


갈수록 어려워지는 오픈소스 보안, 이젠 국내에서도 관리가 필요할 때

- Log4j 보안취약점 사태를 중심으로

주식회사 스파로우 SP사업2팀 팀장 김성운

Log4j 보안 취약점

ZERO-DAY INTERNET VULNERABILITY

A grayscale photograph of a person wearing a black hoodie, sitting and typing on a laptop. The person's face is obscured by the hood.

Log4j 사태란

- 종류: 인터넷 로깅* 프로그램
- 개발사: 아파치재단
- 역할: 인터넷 사용 시 발생하는 정보 저장
- 특징: 무상 공개된 '오픈소스'
- 범용성: 세계 주요 기업 및 정부기관 사용 중
- 취약점: -특정 메시지를 입력하면 원격 침투 가능
-랜섬웨어 등 악성코드 심는 통로가 됨

*로깅: 시스템 정보를 일컫는 '로그'를 저장하는 행위

오픈소스 리스크 분석 현황



Source : MF Fortify 리서치 2019

OpenSource = everywhere



오픈소스 활용 현황

산업별 오픈소스

오픈소스가 포함된 코드베이스의 비율 ('21년 기준, 17개 주요 산업별)



84%

취약점이 최소 1개 이상 있는 코드베이스의 비율

65%

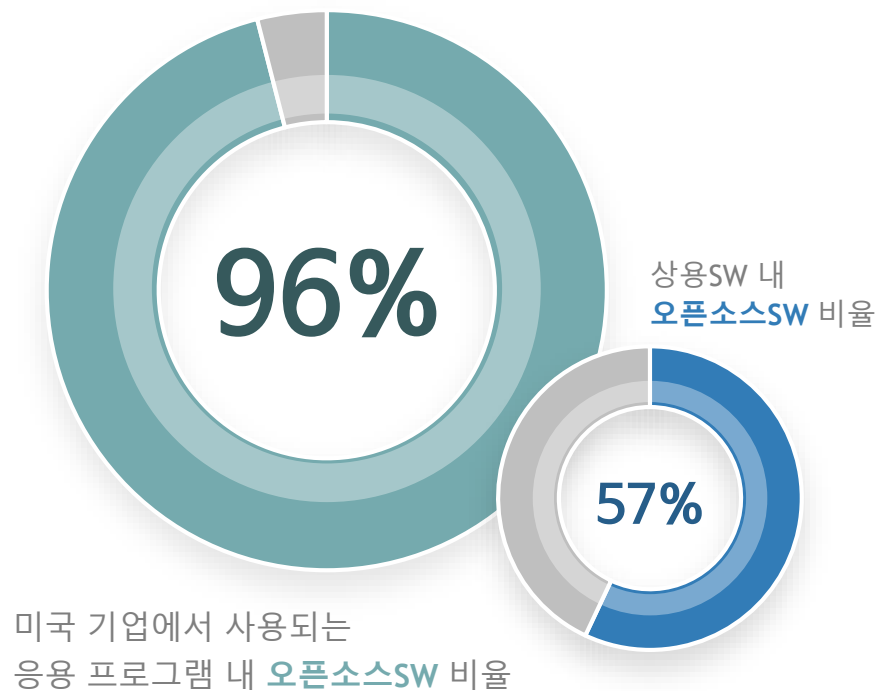
라이선스 충돌이 발생한 코드베이스 비율

75%

오픈소스로 구성된 코드베이스의 비율

Source : 2021 OSSRA Report

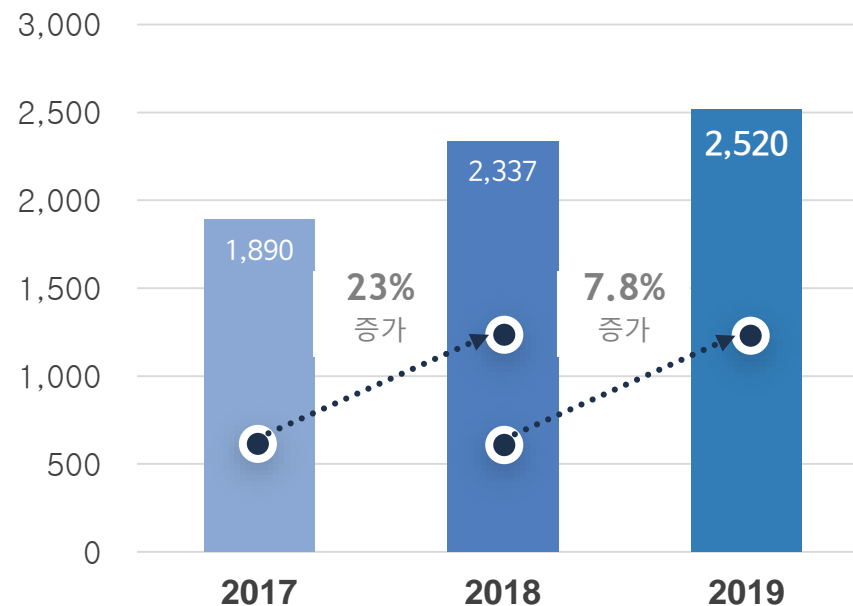
국내외 오픈소스 활용 동향



글로벌 오픈소스 활용 현황

미국 기업의 **78%**가 오픈소스 기반으로 회사를 운영
 SW가 필요할 때 **66% 이상의 기업**이 '오픈소스가 있는지'를 우선 확인
47% 기업이 자사의 툴과 프로젝트를 오픈소스로 공개

기업 오픈소스 시장규모 (단위: 억원)

