이트 과정에 침입 정상적인 SW를 가장한 악성SW 설치



특징 1

패치 등 신뢰 기반 경로 활용
공격 경로 완전 차단 불가

특징 2

기존 경계기반 탐지 시스템
완전히 우회하는 공격

특징 3

막대한 사회적 피해와
국가적 혼란 야기



국내 사이버보안 관계 기관 및 다수의 주요 전망에서 모두 2024년 공급망 공격의 위협에 대비해야 한다고 경고하고 있음



「2024 사이버보안 위협 분석과 전망」 2023/12/17

“피해 자체를 모르게 하는 은밀하고 지속적인 SW 공급망 공격”



「2024 디지털금융 및 사이버보안 이슈 전망」 2023/12/17

“SW공급망 공격 성행, SBOM의 중요성이 강조”



「2023 국가 사이버안보 연례보고서」 2024/01/25

“2023년 주요 공격으로 SW 공급사 내부망 해킹을 통한 악성코드 유포”

사이버보안 시장 조사 기관

「The 2023 Software Supply Chain Attack Report」

“SW 공급망 공격으로 인한 전 세계 기업의 연간 비용이 2023년 460억달러 (62조)에 이르며, 2025년 600억 달러(80조)에 이를 것이다”



국내 보안 관제 기업

사이버보안 업계가 선정한 2024년 보안 위협 트렌드 Top 5

“국내 주요 보안 관제기업 4곳이 발표한 공동된 2024년 Top5 사이버위협 이슈 중에서 첫 번째는 국가 지원을 받는 해킹 그룹의 공급망 공격 증가이다”



글로벌 미디어 그룹

Navigating The Cybersecurity Landscape In 2024

“공급망 공격은 계속될 것이며, 기업은 엄격한 공급망 보안 조치를 구현하고 잠재적인 위협을 감지하고 완화하기 위한 사전 예방적 접근 방안을 채택해야 합니다”



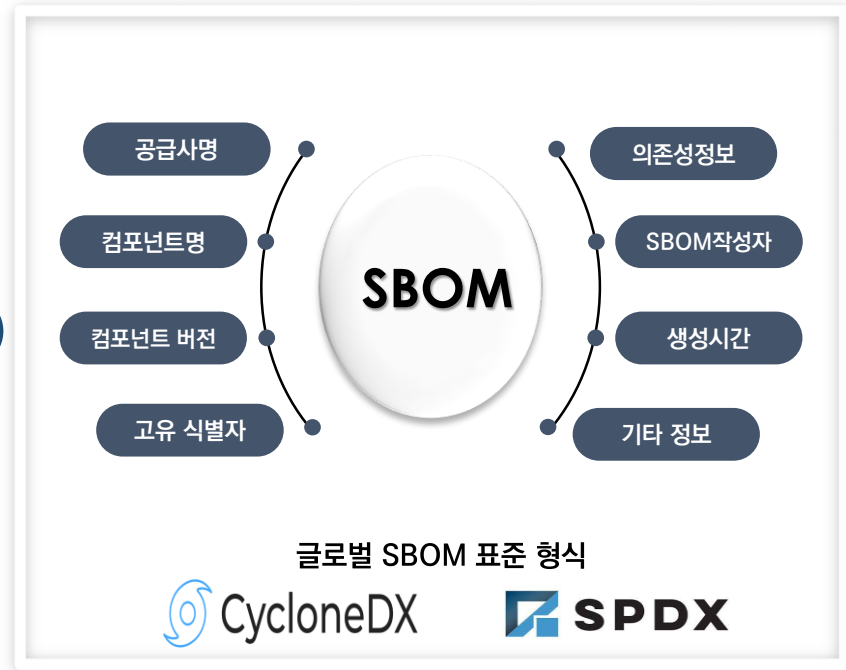
SBOM은 소프트웨어의 구성요소를 고유하게 식별하기 위한 메타데이터로 SW의 투명성 확보를 위한 기초 정보를 제공한다

식료품의 안정성 및 유해성분 정보

‘식품위생법’ 표시관련 규정

유통되는 식품에 관한 Food Ingredient가 해당 제품의 구성요소, 영양 정보, 위험성 등에 대한 명세를 담고 있듯이

SW의 투명성 확보를 위한 제반 정보



Software Bill of Materials(소프트웨어 구성명세서)는 SW의 투명성 확보를 위한 제반 정보를 기계판독(Machine Readable) 가능한 형식으로 표현한 것

