군 사이버 위협 대응 을 위한
신기술 소개 및 적용 세미나

소프트웨어 공급망 위협 대응 기술

“수요자관점의 SW 공급망 보안 대응”

2023.11

RedPenSoft

RedPenSoft 공격자의 전술을 완벽히 꿰뚫는 소프트웨어 공급망 보안 전문기업

CONTENTS

1. SW Supply Chain Attack

최신 급증하는 SW공급망
공격의 정의와 특징,
그 사례들을 살펴본다

SW공급망 공격 정의

소프트웨어의 생산 및 전달과정

해커의 악의적인 공격
의도하지 않은 취약점

"2025년까지 전세계 기업의 45%가 공급망 공격 경험"
『2022, Gartner』

국가후원 APT 해킹그룹

최신의 모든 사회공학적기법

성공할 때까지 끈질기게 시도

SW Supply Chain Attacks

주요공격기법

- Hijacking updates
- Undermining code signing
- Compromising open-source code
- Zero-Day Vulnerability

최신의 SW 공급망 공격

최근 SW공급망 공격은 급격하게 증가하고 있으며 공격의 특성상 밝혀지지 않은 공격은 더 많음
한국은 지정학적 특수성상 북한 발 APT공격 등 SW공급망 공격의 주요 타겟이 되고 있음

2021.07
방산업체 기밀문서 탈취
북한 해킹그룹 추정
VPN취약점 악용

2021.08
카세야(Kaseya)
Revel Group
원격접속SW 권한 획득

2022.03
보안업체 I사
보안패치 위· 변조
47개 기업 및 기관 피해

2022.09
채팅제공업체 Comm100
설치프로그램 하이재킹
51개국 수천명 피해

2023.02
국내 파일전송프로그램
Agent 취약점 악용
악성코드 유포

2023.03
3CX VOIP 화상통화
북한 UNC 4736, 제2 솔라윈즈
최초의 연쇄 SW공급망공격

2023.04
보안인증프로그램
취약점 악용
언론사 포함 61개 기관 피해

2023.04
MOVEiT 파일전송 프로그램
Clop랜섬웨어 갱단
약 1,500개 기업 피해

2023.06
보안업체 G사
업데이트 정책서버 침해
가상자산거래소 등 공격의심

2023.07
Jump Cloud 계정관리 업체
북한의 미로 천리마
가상화폐 암호화폐 탈취

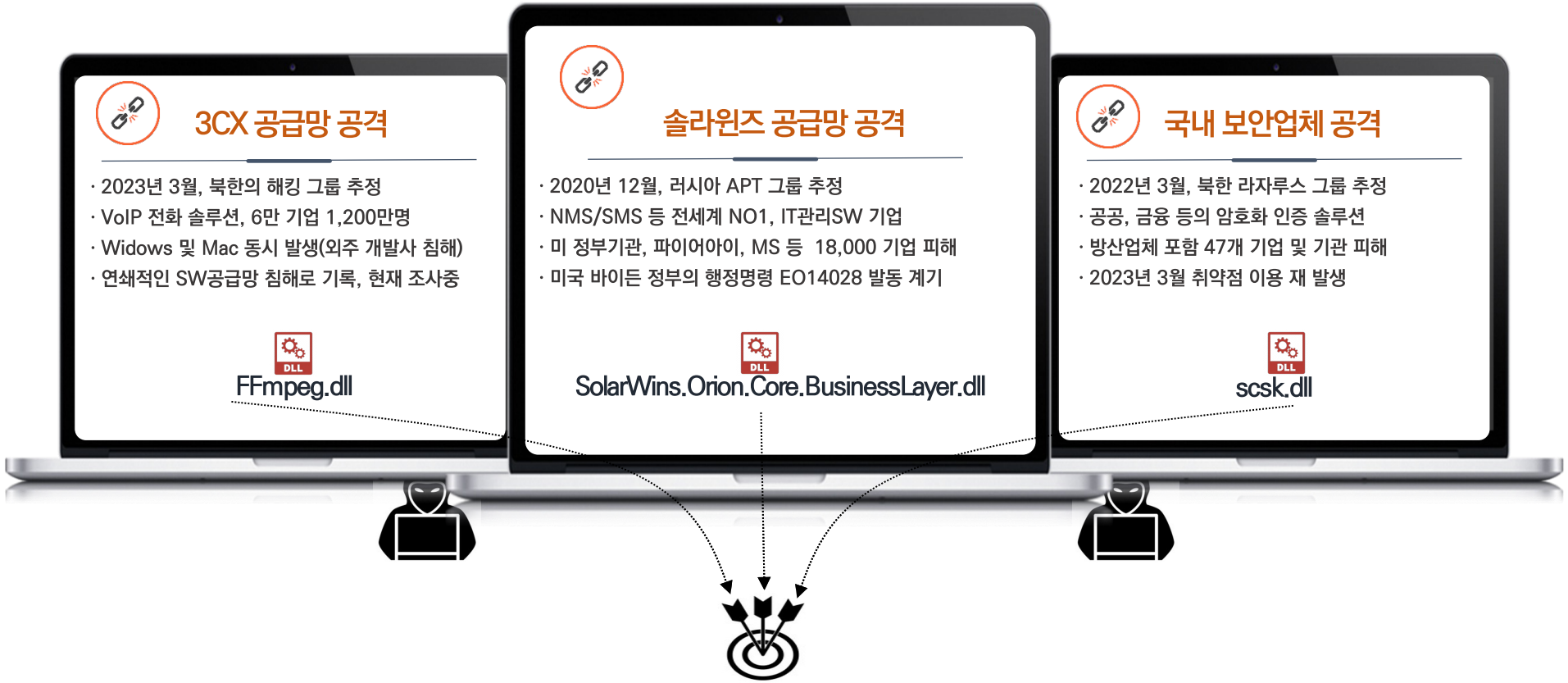
국내외 주요 SW 공급망 공격 분석

Insigthts

- 우리나라는 국내 시장을 장악하고 있는 보안 벤더의 EndPoint 솔루션이 주요 공격의 대상이 되고 있다
- 업데이트 위변조, 제로데이 익스플로잇이 SW공급망 공격의 핵심 공격 기법으로 사용되고 있다
- 북한이 국내외 SW 공급망 공격의 주요 Threat Actor로 전면에 부상하고 있으며, 주로 금전적 이득을 목적으로 한다

대표적인 SW공급망 공격 사례 분석

국내외 대표적인 공격 사례 분석을 통해 SW공급망 보안 대응에 필요한 핵심 요소 기술을 통찰



공격자 관점

Insights

- 이전 버전에서 동일하게 쓰이던 특정 SW 컴포넌트(DLL)가 위·변조되었다
- 기존 경계 보안 시스템 (백신/샌드박스 등) 탐지망을 통과하였다
- 보안 SW, 업무 SW 등 외부 반입 상용 SW의 패치 과정에서 발생하였다

