전자정부 정보보호(eGISEC) 콘퍼런스

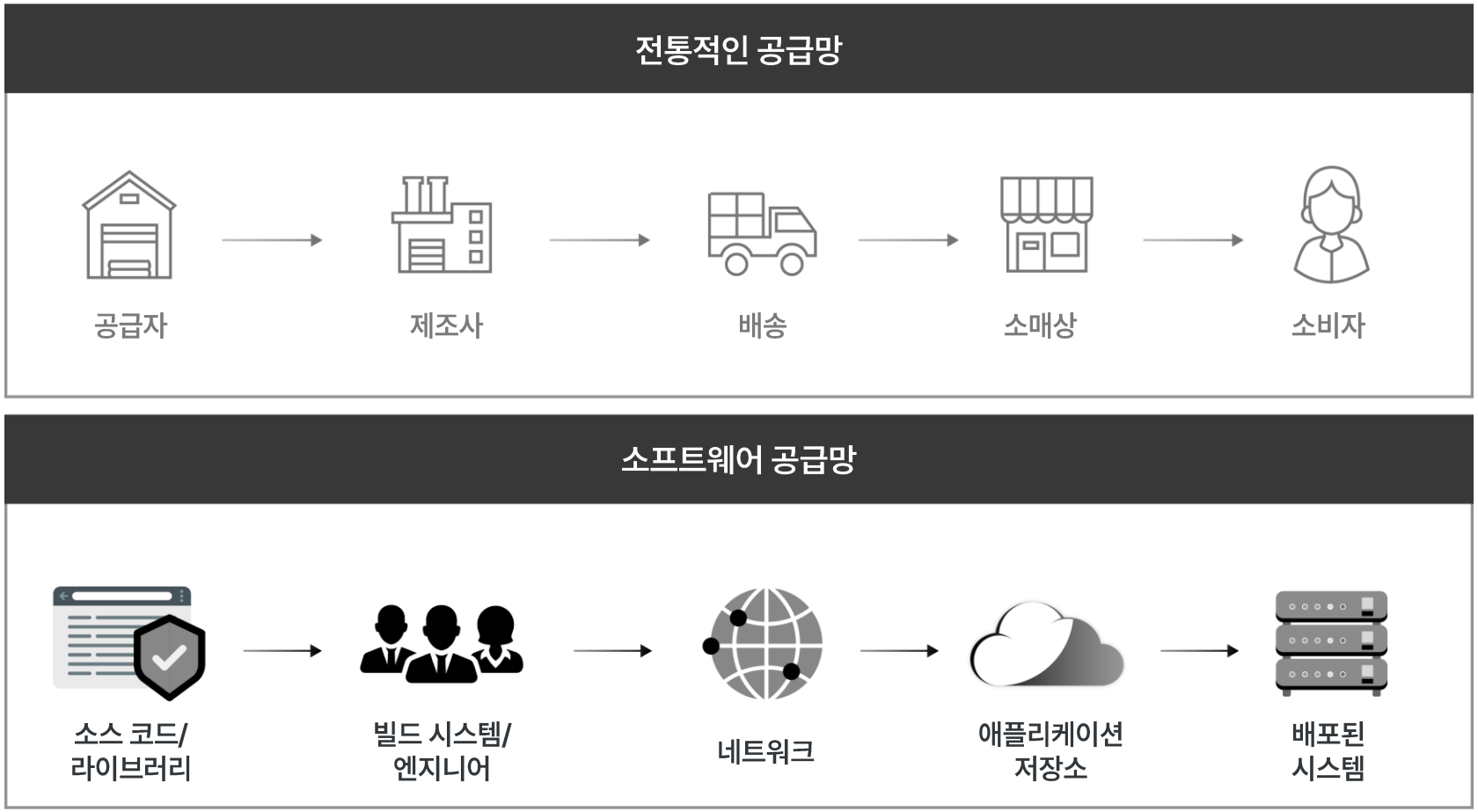
공급망 위협에 대응하기 위한 소프트웨어 개발 보안 방안