NIS SBOM 표시 예제

NIS SBOM 표준 출력			
번호	항목	설명	내용 (data)
1	SBOM Standard	SBOM 표준	NIS
2	SBOM Type	SBOM 생성단계	Deployed
3	CycloneDX No.	CycloneDX 번호	-
4	SPDX Doc. ID	SPDX 문서번호	-
5	SBOM ID	NIS 식별자	20240124-certutil.exe-0011
6	Product Name	제품 이름	certutil.exe
7	Product Version	제품 버전	-
8	SBOM Author	SBOM 작성자	XSCAN
9	Unique Identifier	고유 식별자	64ad18f4d9bef01b86e39ca1e774dfa37db46bc8267453c418dd7f723d6d014c
10	Dependency Relationship	종속성 관계	nssutil3.dll, smime3.dll, nss3.dll, plc4.dll, plids4.dll, nspr4.dll, msvcrl20.dll, kernel32.dll
11	Timestamp	SBOM 생성일시	2024년 1월 24일 16시 29분 39초
12	Component Name	컴포넌트 이름	firefox
13	Component Alias	컴포넌트 별칭	-
14	Component Version	컴포넌트 버전	51.0-b5
15	Component Path	컴포넌트 경로	/22.02.08__delfino-g3-sha2.exe)/tmp/(delfino-g3-setup-x86.exe)/tmp/nss_sql
16	Component Hash	컴포넌트 해쉬	-
17	Component Supplier Name	컴포넌트 개발자 이름	firefox
18	License Name-Version	라이선스 이름-버전	MPL
19	Vul. DB	취약점 DB	NVD
20	CVE ID(CVSS)	CVE 식별자(취약점 등급)	CVE-2020-6820 (8.1) (KEV) , CVE-2019-17026 (8.8) (KEV) , CVE-2022-26486 (9.6) (KEV) , CVE-2022-26485 (8.8) (KEV) , CVE-2019-11707 (8.8) (KEV) (HE V) , CVE-2019-11708 (10.0) (KEV) , CVE-2020-6819 (8.1) (KEV)