SW공급망 공격 특징

개발사의 네트워크에 침투하여 소스코드를 수정하거나 배포 서버에 잠입하여 파일을 위·변조

피해 사실을 실시간으로 파악 어려움

- 개발사(SW벤더)와 고객사간 신뢰를 바탕으로 프로그램 반입
- 패치를 위장한 악성 파일에 대해서 정상프로그램으로 인식함

제로 트러스트 관점의 대응 필요

- 기존 SW 반입 관행·체계 및 프로세스를 개선
- 모든 SW자산에 대한 반입 이력 시스템화

공격경로 원천적으로 차단 불가능

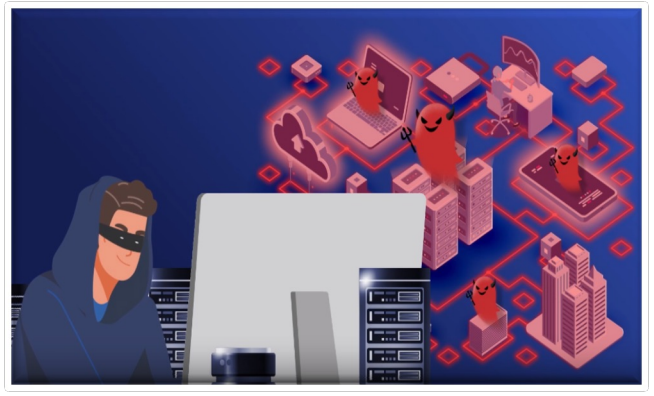
- 모든 프로그램은 기능 및 보안 강화를 위해 주기적으로 업데이트를 실행함
- 백신이나 이메일 게이트웨이 등 기존 경계 보안 악성코드 대응 시스템으로 탐지 불가능

혁신적인 SW 무결성 검증 방안 필요

- 업데이트 가로 채기 등을 통한 위·변조 된 서비스 검증
- 권한 상승 등의 의심속성 및 오픈소스 취약점

사회적 파급력이 크다

- 다른 해킹보다 훨씬 많은 기술과 노력이 필요 (주로 국가 후원 APT 그룹이 공격 주도)
- 한번의 공격으로 대규모 파급효과 및 피해 발생 (금전적 이익/ 사회혼란/ 기밀 정보 탈취가 목표)



국가적 관점의 대응 방안 마련 필요

- SW 공급망 공격 방어를 위한 가이드라인 마련
- 주요 기반시설 및 대민 서비스 관련 대응체계 고도화

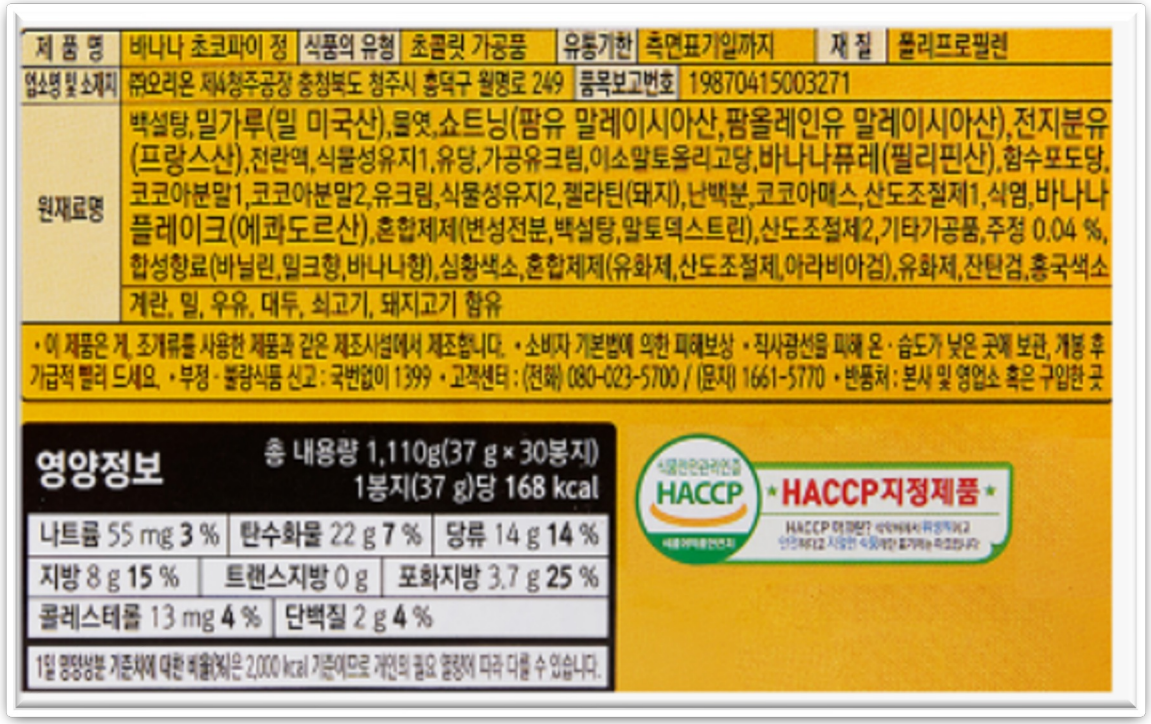
2. 표준 기술로서 SBOM의 부상

SW공급망 공격 위협에 대응하기 위한 글로벌 표준 기술로 자리매김하는 SBOM에 대해 살펴본다

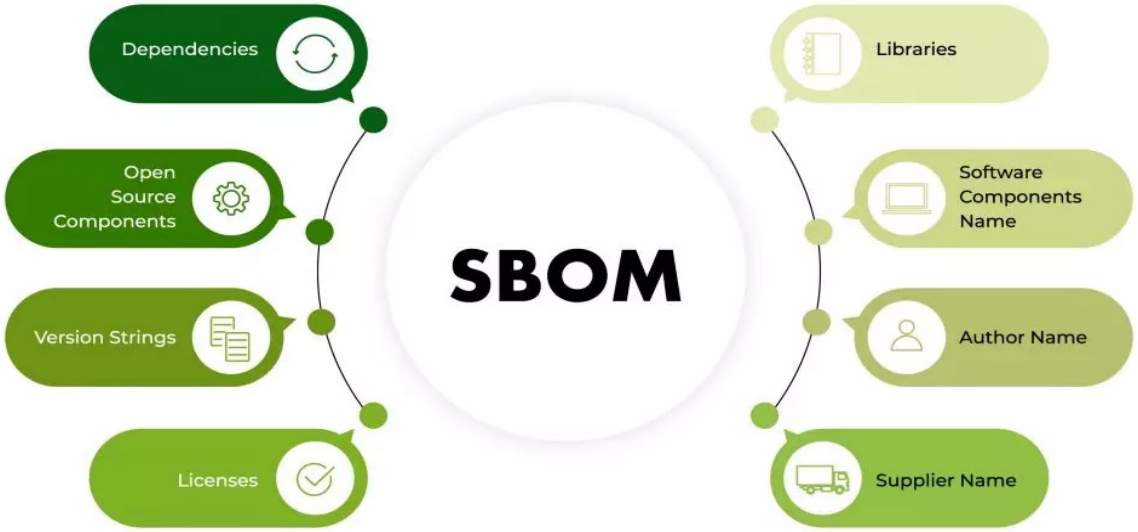
SBOM이란 무엇인가?

SBOM은 SW 공급망 보안을 위한 핵심 표준 기술로 부상하고 있다

유통되는 식품에 관한 Food Ingradient가 해당 제품의
구성요소, 영양 정보, 위험성등에 대한 명세를 담고 있듯이...