주식회사 스패로우

윤종원 팀장

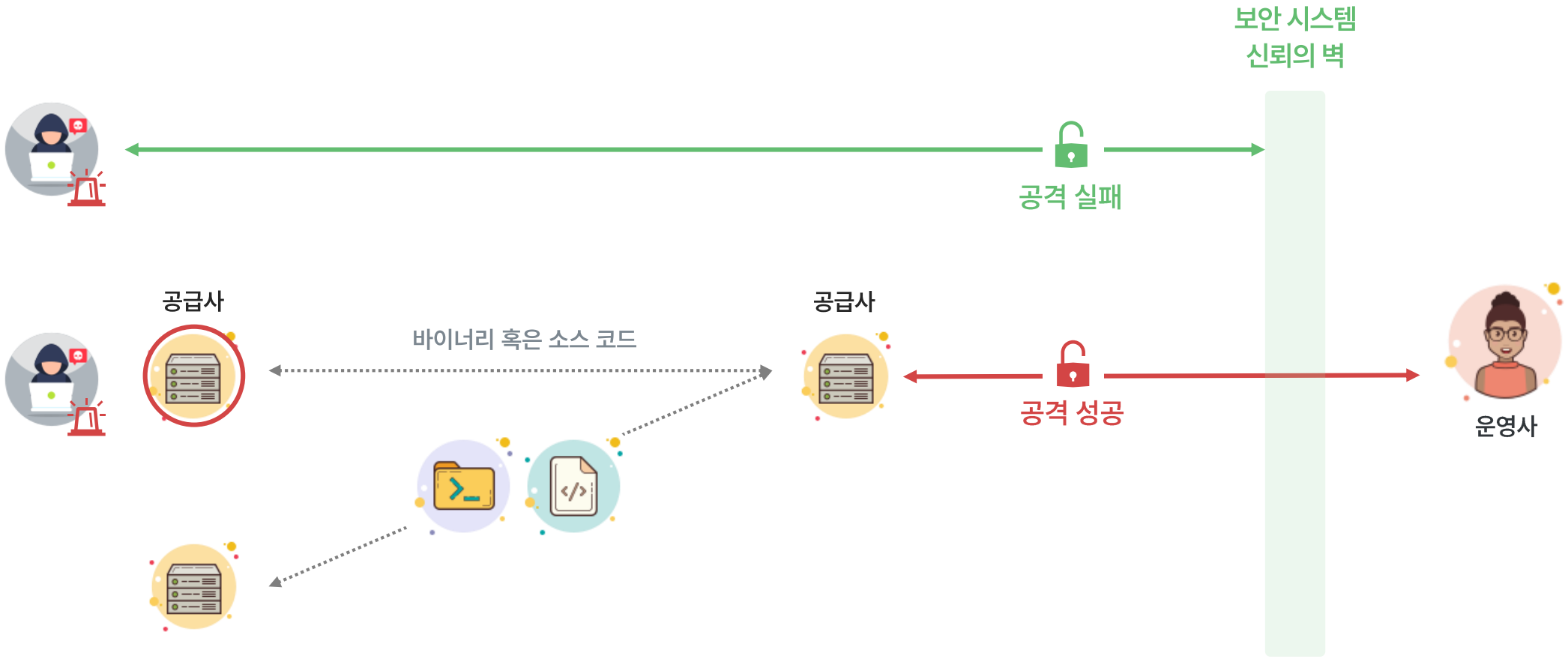
소프트웨어 공급망 (Software Supply Chain)