NIS SBOM은 사용자의 SBOM 가독성을 증대시키고 초고도 취약점 기반의 관리를 강화하기 위한 국내 표준 SBOM

2021년 미국의 행정명령을 시점으로 **전세계적으로** SW 공급망 보안 위협 대응을 위해 **SBOM이 확고한 기술 표준으로 자리잡음**



- ▶ 2021. 행정명령 EO14028
- ▶ 정부납품 SW에 SBOM제출 의무화 추진



- ▶ 2022. 사이버복원력법 제안
- ▶ 24시간내 취약점 보고 의무화 추진



- ▶ 2022. 정부 주도 공급망보안 TF
- ▶ 실증사업 및 가이드라인 마련중



- ▶ 2022. 실증사업 및 3단계 로드맵
- ▶ SBOM 도입 가이드 발표

SBOM은 SW 공급망
보안의 시작점

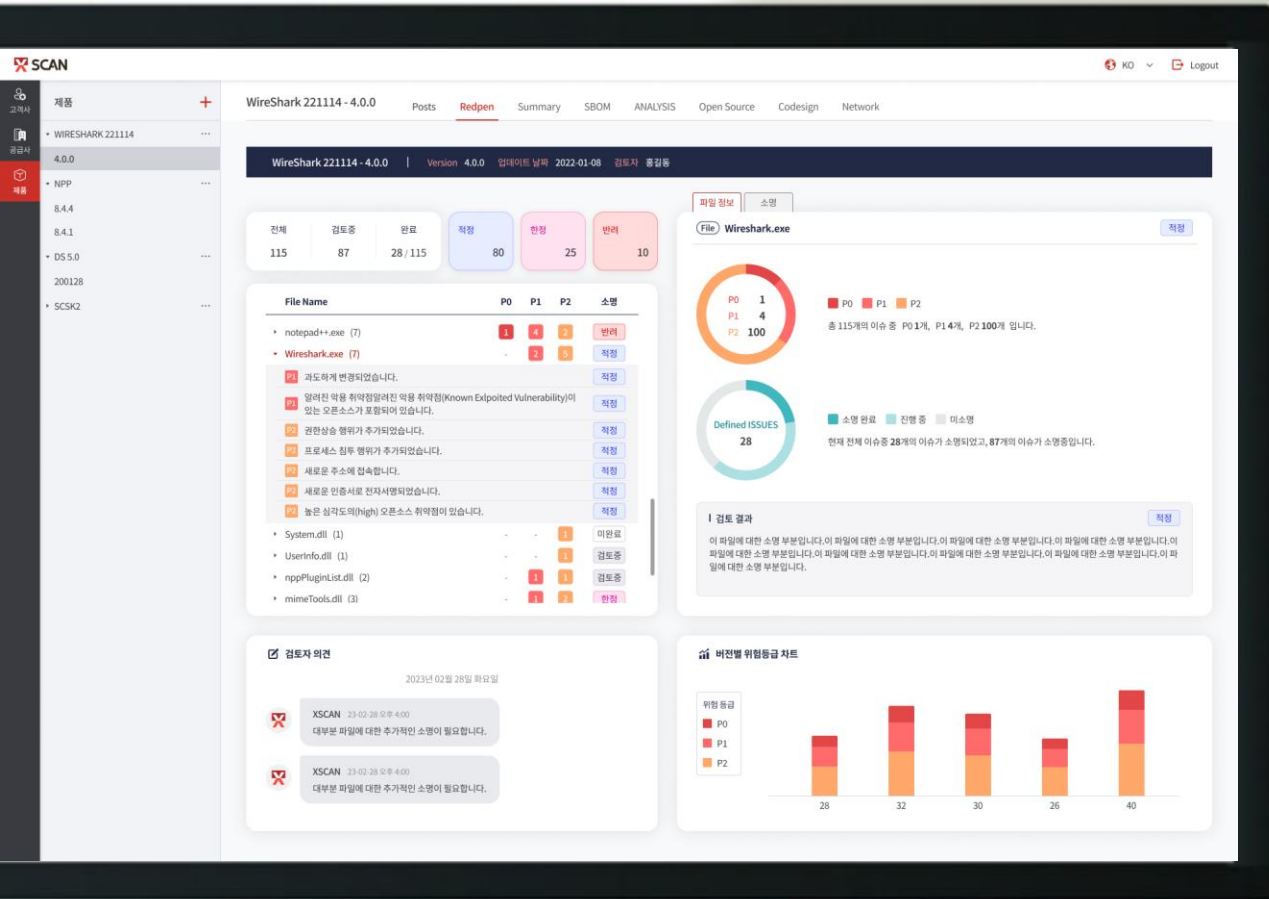


소프트웨어 생태계의
Communication Protocol



공급자와 수요자 간에
증거기반의 메타데이터 제공





01

클라우드 기반

- SaaS기반 단일한 프로세스의 구축

02

소프트웨어의 반입과 검증 혁신

- 'SW파일 분석시스템과 분석방법' 글로벌 특허 보유

03

세계 최초 AI 자동화 기법 탑재

- ChatGPT 발견된 위협 및 취약점 해석 및 조치 권고

04

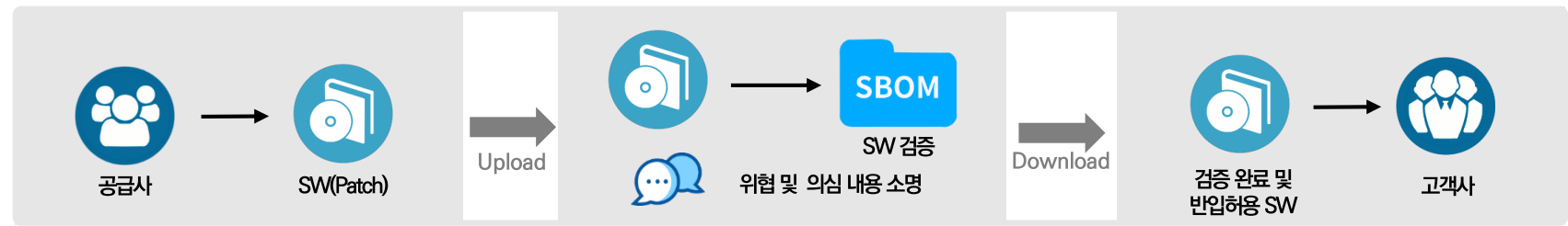
SW공급망 위협 대응 서비스

- 자동화된 시스템으로 사이버보안 관제 사각 지대 해소

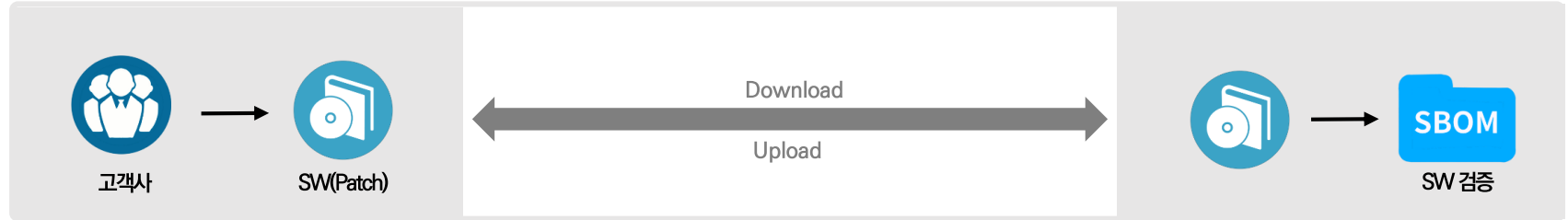
엑스스캔은 기존 일방적 전달에 머물렀던 SW 반입 프로세스를 혁신하였습니다