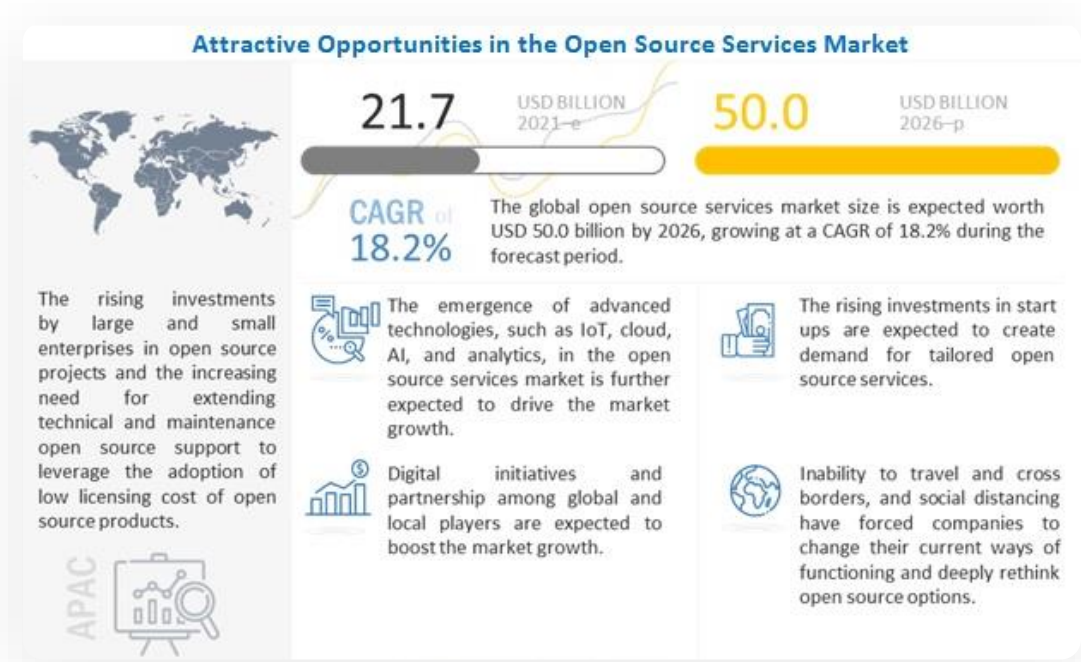


국내 오픈소스 활용 현황

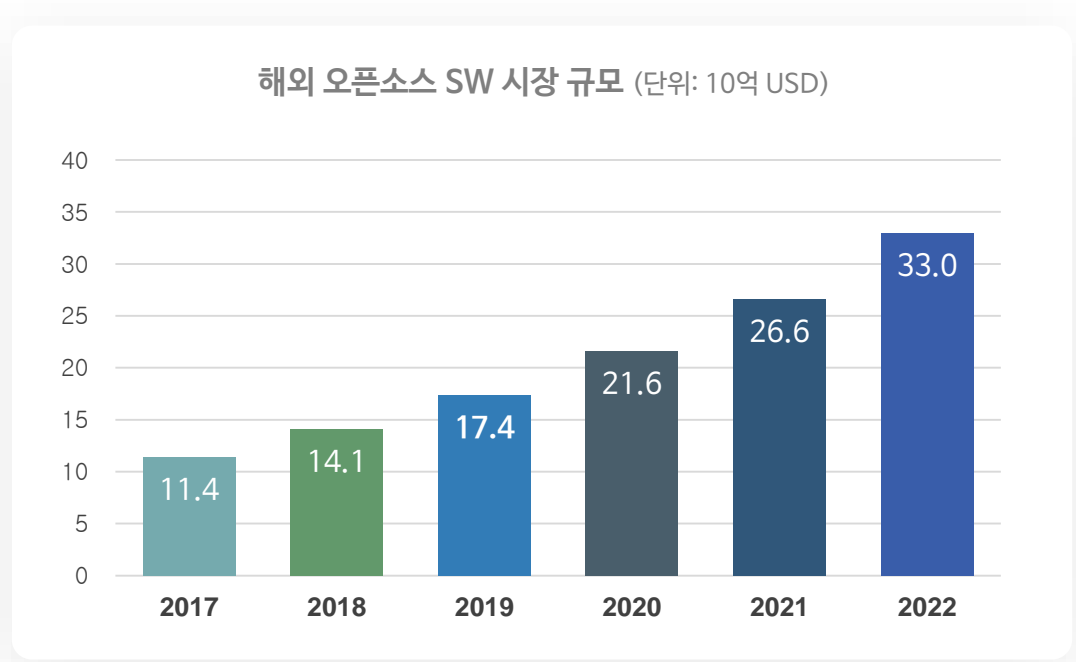
최근에는 인식(자연어·음성·이미지 등)과 딥러닝 등 **AI분야 SW**가 오픈소스로 공개 및 공유되고 있으며,
 다른 **연관 산업의 경쟁력을 강화**시키는 **핵심 성장 동력**으로 자리매김 중

국내외 오픈소스 시장 규모

4차 산업 기반에서의 오픈소스 시장 규모



COVID-19 상황에서도 글로벌 오픈소스 시장은 더욱 가속화 되는 추세임

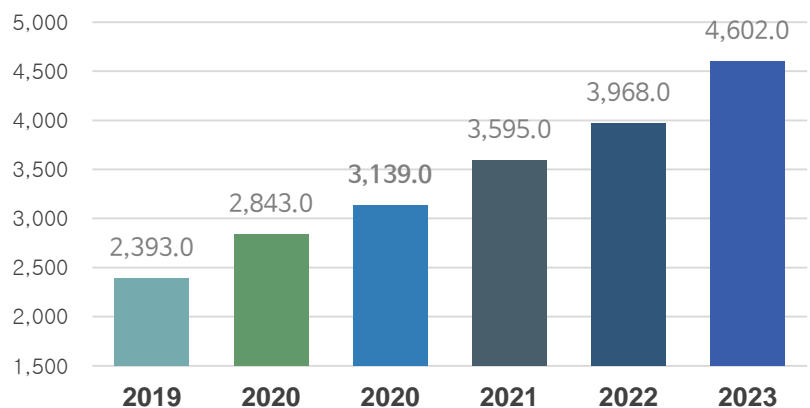


소프트웨어 라이선스 비용 감소와 관리 간소화 등으로 글로벌 오픈소스 서비스 시장 규모는 연평균 18.2% 증가하여 2021년 217억 달러에서 2026년 500억 달러에 이를 것으로 예상