Sparrow



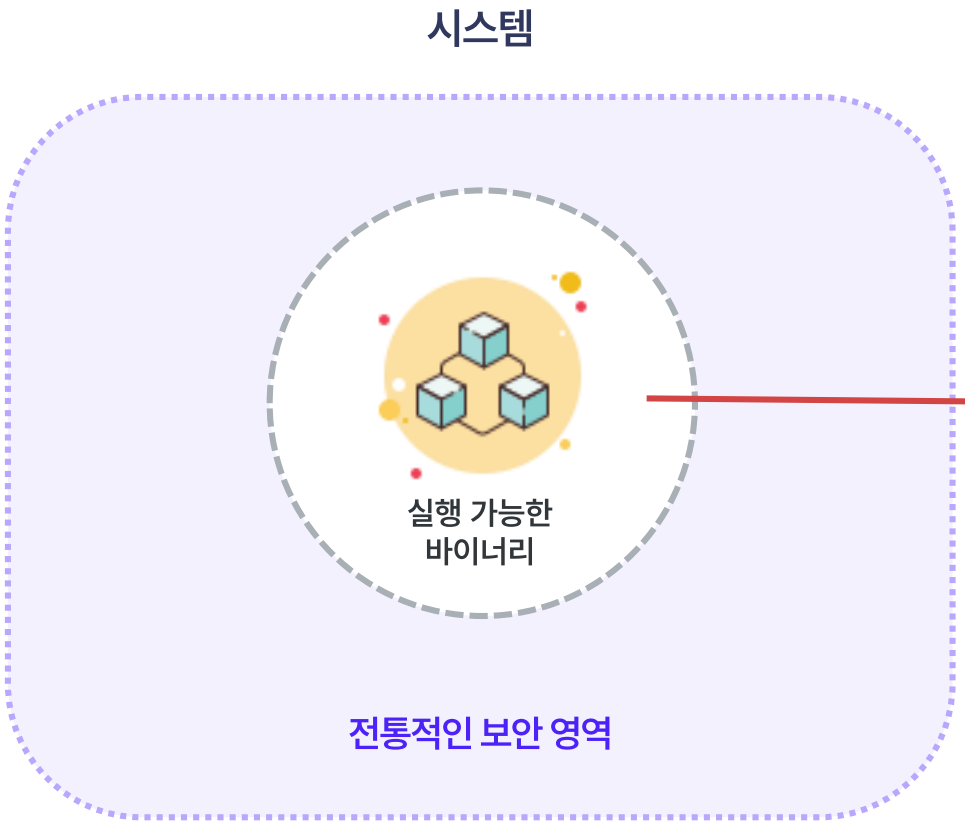
소프트웨어 공급망 공격

Sparrow



공급망 공격의 특징

Sparrow



공급받은 솔루션 내의 실행 파일,

만약 이 안에

취약점이 들어 있다면..?

공급망 위협 해결 방법

Sparrow

현실의 벽

- 도입 시 인증정보 확인,모의 해킹, 보안감사 등 보안 프로세스 적용
- 도입 시 보안 프로세스를 적용하더라도 유지보수 과정 중에는 생략하는 경우가 많음
- 솔루션 패치시마다 보안성 심의를 적용하는 것은 공급사의 큰 부담