우리는 클라우드 기반에서 공급자와 사용자가 소통할 수 있도록 구현하였습니다

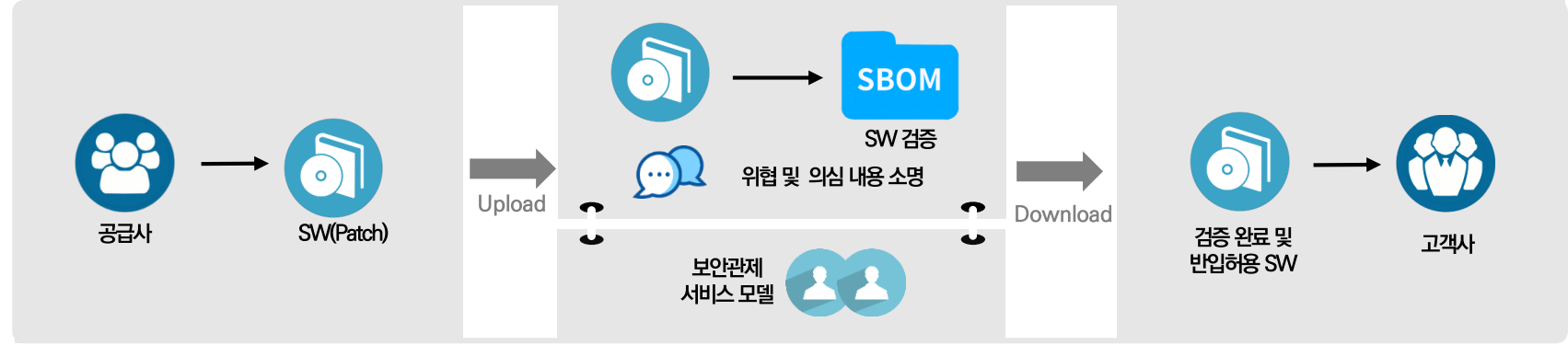
Case1: 공급사와 고객사 소통



Case2: 고객사가 직접 검증

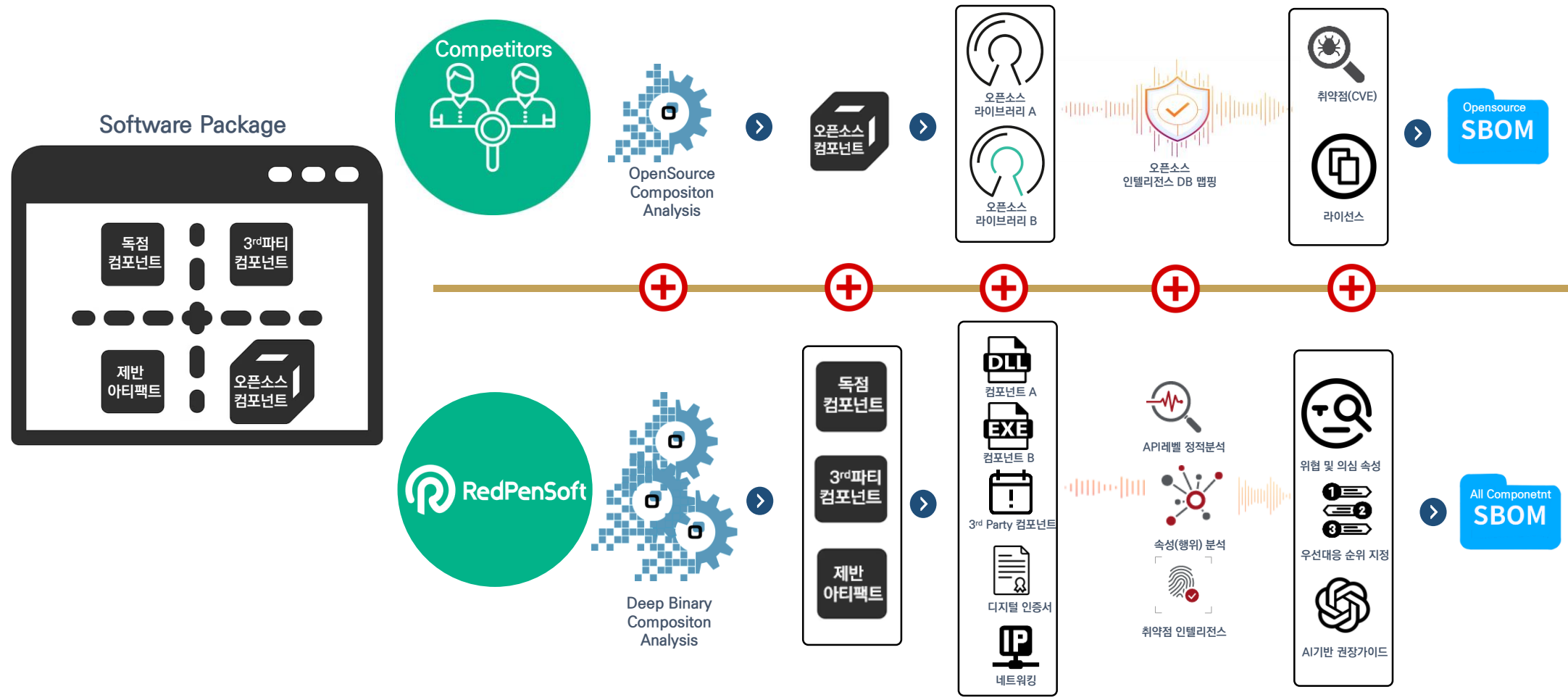


Case3: 제3자 검증



오픈소스 분석은 공급망 보안의 일부분일 뿐입니다

우리는 소프트웨어를 폭파 수준에 이르기까지 완전 분해했습니다



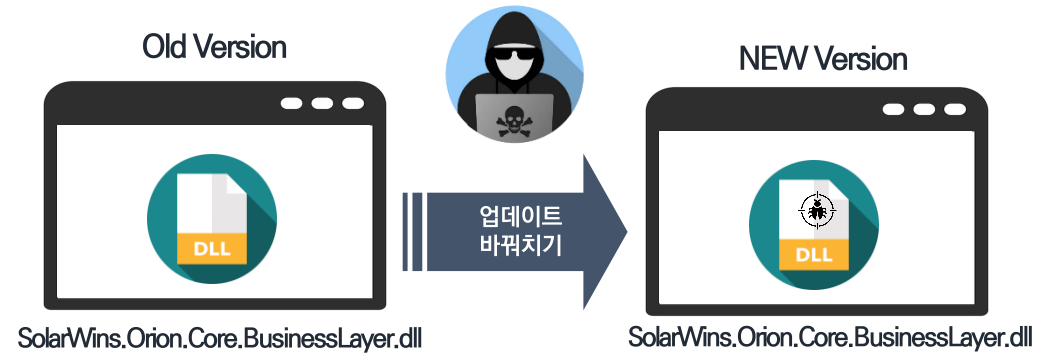


야생의 실제 공격은 특정 컴포넌트의 바꿔치기를 주 공격기법으로 하고 있었습니다

우리는 이전 버전 대비 변화되는 패치의 형상 관리가 그 해답임을 찾았습니다

솔라윈즈 공급망 공격

- 2020년 12월 발생한 본 공격은 러시아 정부 후원 해킹 그룹이 배후
- 솔라윈즈는 NMS/SMS 등 전세계 NO1, IT관리 SW 기업
- 미 정부기관 등 18,000 기업 피해, 바이든 정부의 행정명령 EO14028 발동 계기



- 이전 버전에서 동일하게 쓰이던 특정 SW 컴포가 위변조되었다
- 고객사의 모든 경계 보안 시스템 (백신/샌드박스 등) 탐지망을 통과하였다
- 공급사(SW개발사)는 침해 사실을 모르고 있었다

레드펜소프트 글로벌 특허



너무나 많은 오픈소스 취약점이 탐지되어 난감할 수 있습니다

우리는 우선 해결해야 할 취약점에 집중할 수 있도록 Pinpoint합니다

KEV

- Known Exploited Vulnerability로 미국의 CISA에서 관리하는 Must Patch CVE List
- 이러한 취약점을 가진 SW는 내부로 반입하면 심각한 위협을 초래할 수 있다