Software Bill of Materials(소프트웨어 자재명세서)는 SW구성
목록을 기계판독(Macine Readabal) 가능한 표준으로 구현한 것



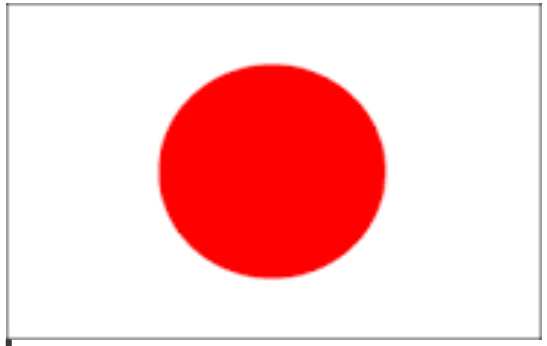
CycloneDX SPDX

SBOM관련 국내·외 관련 규제 및 기술 도입 현황

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

- 2021.05 바이든 행정명령 EO14028
- 중요 SW 범주 및 보안 지침 등 발표
- SBOM의 최소 요건 및 표준 등 발표
- 2023.09 정부기관 납품 SW에 대한 SBOM 제출 또는 자체인증서 의무화

- 2022.09 Cyber Resilience Act
- EU내 디지털 제품의 사이버보안 강화 목표
- 공급망 보안 필수 요건으로 SBOM 명시
- 해당 법안은 2026년 시행 예정임

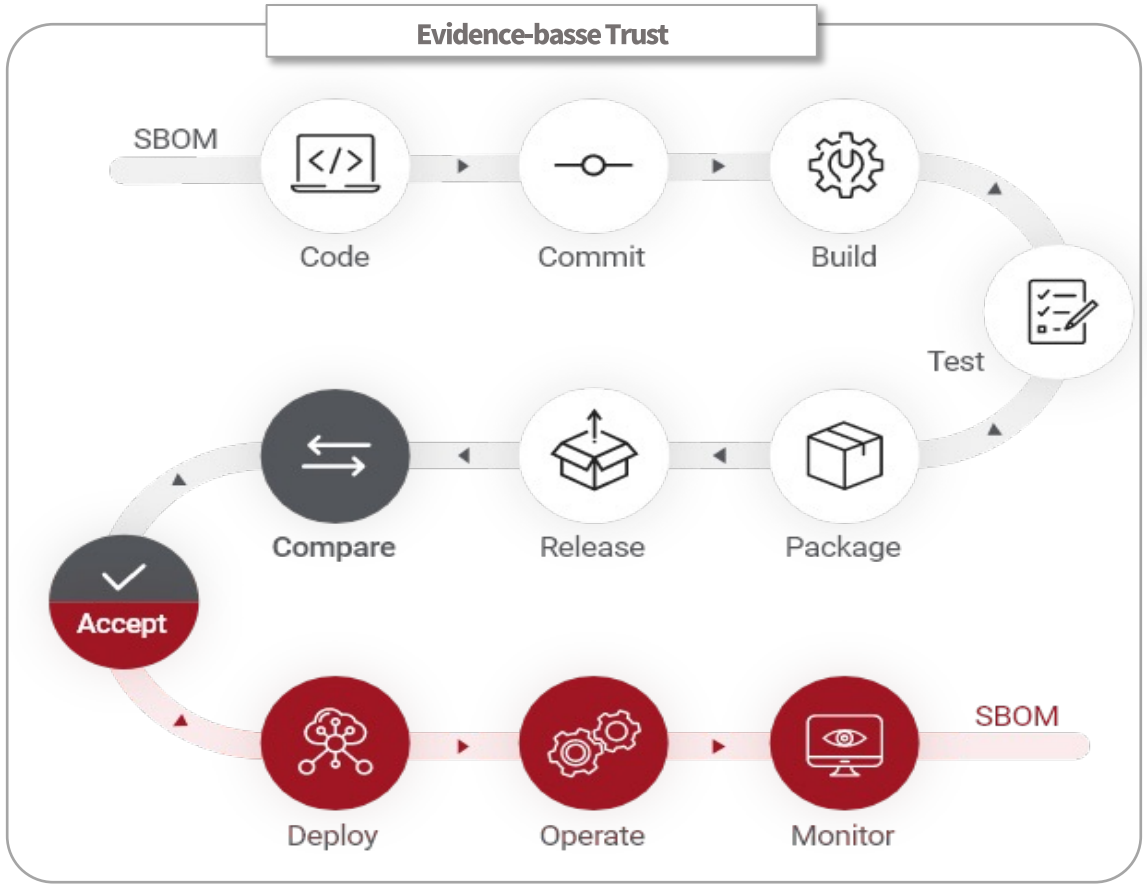


- 2022.08 SBOM 정책 로드맵 발표
- METI(경제산업성) 주도 전담 TF 구성
- SBOM도입에 대한 개념증명 사업시행
- 25년 3월까지 3단계 걸친 세부 과제 제시

- 2022.10 과기부 공급망보안 포럼 출범
- 2023.08 국정원 공급망 보안 TF 구성
- 과기부 SW공급망 보안 실증 사업 시행
- 2023.04 디지털플랫폼정부 계획 발표 (제로트러스트와 SW공급망보안 구현)
- SBOM 활용가이드 및 SW공급망 보안 점검 기준 가이드 마련 중(2024년 공표)

왜 SBOM이 중요한가?

소프트웨어의 전체 라이프사이클에서 SBOM을 기준으로 SW의 무결성 및 취약점 이슈를 해결할 수 있음



[Source] “Deliver Uncompromised : Securing Critical Software Supply Chains” 2021.03 MITRE Corporation.

STEP 01 증거 기반의 신뢰

소프트웨어 전체 Life Cycle에서 표준 소프트웨어 부품 명세서(SBOM)를 메타 데이터로 관리

STEP 02 비교 분석

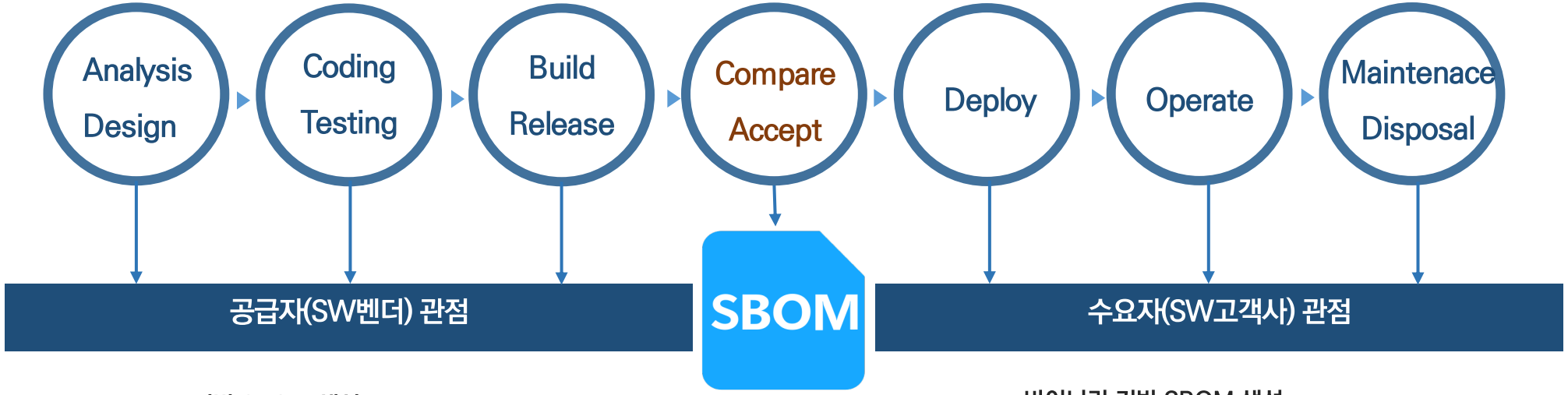
공급사 제공 SBOM에 대해 수요자 관점에서 무결성 검증 등 비교 분석 수행