국내외 오픈소스 시장 규모

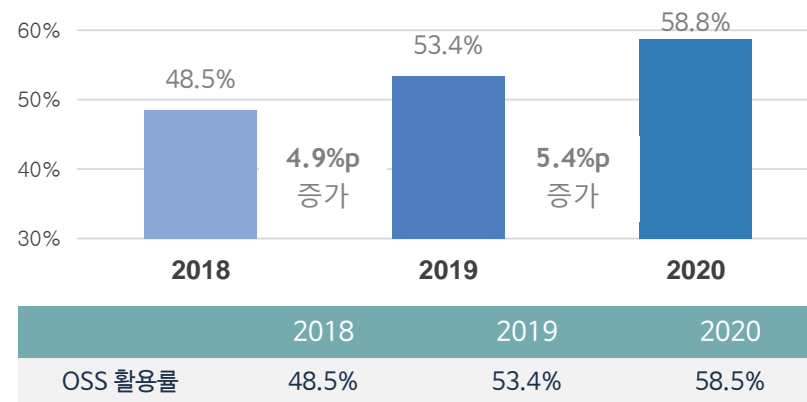
4차 산업 기반에서의 오픈소스 시장 규모

국내 오픈소스 SW 시장 규모 (단위: 억원)



Source: NIPA ('21)

OSS 활용률 추이



Source: NIPA ('21)

- 국내 기업의 OSS 활용률은 18년에 48.5%, 19년에 53.4%, 20년에 58.8%로 꾸준히 증가
- 국내 OSS 시장 규모는 매년 성장할 것으로 예측되며, 2020년 OSS 시장규모는 2019년 대비 18.8% 성장한 2,834억 원

오픈소스 관리 필요성

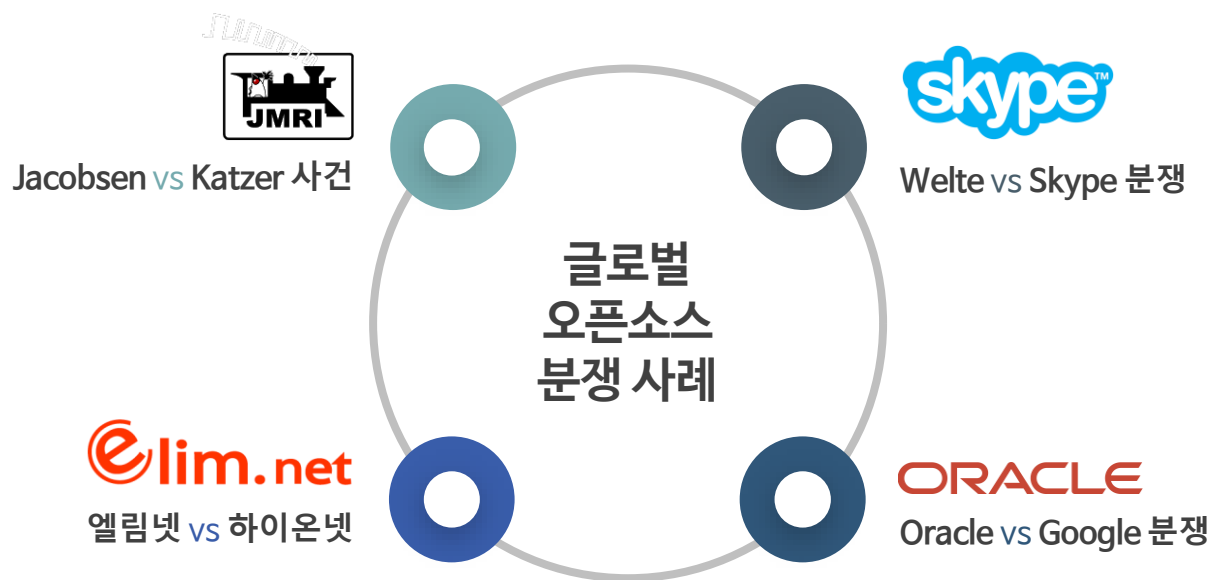
오픈소스 라이선스와 준수 의무

오픈소스 라이선스

오픈소스 라이선스란 기업 혹은 커뮤니티가 소스코드를 공개할 때 제시하는 제반(소스코드의 사용, 생산, 수정 및 배포 등) 규정

오픈소스 라이선스 분류

소스코드가 **공개되고 추가 수정 및 배포**할 수 있는 권리 및 기타 조건을 포함하는 라이선스 모델은 크게 **GPL, LGPL, MPL, BSD**로 구분