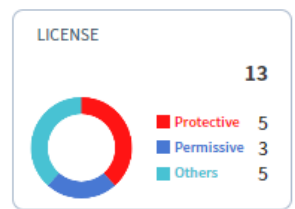
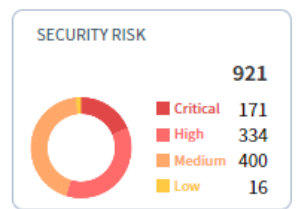
HEV

- Highly Exploitable Vulnerability로 FIRST(국제사이버사고대응포럼)의 EPSS 맵핑
- 30일 이내 익스플로잇 될 가능성이 70% 이상인 취약점

InternetBanking_INI****_Financial Certificate-3.3.2.41 | Version 3.3.2.41

Changes full story Open Source SBOM

Used Open Source 13



Known Exploited Vulnerability 7

Highly Exploitable Vulnerability 26

LITIGATOR 0

file list Threat Analysis

Threat Analysis(7)

P1 There is a file containing open source content with a Known Exploited Vulnerability. (One)

Scanned File	Matched Comp.	Component	Comp. Version	Security Risk	K.E.V.	HEV
certutil.exe	One	-	-	159 301 331 8	7	7
		firefox	51.0~b5	159 301 331 8	7	7

SBOM을 쉽게 이해하고 세부적으로 분석하기가 쉽지 않습니다

우리는 글로벌 표준 및 세부분석을 위한 자체표준, 그리고 국가표준 SBOM을 지원합니다

SBOM을 XSCAN 자체 양식(세부분석 지원) 및 글로벌 표준인 CycloneDX, SPDX 그리고 NIS SBOM까지 지원

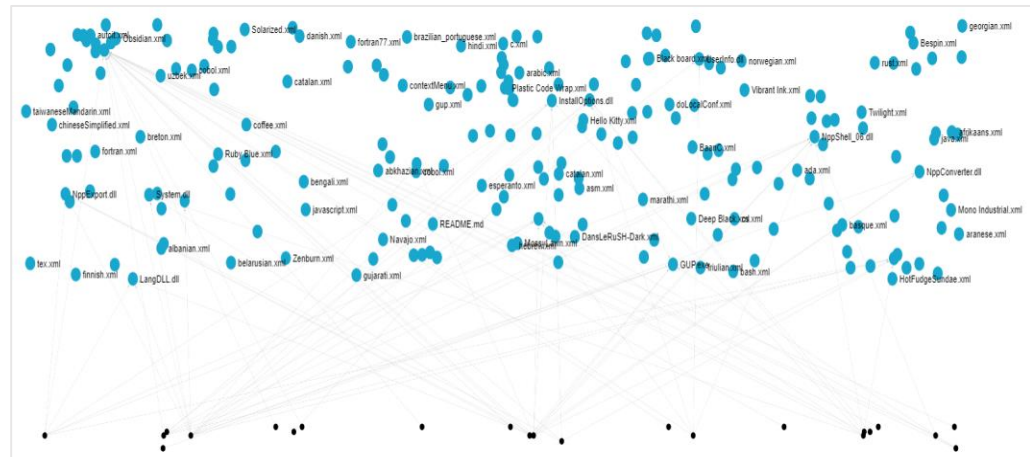
The screenshot shows the XSCAN interface for generating SBOMs. On the left is a sidebar with a product tree. The main area has tabs for 'Component' and 'Dependency Graph'. Below these are dropdowns for 'NIS' and 'All'. A table lists generated SBOMs with columns for format, generation time, stage, author, CycloneDX version, SPDX document number, NIS identifier, product name, version, NIS identifier, and continuation link.

Format	SBOM 생성일시	SBOM 생성단계	SBOM 작성자	CycloneDX 번호	SPDX 문서번호	NIS 식별자	제품 이름	제품 버전	고유 식별자	종속성 관계
XSCAN	2024년 1월 26일 17시 ...	Deployed	XSCAN	-	-	20240126-ipworks...	ipworks9.dll	9.0.0.5724	4eae8077f4770b3710...	kernel32.dll, user32...
SPDX	2024년 1월 26일 17시 ...	Deployed	XSCAN	-	-	20240126-python27...	python27.dll	2.7.11	8669a14f9bd7033f96...	kernel32.dll, user32...
NIS	2024년 1월 26일 17시 ...	Deployed	XSCAN	-	-	20240126-python27...	python27.zip	-	fe6fd815ddc3b75b7e...	-
NIS	2024년 1월 26일 17시 ...	Deployed	XSCAN	-	-	20240126-nvwintvne...	nvwintvne37.dll	2.7.219.0	741e4hd87410e9h73...	advant32.dll, user32...