STEP 03 사용자 승인 반입

단일한 체계와 경로를 통해 소프트웨어를 검증하고 최종 승인을 통한 SW(패치)의 반입 및 배포

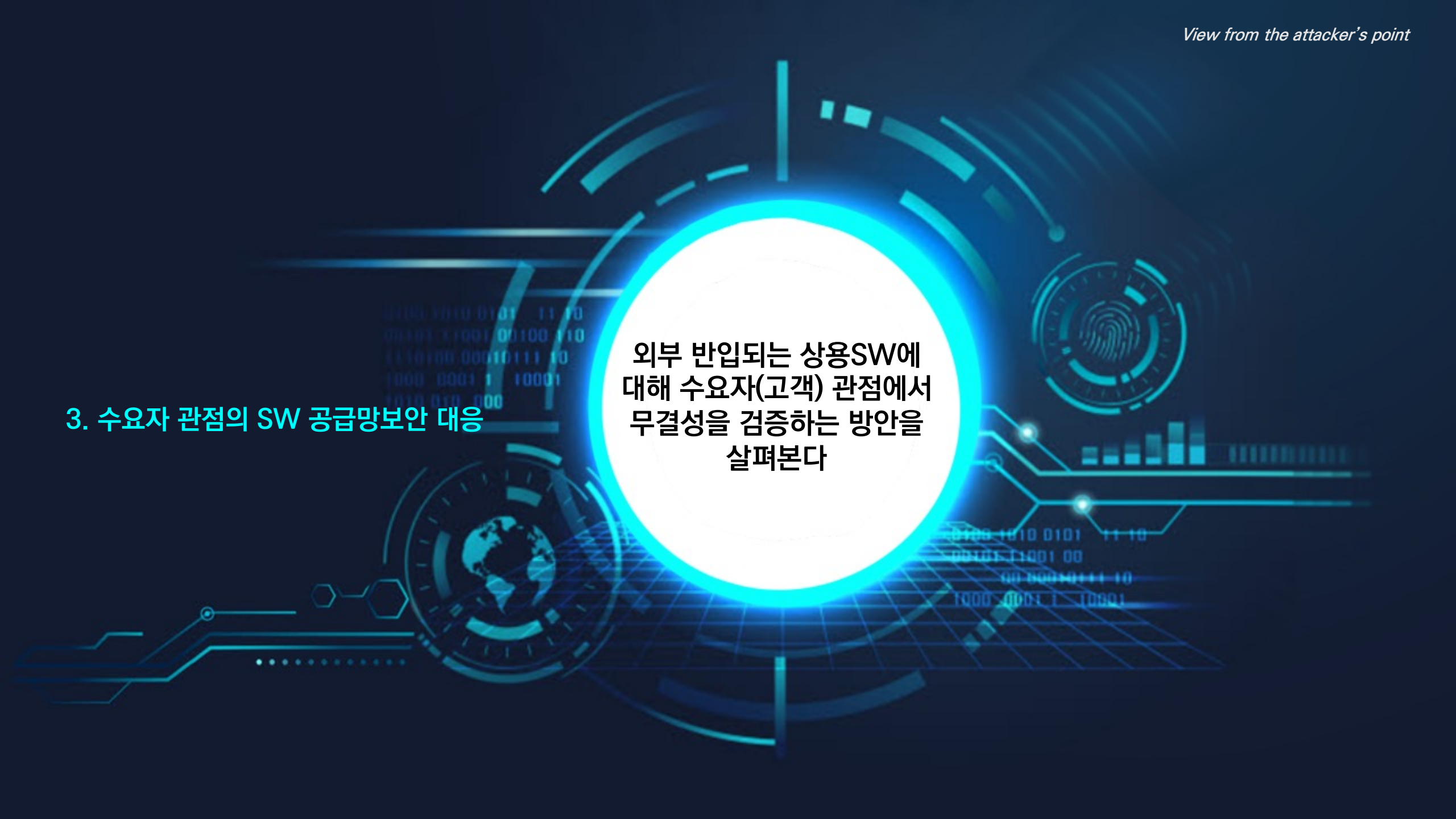
SBOM의 활용

공급자와 수요자 모두 SBOM을 기준으로 SW Life Cycle상에 수행해야 할 역할을 재정의 해야 함



- 소스코드 기반 SBOM 생성
- 개발 테스트 과정 SBOM 기반 SW 컴포넌트 관리
- SBOM 기반 외부 제3자 컴포넌트의 취약점 검증
- SBOM 기반 오픈소스 코드의 취약점 이슈 관리
- 릴리스 버전의 최종 형상 SBOM 고객사 제출

- 바이너리 기반 SBOM 생성
- 공급사 제출 SBOM의 진본성/무결성 확인 및 비교 분석
- SBOM 기반 오픈소스 등 취약점 확인, 인증서 검증
- SBOM 통한 유지보수/패치 파일의 서비스 위변조 탐지
- 내부SW자산 SBOM 목록화 : 제로데이 취약점 즉각 대응

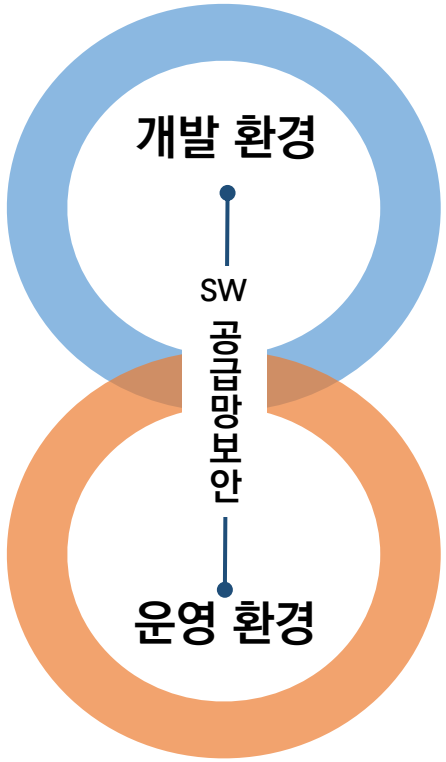


3. 수요자 관점의 SW 공급망보안 대응

외부 반입되는 상용SW에 대해 수요자(고객) 관점에서 무결성을 검증하는 방안을 살펴본다

왜 수요자 관점이 필요한가?