시대 흐름의 변화

- 민간 시장의 자발적 참여에서 정부기관의 적극적인 개입으로 변화
- 무결성과 신뢰성, 책임추적성에 초점을 맞추어 공급사에게 요구하는 기조

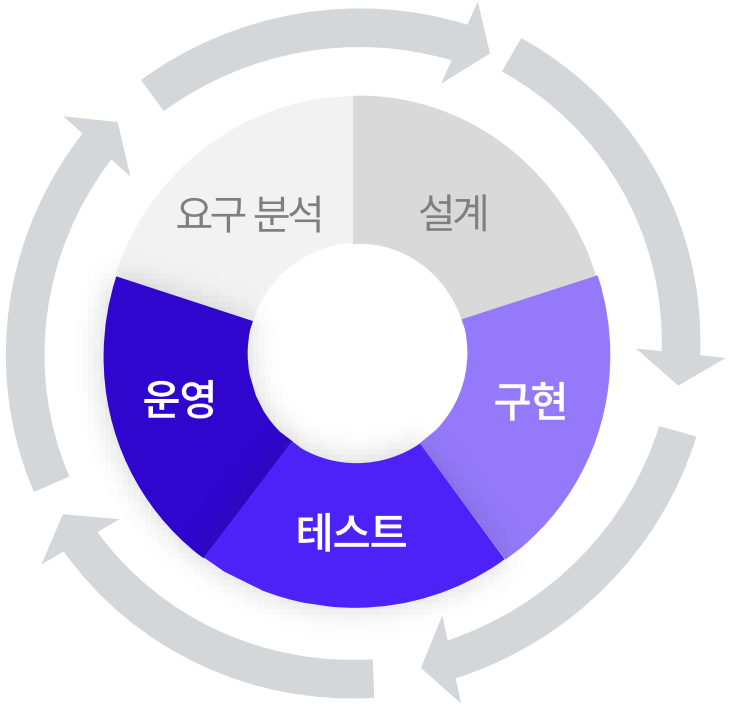
근본적인 해결책

공급사가 **생산 과정에서 보안 프로세스를 도입**, 관리해야 함

소프트웨어 개발 생명 주기 (SDLC) 와 보안

Sparrow

공급사내 빌드 서버 등
내부 시스템 보안 대책



SW 개발 과정 중
내포된 취약점 확인

릴리즈된 SW에 대한
자체 보안 감사

소스코드 보안 약점 점검

Sparrow

구분	설계단계	코딩단계	통합단계	베타제품	제품출시
설계과정 결함	1배	5배	10배	15배	**30배**
코딩과정 결함		1배	10배	20배	**30배**
통합과정 결함			1배	10배	20배

(미국 국립표준기술연구소, NIST)

소스코드에 존재할 수 있는 **잠재적인 보안 약점**을 제거

개발 단계에서부터 보안 약점을 진단하고 수정하여 투입되는 비용 절감

개발보안 관련 가이드 준수

Sparrow

오픈소스 취약점 점검

Sparrow

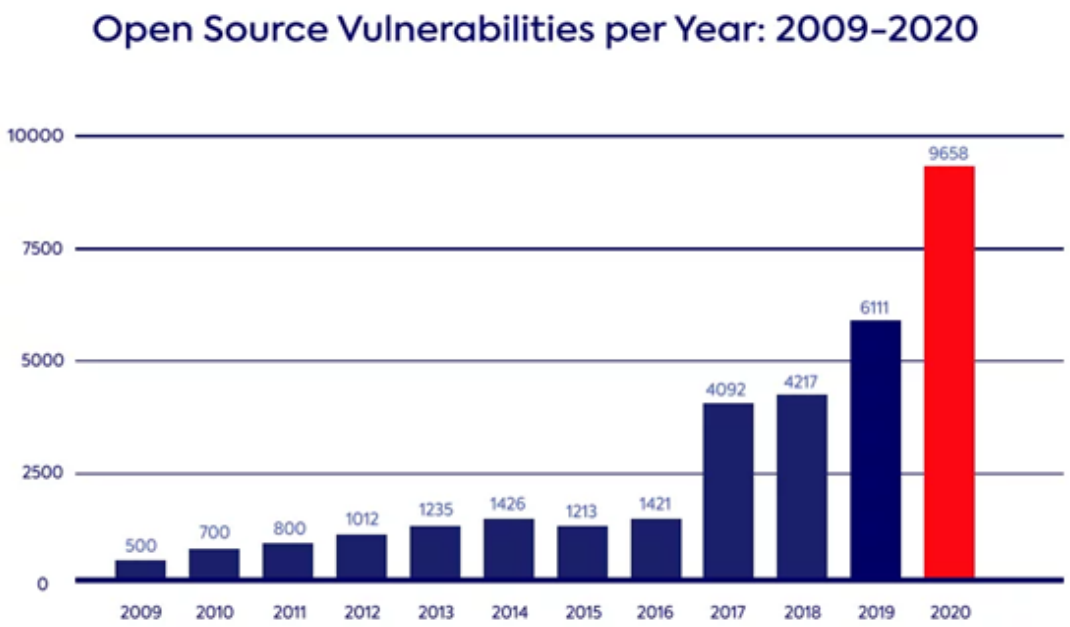
오픈소스 보안취약점 매년 큰 폭으로 증가

평균 6.6년 이상 된 오픈소스 보안 취약점을 포함

오픈소스 보안취약점 평균 수명 기간

(단위 : 년)

6.6년



<신규 오픈소스 보안취약점 발생 추이>

오픈소스 보안취약점 발생 현황:

국내 대다수 기업이 수많은 **보안취약점이 존재함에도 방치**하는 상황

전세계 Heartbleed 현황, 한국 2위

기업 발견 현황 중, 국내기업 상위권

코드베이스 약 43% 10년 이상 된 보안 취약점 보유

10↑

SBOM?