CycloneDX SBOM 출력

The screenshot shows the JSON output of a CycloneDX SBOM. The root object contains 'bomFormat' (CycloneDX), 'specVersion' (1.4), 'version' (1), 'components' (34 items), 'dependencies' (207 items), and 'vulnerabilities' (27 items). A vulnerability entry is shown with details like 'bom-ref', 'id', 'ratings', and 'properties'.

Dependency Graph 출력




모두가 왼쪽(Shift Left)만을 이야기할때...

우리는 오른쪽(Shift Right)을 바라보았습니다.

제로트러스트 관점에서, 수요자가 SW의 무결성을 검증해야 합니다.



공급자 관점의 공급망 보안 대응
오픈소스 분석 도구 등



수요자 관점의 공급망 보안 대응



- SW벤더의 개발자가
- 오픈소스 분석도구 등을
- 개발 단말 및 SaaS환경에서
- SW개발 및 테스트 사이클에
- 안전하고 고품질의SW개발을 위해서
- 소스코드 기반 자동화된 기법

**5W
1H**

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

기존 5단계 검증 시스템에 SBOM기반 SW 취약점 관리 필요성이 제기

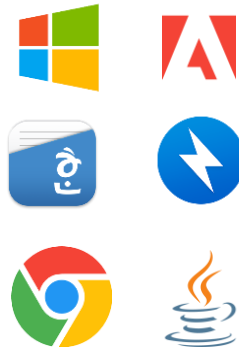
프로젝트 배경 및 목적

- 군 운용 SW 자산에 대해 5단계 검증 시스템을 구축하여 운영중에 있으나, **SBOM 기반 SW취약점 관리 필요성 제기**
- 반입 SW의 무결성 검증을 위해 기존 운영버전 대비 신규 패치 버전의 변화관리 필요성 제기됨
- 파일사이즈가 큰 SW(Windows OS 등)의 분석 제약 및 과다 시간 소요

적용 대상 및 운용 예시

- 3군 표준 운용 SW중 지속적인 패치가 이루어지는 SW 선정
- Windows 10, 아래한글, 반디집, 크롬, Java SE, Acrobat 등 총 10종 SW 대상 적용
- 매월 신규 패치 적용 전에 이전 버전과 패치 버전의 비교 및 변화 추적

3군 운용 표준 SW



Before



After





SW 공급망 공격의 주타겟이 되는 대국민 금융서비스의 보안인증 프로그램에 적용 및 SI최종 산출물의 SBOM 생성

금융 도입 사례

프로젝트 배경 및 목적

- 오픈소스 분석 툴이 도입되어 있으나 이는 내부 업무 개발을 위한 개발자들의 활용 용도, 보안 운영 관점의 툴 필요
- 대국민 금융서비스에 필수 설치 단말 SW의 무결성 검증 제기
- 이메일 등을 통한 상용SW(패치)의 반입 프로세스 및 체계 개선

적용대상 및 운용예시

- 베라포트 등 보험 서비스시 필수 설치 보안 단말 SW : 검증 후 배포
- SW공급망 공격의 핵심 타겟이 되는 보안 툴 및 IT인프라 관리 핵심 도구
- 추후 모바일 앱 및 도커이미지로 대상 SW 확대 예정

공공 도입 사례

프로젝트 배경 및 목적

- 국가 규정 준수와 비밀관리 내부 통제를 위한 SI 프로젝트 시행
- 프로젝트시 도입되는 제반 상용 SW 및 최종 결과물에 대한 고객사 관점의 무해성 검증 제기

적용대상 및 운용예시

- 도입되는 국내외 상용 SW내의 오픈소스 의존성(취약점 및 라이선스)
- 최종 산출물에 대한 SBOM 생성 및 관리
- 검증 전문 벤더사(레드펜소프트)에서 제3자 검증 시행



OTHERS vs XSCAN

모두가 'SW공급망 보안'을 이야기합니다
오픈소스 검증을 수행하는 필요하고 훌륭한 도구들입니다.