기업이 획득하는 SW는 작성자, 저작권 소유, 획득 방식 등에 따라 3가지 유형으로 구분되며
각 SW 유형별로 핵심 구현 기술 및 대응방안과 주체가 달라져야 함



1st Party SW	2nd Party SW	3rd Party SW
· 기업내부 연구소 혹은 개발팀이 직접 개발 · 소스코드 기업이 직접 보유 · SW구성 가시성 확보 가능	· SI 등 외부 기업(용역)을 통한 개발 · 계약 유형에 따라 소스코드 보유 가능 · SW구성 가시성 확보 쉽지 않음	· 완성 제품(상용 SW)의 구매 · 소스코드 제공되지 않음 · SW구성 가시성 확보 어려움
Secure Coding, SAST/DAST Open Source Control 구현	RFP등에 개발환경 보안 관련 명시 및 SW검증을 위한 테스트 강화	SW 납품 업체에 대한 일상적인 개발환경 통제 및 관리 감독이 불가능함

SW 획득 방식에 따른 SW공급망 위협 대응 과제 및 주체의 변화

개발자 및 공급사 관점의 대응방안

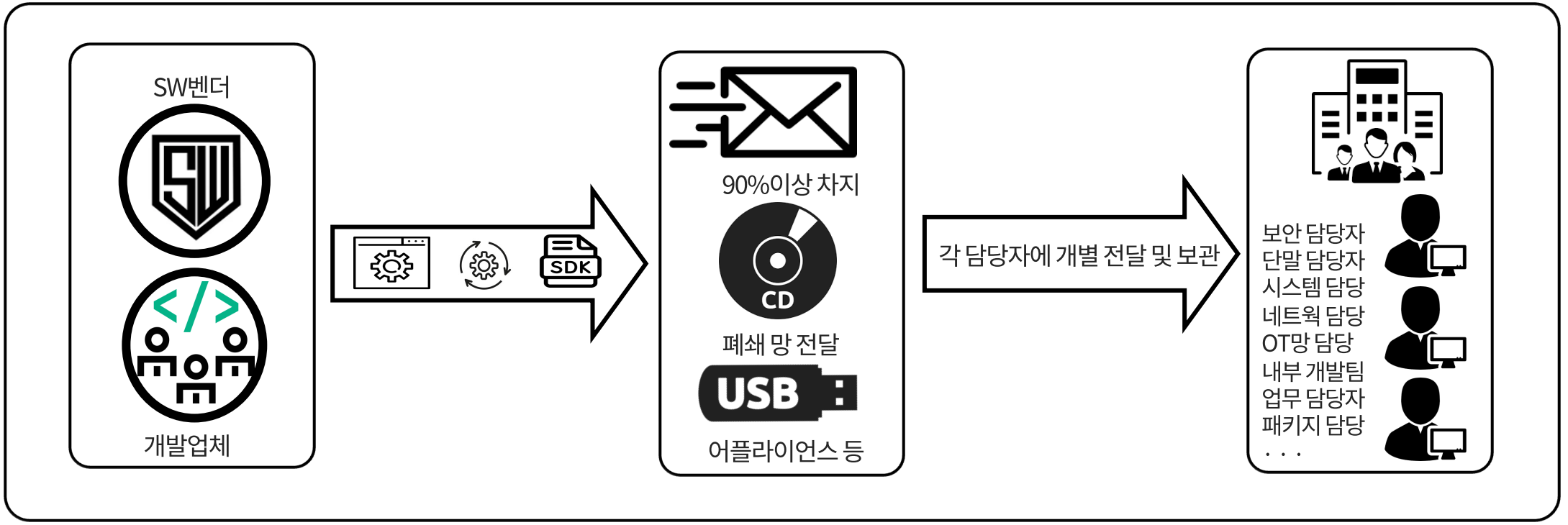
개발자 관점의 개발 가이드라인 준수 및
Open Source Control이 주요 과제로 제기됨

수요자[고객사] 관점의 대응방안

야생의 현실에서 발생하는 모든 SW공급망 사건에 해당
공급사(개발과정)가 침해될 수 있다고 가정
보안팀의 R&R 및 관제 프로세스로 정립 필요

수요자 관점 이슈 : SW 반입 경로 이슈

주로 Email에 의존하고 있는 현행 SW 반입 체계는 그 자체로 심각한 문제점을 안고 있음



[1] BEC : Business Email Compromise 신뢰하는 사람이나 조직에서 온 메일처럼 위장하는 사칭 메일 공격
[2] EAC : Email Account Compromise 실제 메일 서버 혹은 계정을 침해한 후 신뢰하는 곳에서부터 들어오는 사기 공격

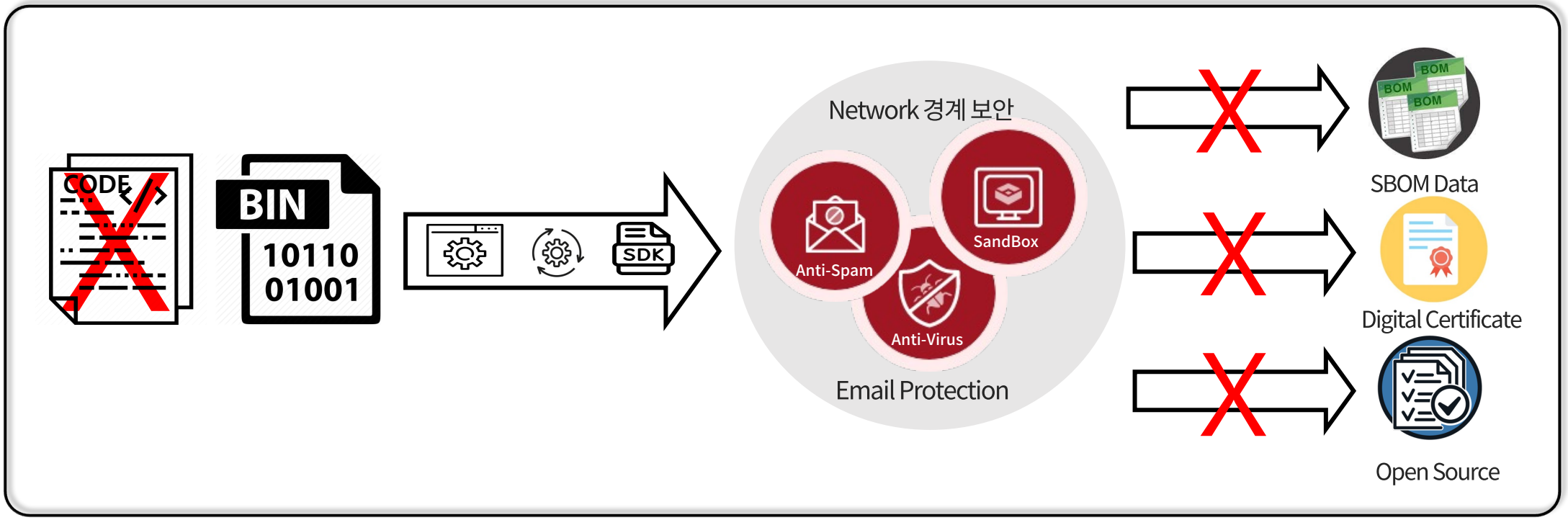
SW의 반입

Insights

- 자산으로서 SW 반입에 대한 단일한 통로(리포지토리)를 확보하고 있지 못하다
- 이메일은 공격자들이 가장 선호하는 공격의 벡터로 작용한다(BEC[1]공격, EAC[2]공격)
- 일방적인 전달이 그치고 있고, 제반 이력을 자동화하기 위한 소통 창구가 없다