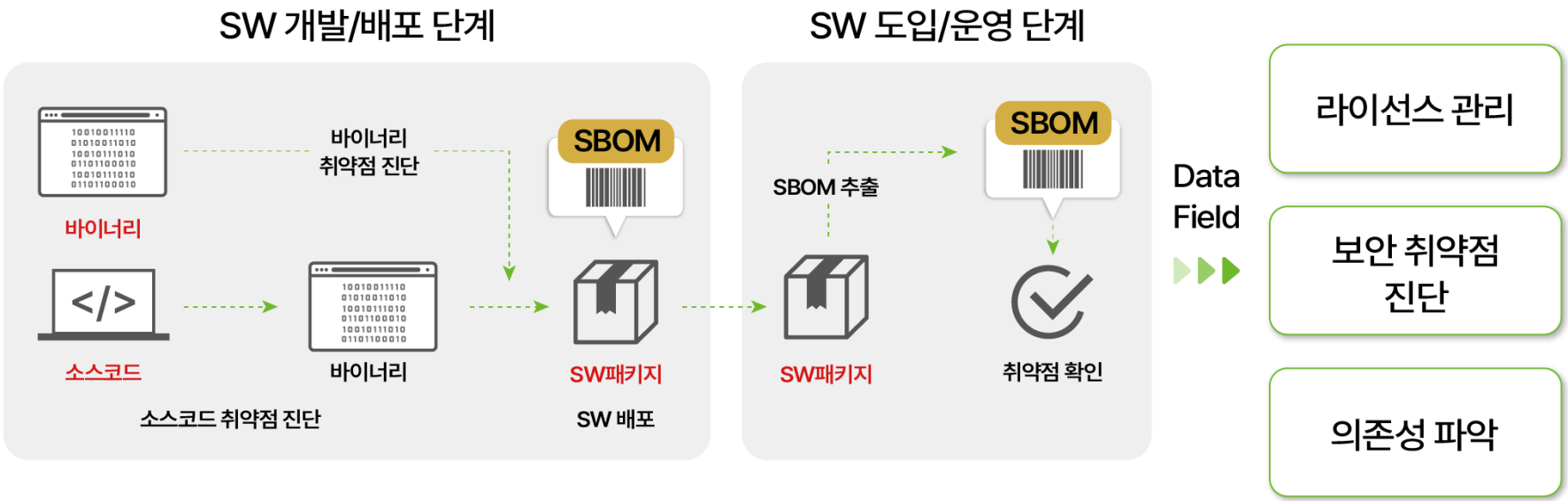
Sparrow

美 바이든 행정부 사이버보안 행정명령 ('21.5.12)

- 바이든 행정부는 보안체계 강화를 위한 행정명령 서명
- 21년 초 솔라윈즈 해킹, 미 동부 송유관 파이프라인 공격 등 발생
- 행정명령의 주요 골자는 소프트웨어 공급망 보안체계 강화
- 또한 **SBOM(Software Bills of Materials)를 도입해 소프트웨어 개발에 사용된 오픈소스나 보안 업데이트 사항을 일일이 명시**하도록 할 것.
- 포장 음식에 성분 재료가 명시되어 있듯, 정부에서 쓰는 소프트웨어가 보안 업데이트 최신 버전이며 누락된 사항 및 취약점이 없도록 하기 위함

SBOM 생성과 관리

Sparrow

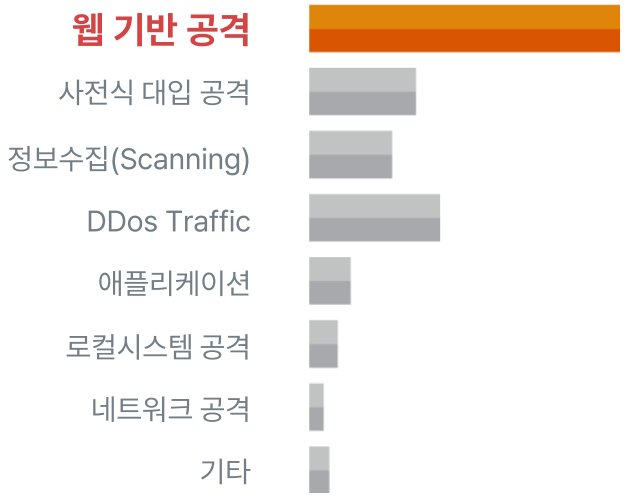


"리눅스 재단 조사, 조직의 78%가 SBOM 생성 및 활용 예정"