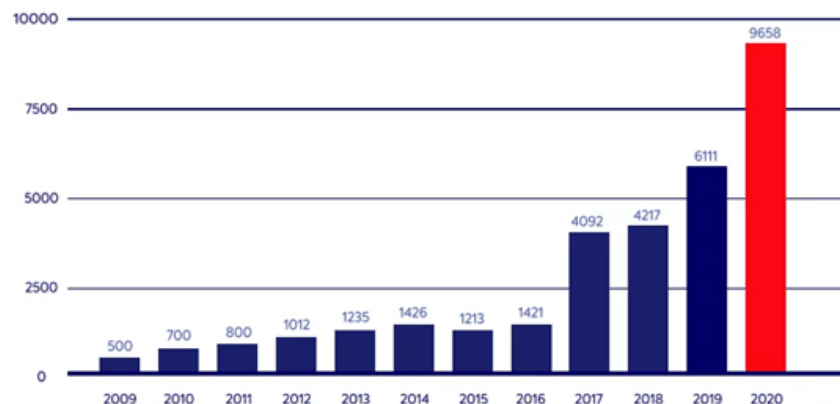


오픈소스 관리 필요성

오픈소스 보안취약점 발생 현황: 국내 대다수 기업이 수많은 보안취약점이 존재함에도 방치하는 상황

신규 오픈소스 보안취약점 발생 추이

Open Source Vulnerabilities per Year: 2009-2020



오픈소스 보안취약점
매년 큰 폭으로 증가

평균 6.6년 이상 된 오픈소스
보안 취약점을 포함

6.6

오픈소스 보안취약점
평균 수명 기간
(단위: 년)