수요자 관점 이슈 : SW 검증 방법 한계 이슈

소스코드가 제공되지 않는 외부 반입 SW는 공급망 공격 방어 관점의 새로운 분석이 추가되어야 함



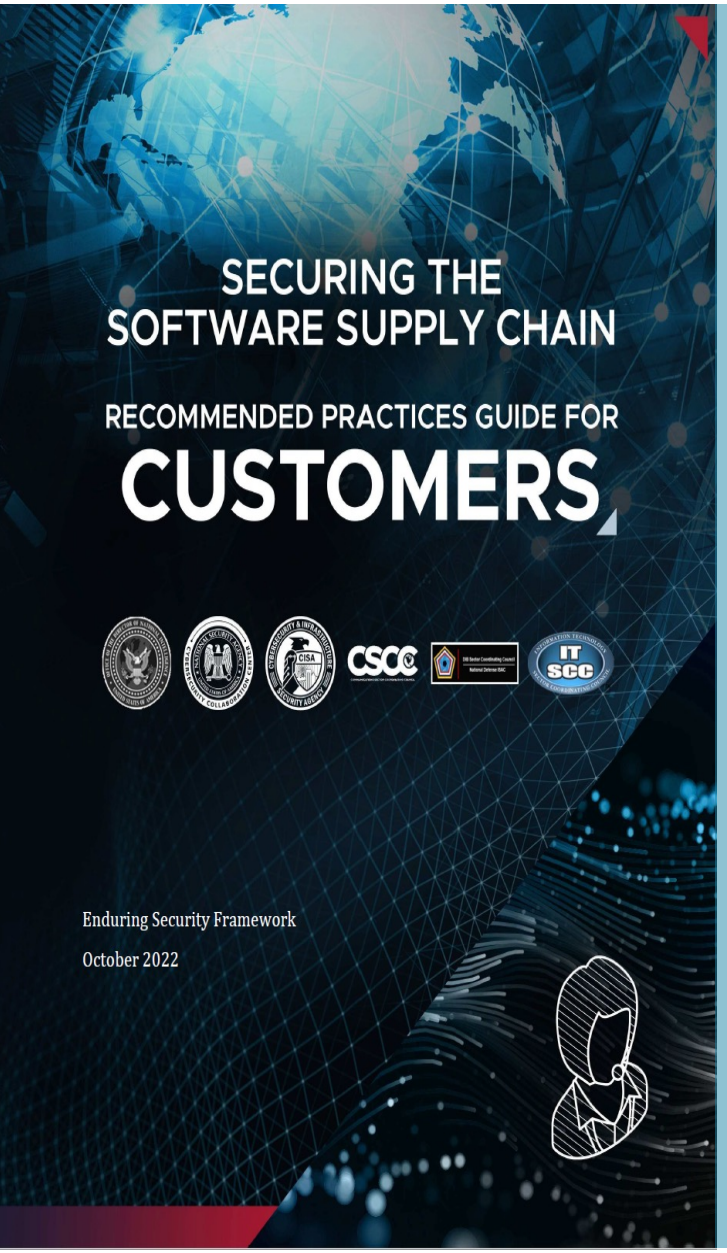
[1] HEAT : Highly Evasive Adaptive Threat 회피성이 뛰어난 지능형 위협

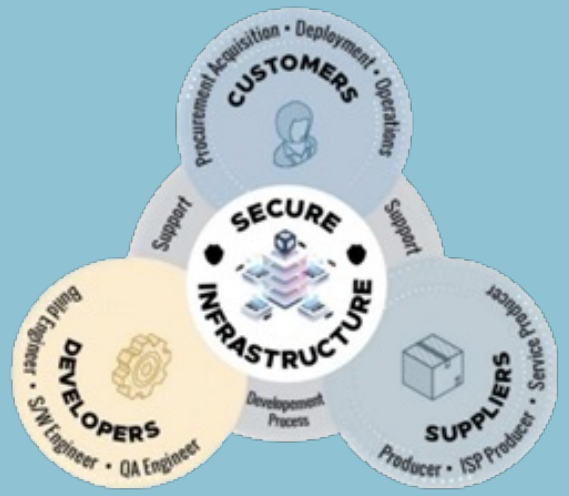
SW의 검증

Insights

- 기존의 경계보안 탐지 시스템은 Heat[1] 공격 방식의 SW 공급망 공격을 방어하지 못한다
- 오픈소스 의존도 분석 및 SBOM에 기반한 SW 검증이 이뤄지지 못한다
- 바이너리 기반에서 SW를 검증할 새로운 시스템 구현이 필요하다

수요자[고객사]관점 대응의 선진사례 벤치마킹





Enduring Security Framework

- 미 국토안보부(DHS)후원, 국가안보국(NSA) 주관하에 주요 인프라의 사이버안보 강화를 위한 공공·민간 전문가 그룹
- 5G, Cloud, SW Supply Chain 분야 등에 선도적으로 Best Practice 등 연구 성과를 CISA에서 리포트 발간

Securing Software Supply Chain

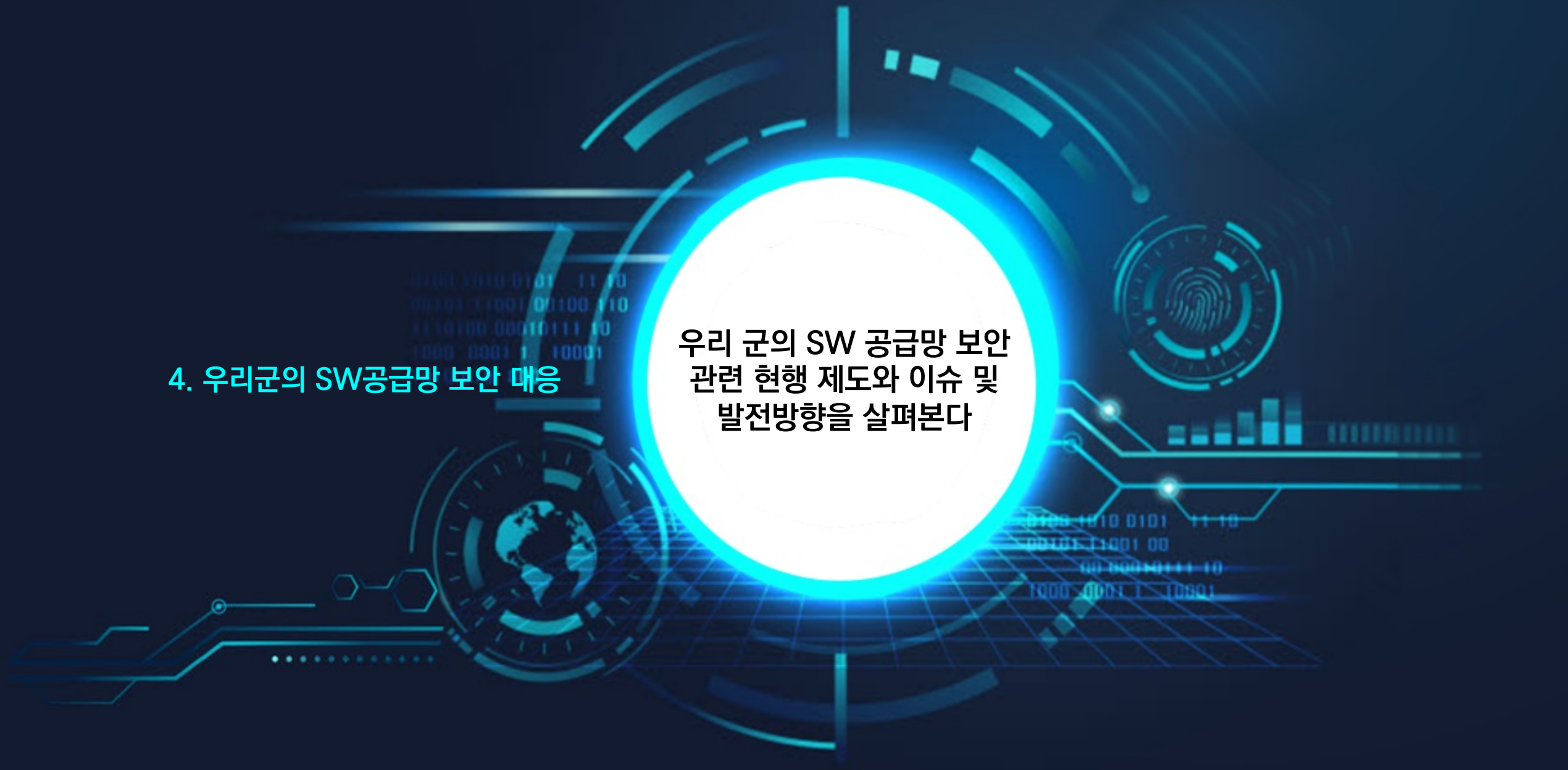
- Guide for Developer(2022/08) / Guide for Suppliers(2022/09) / Guide for Customer(2022/10)
- 발생가능한 위협 및 권장 조치 사항 가이드