웹 취약점 동적 점검

Sparrow

전체 해킹 공격 가운데
웹 기반 공격이 **47.2%**로 가장 높은 비중 차지

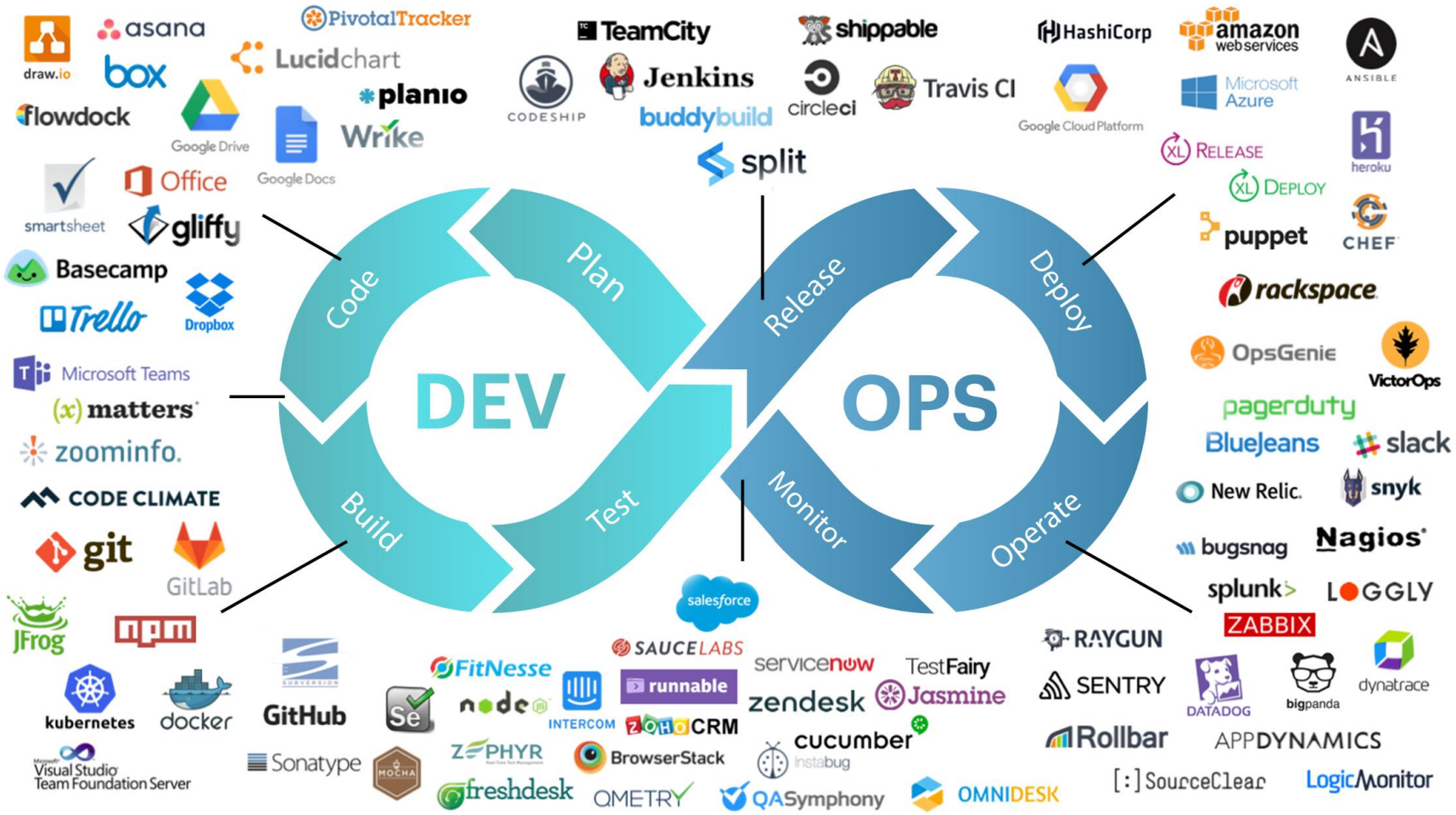


(해킹 공격 유형에 관한 보고서, 보안뉴스)

개발 단계 발견하기 힘든 **운영 단계에서 발생 가능한** 보안 취약점 검출

DevOps?