전세계 Heartbleed
현황, 한국 2위

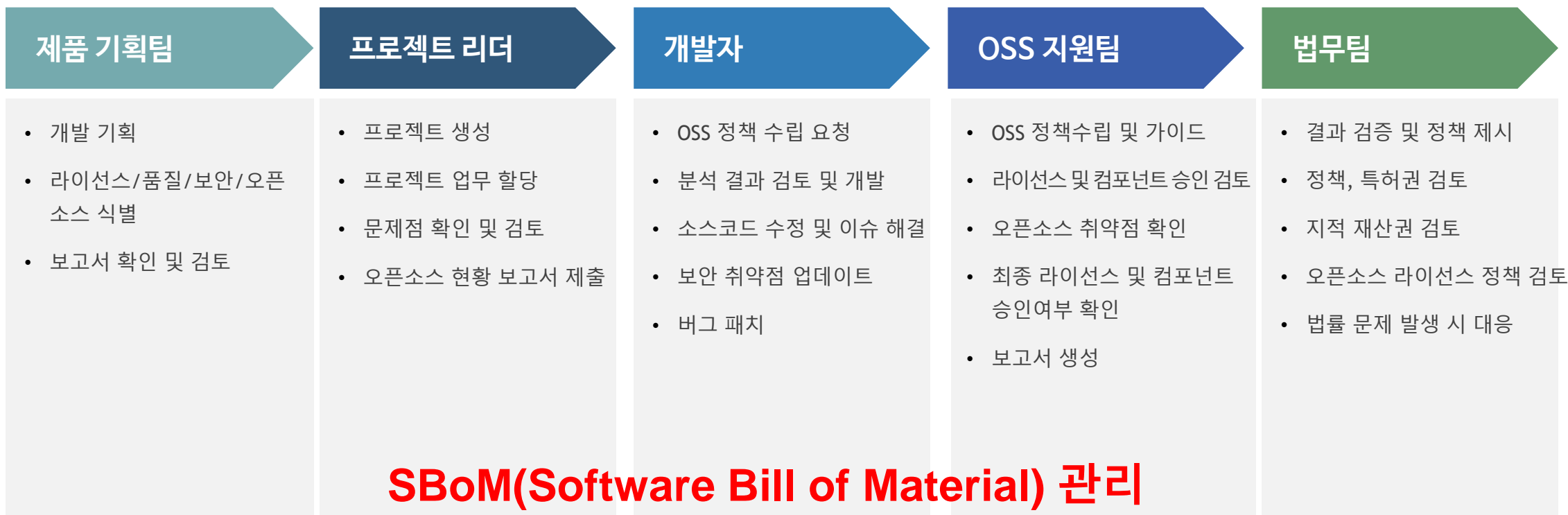
기업 발견 현황 중,
국내기업 상위권



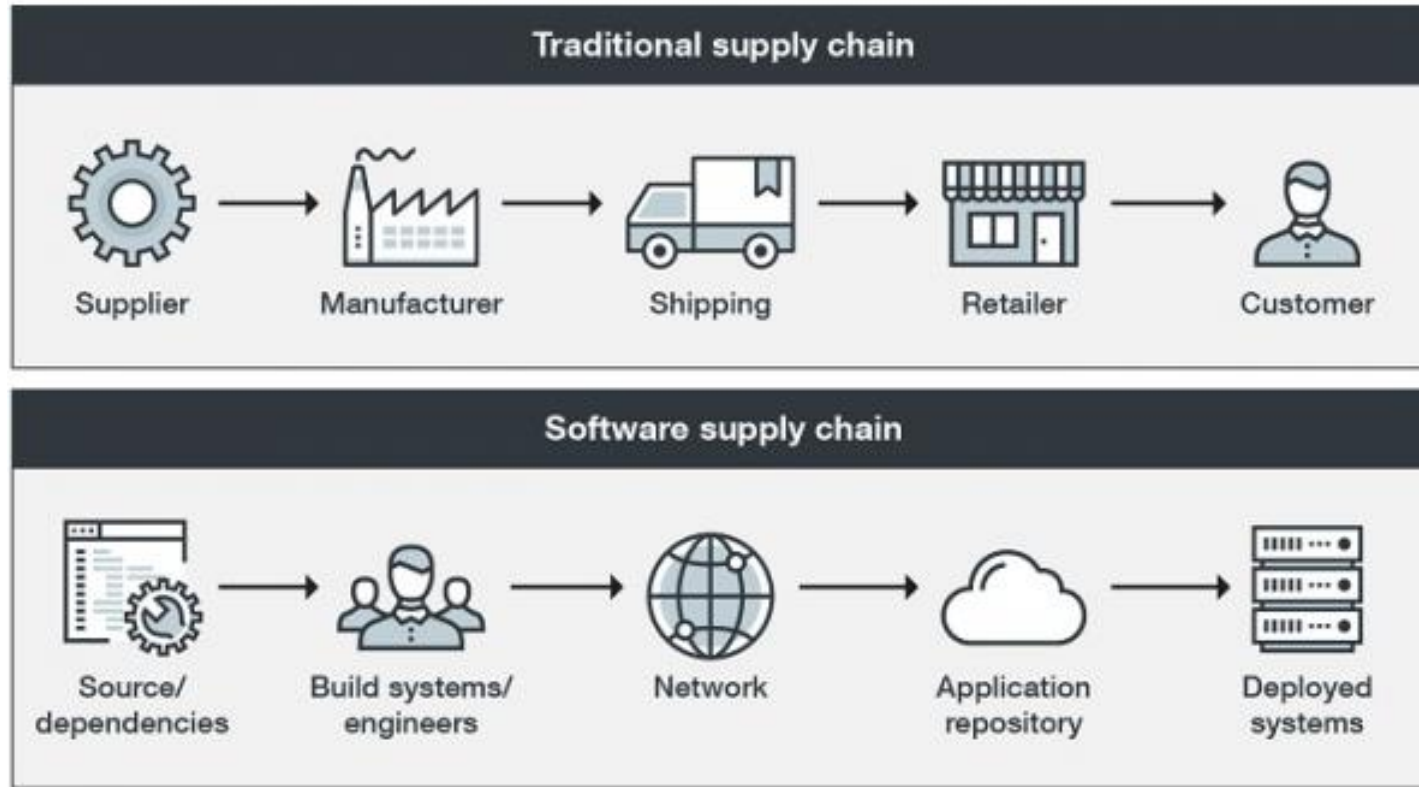
10↑

코드베이스 약 43%
10년 이상된
보안 취약점 보유

오픈소스 관리 프로세스



Software 공급망 관리



SBoM(Software Bill of Material) 관리

Thank You
감사합니다