엑스스캔은 경쟁제품이 없습니다
다만 파트너십이 있을 뿐입니다

비교 관점		OTHERS	XSCAN
제품정의		오픈소스 분석 도구	Binary 기반 소프트웨어 공급망 공격 대응 도구(오픈소스 분석 포함)
적용단계		소프트웨어 개발 단계 (일부 바이너리 기반 도구는 릴리스 단계 적용 가능)	SW개발(릴리스 단계), SW운용(획득/패치/유지보수 전 단계)
오픈소스 분석기능	취약점	CVSS2, CVSS3 Metric	CVSS2, CVSS3 Metric + KEV 및 HEV
	라이선스	컴포넌트 라이선스 자동 식별	컴포넌트 라이선스 자동 식별
	지원언어	소스코드 기반 제품은 지원 언어에 제한적일수 있음	C/C++/Java/Java Script/Python/Go Lang 등 모든 언어
	AI연계	없음	ChatGTP 연계하여 취약점에 대한 요약 및 권장 가이드 제시
SBOM	대상	오픈소스 컴포넌트 Only	오픈소스를 포함한 SW구성상의 모든 컴포넌트 대상 SBOM생성
	지원표준	CycloneDX/SPDX 등 글로벌 표준	자체 표준 및 CycloneDX/SPDX 등 글로벌 표준 + NIS SBOM
디지털 인증서 검증		해당 기능 없음	만료, 폐기(회수요청), 블랙리스트 등 코드사인 인증서의 무결성 검증
의심 및 위협 속성 분석		해당 기능 없음	권한상승, 프로세스 인젝션, 네트워킹 등 의심 및 위협 속성 분석
이전 버전 대비 비교		해당 기능 없음	SW 패치의 변화 관리를 통해 서비스 위변조 등 탐지
도커 이미지 분석		오픈소스 분석에 한함	오픈소스 분석(현재 지원) 및 다양한 이미지 취약점 스캐닝(24 Q1)

Question?	Answer
어떤 유형의 SW를 지원하는가?	<ul style="list-style-type: none"> ▪ 현재 Windows 운영 환경의 모든 SW 분석 가능, 오픈소스만 분석 시 Windows, Linux, Mobile APP, 클라우드 등 모든 유형의 어플리케이션 지원 ▪ 2024년 Q1 도커이미지 스캐닝 (현재 벌어지는 거의 대부분의 공급망 공격은 Windows 환경에서 시행)
SW 검증에 걸리는 소요 시간?	<ul style="list-style-type: none"> ▪ SW의 파일 사이즈 및 구성 컴포넌트에 따라 의존적. 작게 수분에서 길게는 몇 십분. ex)Windows 10 OS 약 15분 소요
누가 SW를 업로드 하나?	<ul style="list-style-type: none"> ▪ 3가지 채널 구성 방식 지원, 고객 스스로 전달받은 SW를 업로드 가능, 유지보수 계약서에 절차 준수 방식 추천
이메일 통한 SW 반입이 왜 문제?	<ul style="list-style-type: none"> ▪ 이메일은 공격자들이 가장 선호하는 공격의 벡터. BEC(비즈니스 사칭 메일)을 통해 SW 공급자 가장한 패치 전달 가능성 높음 ▪ 기업의 자산으로서 SW 및 SW 패치에 대한 통합적인 리포지토리 및 이력관리 시스템으로 위치할 수 있음
망분리 환경에서 사용가능한가?	<ul style="list-style-type: none"> ▪ 이슈 없음, 현재의 Email 및 CD등을 통한 반입 체계를 클라우드로 대체한 것임.엑스스캔 검증된 SW는 다시 망연계 통해 내부 반입 수행
이미 오픈소스 분석 툴을 사용...?	<ul style="list-style-type: none"> ▪ 현재 보유한 오픈소스 분석툴은 내부 개발자들의 사용 용도에 국한. 외부에서 반입되는 상용SW등은 적용되지 않음

귀사 어플리케이션의 SW공급망 위험 및 취약점을 점검해볼 수 있는 무상 서비스를 제안 드립니다

- ✓ 로그포제이와 같은 제로데이 취약점이 다시 발생한다면 어떻게 하시겠습니까?
- ✓ SW공급망 공격으로부터 안전하다고 자신할 수 있습니까?
- ✓ 미션 크리티컬한 대국민 서비스를 운영하고 계십니까?

01

기업의 인프라에 아무것도 설치되는 것이 없습니다.

02

계정을 받으시고 대상 서비스를 업로드 후 리포트를 보기만하시면 됩니다.

03

모든 과정은 2024년 말까지 무상으로 제공됩니다.

지금 바로 XSCAN 무상 서비스를 활용하세요

Make Trusted Software Value Chain



Visit Redpensoft

www.redpensoft.com
redpensoft.tistory.com



Copyright 2024 RedPenSoft Co.,Ltd.