발생 가능한 위협

- SW획득 과정에서 보안 요구 사항의 결여
- 공급자로부터 제공된 SBOM의 불완전성
- 계약과 다른 제품, 버전, 모조 제품의 납품
- Event-driven Malware
- 시간 변화 및 환경 변경으로 인한 악성행위 발현
- 업그레이드시 개발자의 의도적, 비의도적 백도어 삽입
- 운영자와 상호 작용없이 자동적으로 일어나는 패치
- SW 폐기시 노출되는 자격증명

권장 조치사항 가이드

- SW획득단계 보안 요구 사항의 최신화
- 모든 아티팩트가 표준화된 SBOM 포맷에 적시
- 획득/배포/업그레이드 전과정에서 무결성 검증 : Hash, Signiture, Code Sign 등
- 납품된 제품의 SBOM 검증
- SW 벤더의 Self-Attestaion 요구
- 악성 및 의도하지 않은 Site로의 접속 차단
- 업그레이드 SW 전달 경로의 무결성 확보



4. 우리군의 SW공급망 보안 대응

우리 군의 SW 공급망 보안 관련 현행 제도와 이슈 및 발전방향을 살펴본다

미국 육군의 SW 공급망 대응

미 육군은 2022년 10월 국방 조달 통한 RFI 공고를 통해 SW 공급망 보안 강화를 위한 미국내 기업의 정보 및 아이디어를 수집함

COTS(Commercial-Off-The-Shelf), GOTS(Government-Off-The-Shelf),
기타 SI업체가 개발한 SW의 보증, 위험 평가 및 완화 기술을 확보하기 위한 것

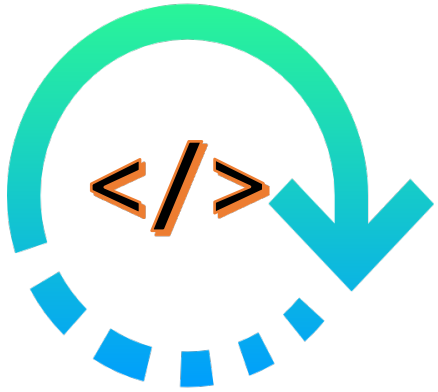
대상 SW	Request for Infomation
SW COMMERCIALS 상용 도입 SW SW GOVERNMENT 정부 보급 SW SW SYSTEM INTEGRATER 하도급개발 SW	1) 귀사는 현재 SW 산출물에 대한 SBOM을 생성하고 있습니까? · 안전한 SW 개발 프레임워크(SSDF)을 준수하기 위해 개발 활동을 추적, 모니터링? · 어떤 SBOM 양식을 사용합니까? 2) SW 공급업체와 정부사용자(군인)가 SW의 취약점에 대해 상호간 완벽히 정보를 공유하기 위한 가장 효율적인 방안은 무엇입니까? 3) 미국 육군에 적용할 수 있거나 보고할 수 있는 SW 추적 및 로깅 과정을 사용하고 있습니까? 4) 꾸준히 진하하는 취약점 공격에 대해 귀사에서 수행하는 SW 모니터링 또는 지속적인 조사 유형은 무엇입니까? (SW 유지보수 기간 동안의 SW 보증 수행 방법) 5) SBOM을 생성하고 관리하는 과정에서 귀사가 성공을 거둔 도구와 방법은 무엇입니까? 특히 SBOM 보고서를 수집, 저장, 처리, 업데이트 하는 간소화된 접근 방식을 사용하거나 알고 있습니까?

※ 이러한 조사를 통해 미국 육군의 SW 공급망 보안 강화에 세부적인 전략을 수립하고 있을 것으로 예측함

우리 군의 SW 공급망 보안 현행 정책 및 제도

우리군은 각 단계에 걸쳐 높은 수준의 보안 정책을 구현하고 있으며, 관리 대상 SW의 확대 및 SBOM의 정착 필요

개발단계



『무기체계 SW개발 및 관리 매뉴얼』

✓ 개발시험평가 14일 전 'SW목록 명세서' "SW 버전기술서'를 포함한 기술 문서 초안 제출 의무화

✓ SBOM 요구는 부재함

획득단계

[SW도입시 유해성 검증제도]

✓ 현재 반입 규정에서 SW의 유해성 검증에 대한 세부 기분 부재 하고 상용 SW는 도입/운영 단계의 검증에서 제외됨

[K –RMF]

✓ "SW 획득전략/도구/방법", "공급업체 개발 프로세스 및 시스템 심사", "공급업체 출처 정보분석" 의 항목이 존재하지만 구체적인 실행방법론이 부재함

✓ SBOM을 통한 관리 및 SW 구성요소에 대한 추출 등의 기술 방법론 정착 필요

운용단계

["취약점분석평가 " 와 "모의침투 "]

✓ SW 공급망 보안을 위한 외부에서 반입되는 상용SW 등에 대한 SBOM을 통한 관리 필요

[K –RMF]

✓ "약점/결함 처리 프로세스 명시되어 있음"

✓ SBOM등의 디지털화된 관리 방안 필요

기존 검증 시스템에서 패치가 주기적으로 발생하는 외부 반입 상용 SW에 대해서 SBOM 기반의 비교 변화 관리를 추가함

프로젝트 배경 및 목적

군 운용 SW 자산에 대해 정밀한 5단계 검증 시스템을 구축하여 운영중에 있으나 최근 급증하는 SW공급망에 선제적으로 대비 및 기존 검증 시스템의 고도화 과제에 직면함

엑스스캔 선정사유

- 적용 대상 10종 SW(3군 표준 운용 단말SW 등)에 대한 사전 검증 및 추후 확장 가능성
- 바이너리 기반 국세 표준 SBOM 생성(SPDX, Cyclone DX)
- SBOM 기반 패치파일의 변화추적에 대한 글로벌 특허 보유

핵심 요구사항 및 기능 명세

"SW공급망 보안 위협 대응을 위한 반입SW 무결성 검증 서비스"