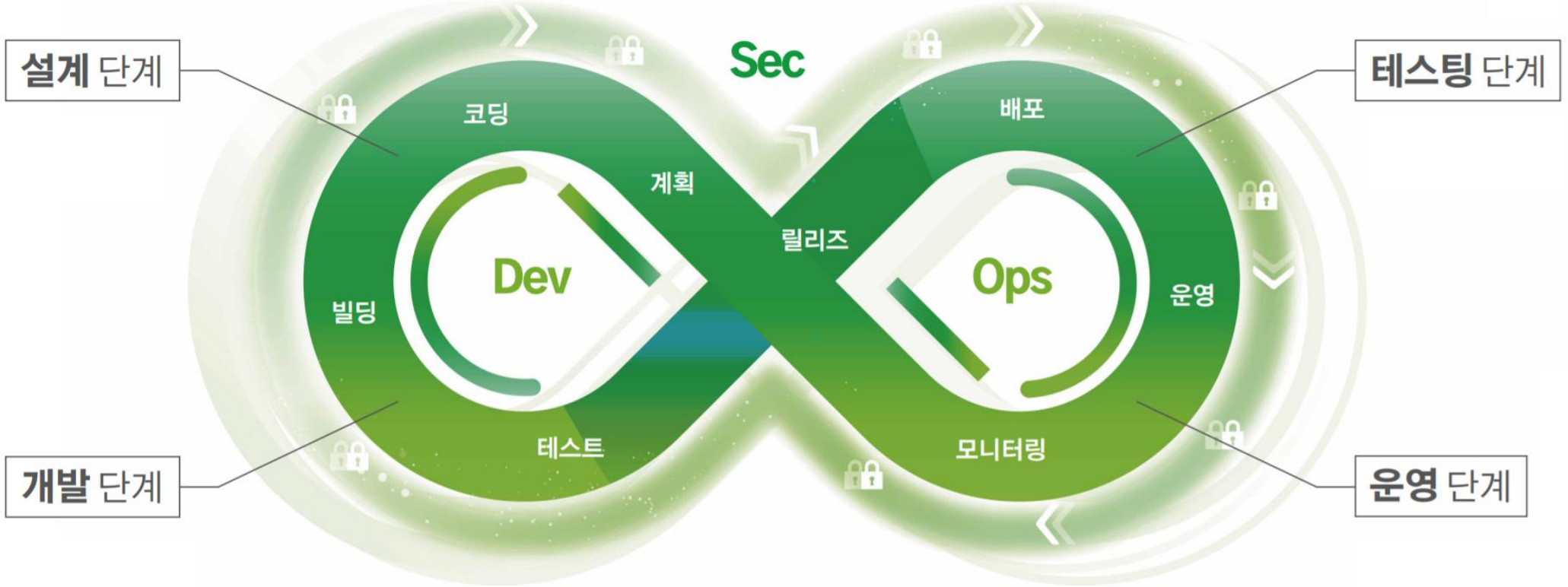
Sparrow



(DevOps tools, Openxcell)

DevSecOps!

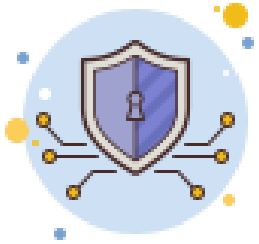
Sparrow



공급망 위협에 대응하기 위한 **공급사의 역할**

Sparrow

신뢰의 근거를 먼저 제시



자사 보안 대책 강화

안전한 소프트웨어 공급망

Sparrow

공급자

소스코드 내 잠재적인
취약점 검출

오픈소스 취약점 검출 및
SBOM 생성

실제 동작 환경에
존재하는 취약점 검출

소스코드 보안 약점 점검

오픈소스 취약점 점검

웹 취약점 동적 점검

수요자

취약점 보고서
제출 의무화

SBOM 검증 및
리스트 관리

취약점 보고서
제출 의무화

감사합니다.