기존 5단계 검증 시스템

기본 검증 ▶ 무결성 검증 ▶ 평판 조회 ▶ 정적 분석 ▶ 동적 분석

※ 악성코드 및 취약점 분석 관점에서 현행 가능한 모든 기술요소 채택

+α

SBOM기반 변화관리

RedPenSoft

X SCAN

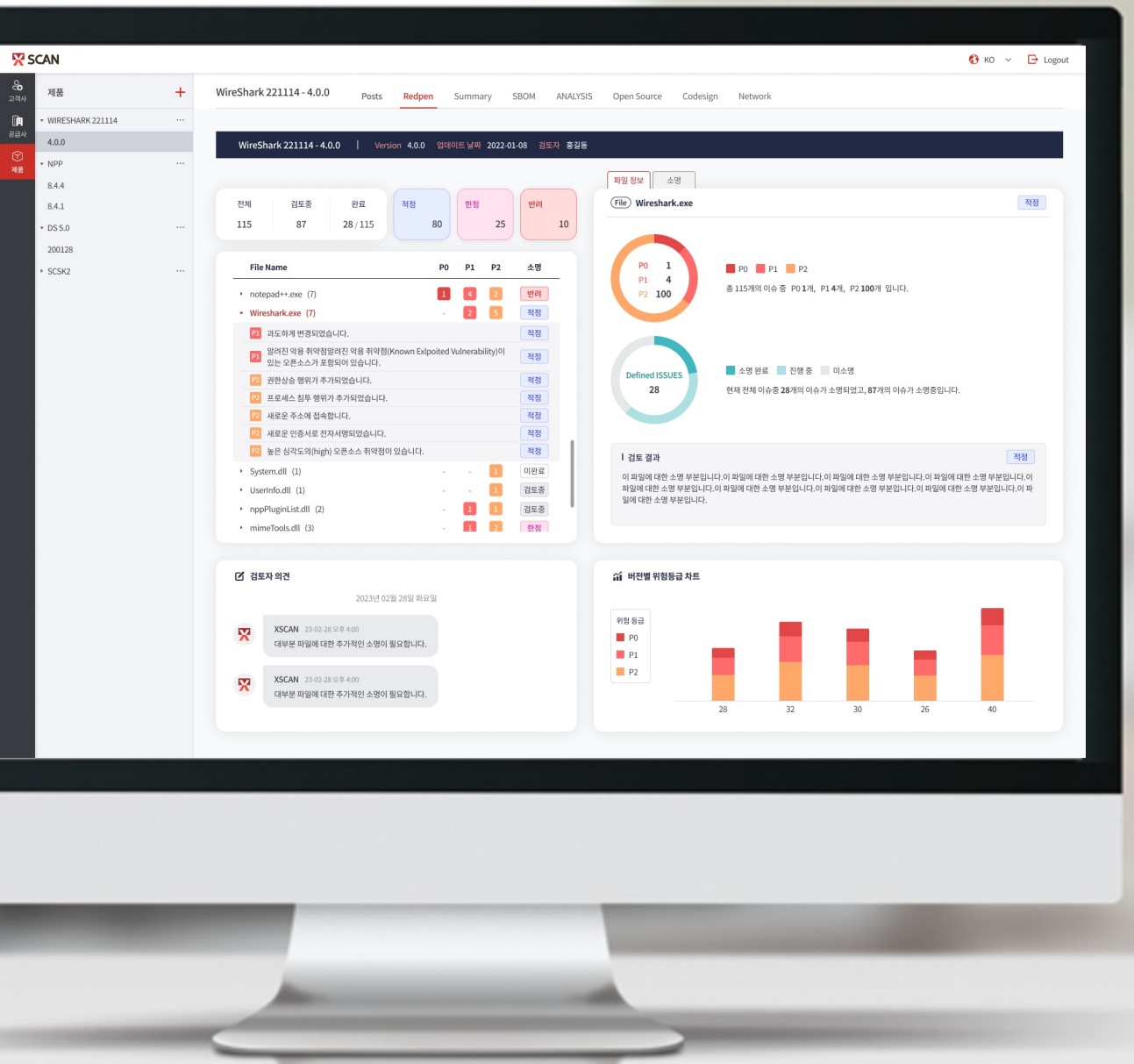
요구 기능 명세서

- 각SW별 SW공급사/수요자/검토자의 채널구성
- Open Source 뿐만 아니라 Proprietary Component 등 모든 컴포넌트 추출
- SPDX, CycloneDX 등 표준 포맷 SBOM 생성
- 이전 버전 대비 신규 버전의 변화도 비교 분석
- 코드사인 인증서 검증
- 위협 및 의심 속성 분석
- 오픈소스 코드 의존도 모니터링(취약점, 라이선스)
- SW반입 적정성 판단 및 소명 기능
- AI분석 지원 및 SW 공급사 관리 기능

5. XSCAN Introduction

XSCAN의 정의 및 차별화된
주요 핵심 기능들을 살펴보다

XSCAN 정의



01 클라우드 기반

- SaaS기반 단일한 프로세스의 구현
- On-premise 구축 가능

02 소프트웨어의 반입과 검증 혁신

- ‘SW파일 분석시스템과 분석방법’ 글로벌 특허 보유
- 오픈소스 뿐만 아니라 모든 컴포넌트 SBOM 생성

03 세계 최초 AI 자동화 기법 탑재

- ChatGPT Integration
- 발견된 위협 및 취약점 해석 및 조치 권고

04 SW공급망 위협 대응 서비스

- 자동화된 시스템과 전문가의 서비스
- 사이버보안 관제의 사각지대를 해소

발상의 전환

SW공급망 공격을 성공적으로 방어하기 위해서는 공격자의 기법을 제대로 이해하고 이에 맞설 수 있는 발상의 전환이 필요함

Zero Trust

- 무작정 신뢰가 아닌 검증하고 신뢰해야 함
- SW공급사가 침해 당할 수 있다고 가정해야 함
- 기존 악성코드 탐지 관점에서 벗어나야 함

Change Management

- SW 구성 세부 컴포넌트에 대한 심화 분석이 필요
- 이전 버전 대비 변화되는 속성(요인)에 주목해야 함
- SBOM변화, 오픈소스 변화, 인증서 변화 ...

Communication

- 의심되는 변화 요인에 대해 공급사와 소통 및 소명
- SW공급망 공격 정황에 대한 공유 및 빠른 대처 지원
- 긴급히 처리되어야 할 취약점에 대한 우선 순위 확정

ChatGPT Integration

- SIEM, SOAR등에 AI기술 접목한 보안 효용성 이미 증명
- 분석 소요 시간 절감 및 적절한 보안조치 가이드라인 생성
- 자동화 지원 프로세스로 보안 관제 효율성 강화

새로운 접근

레드펜소프트는 실제 야생에서 발생했던 글로벌 공급망 공격의 TTPs(전술, 기술, 프로시져)를 꿰뚫고 혁신적인 기반의 새로운 접근을 시도함

1 자동화 엔진

Software 컴포넌트 완전 분해

- Reverse Engineering
- Deep Binary Analysis
- Open Source Analysis

이전 버전 대비 변화 비교 분석

- SBOM 비교 분석
- Open Source 비교 분석
- Digital 인증서 비교 분석

2 세부 검증

위·변조 검증
동일명(name)의 컴포넌트가 이전 대비 크게 변화된 사항은 없는가?

의심 컴포넌트 검증
권한상승, 원격접근 등 의심되는 속성이 추가되었는가?

인증서 무결성 검증
블랙리스트, 회수된 인증서, 만료된 인증서의 사용은 없는가?

오픈소스 검증
새로 추가된 오픈소스의 취약점, 라이선스 이슈는 없는가?

3 소통 및 조치

SW 개발사의 인지
개발사는 내용을 인지 하고 있는가?

SW 개발사의 소명
의심되는 내용에 대한 소명은 적정한가?

우선순위 지정
긴급을 요하는 취약점 및 개선 사항은?

유연한 아키텍처

엑스스캔은 기존 일방적 전달에 머물렀던 SW 반입 프로세스를 클라우드에 기반하여 자동화된 검증 및 공급자 사용자가 소통할 수 있도록 아키텍처의 혁신을 달성함