SPARROW

SW 공급망 보안 강화 로드맵

고객 안내 자료

관계부처 합동(과기정통부·국정원) 「SW 공급망 보안 강화 로드맵」 2026.6.24 기반

목차

01

SW 공급망 보안 강화 로드맵: 핵심 요약

■ 왜 지금인가 — SW 공급망이 새로운 표적이 되었다

84%

취약점 포함 코드베이스

시놉시스 OSSRA 2024

$46B → $138B

글로벌 피해액 '23→'31

가트너

99%

AI 도구 활용 개발자

시놉시스 OSSRA 2024

배경

AI 기반 공격의 고도화	광범위한 취약점 탐지 & 빠른 공격 속도, 높은 파급력→ 기존 경계 기반 보안으로는 대응 한계 有
SW 공급망의 복잡·불투명화	공개SW·타사SW 활용·AI 생성 코드·제3자 개발 확대로 개발주체와 책임이 불명확해짐
SW 공급망 보안 = 무역장벽	美·EU 등 주요국은 개발·공급자의 책임 강화 및 지속적 사후관리 요구하고 있음

■ 시사점 및 추진 방향

운영 단계에서 개발·공급 단계로 확장되는 위협 — SW 공급망 全 단계의 보안·투명성·복원력 확보가 필요함

	현황 및 문제점	대응 방향
개발·공급 단계 위협 증가 예방	• 개발 단계를 노린 공격에 취약 • 복잡해진 SW 공급망 • 기능·성능 중심의 개발 관행	→ • **개발·공급기업의 보안 내재화 지원** • **SBOM 활용 공급망 투명성 확보** • **보안 중심 개발문화 정착**
피해 확산 방지 미흡 복원	• 초기 탐지의 어려움 • 2차 피해로 연쇄 확산	→ • **위협정보 발굴 체계 다각화** • **공급망 참여자 간 보안정보 공유·협력체계 마련**
공급망 보안 기반 부족 기반	• 공급망 보안 관련 기준 부재 • 전문인력 부족 • 시험·점검 환경 부재	→ • **공급망 보안 원칙·가이드라인 등 개발** • **전문인력의 공급망 보안 역량 강화** • **공급망 보안 테스트베드 조성**

예방 안전하게 개발하고 책임 있게 공급하는 보안 내재화 촉진

복원 공급망 가시화를 통한 신속한 복구·대응 체계 마련

기반 사이버 복원력 확보를 위한 정책·제도적 기반 조성

■ 비전 · 3대 전략 · 9대 과제

비전 안전하고 책임 있는 공급망 보안 체계의 전환을 통한 **사이버 복원력 확보**

가. 예방 역량 강화

① 공급망 전주기의 보안 내재화 지원

② SW 공급망의 투명성 제고

③ 보안 중심 개발 문화 정착

나. 신속 탐지·대응

④ 공급망 위협정보 모니터링·탐지 강화

⑤ 공급망 보안 위험관리 체계 구축

⑥ 신속한 피해확산 차단

다. 정책·제도 기반

⑦ 정책 추진체계 구축

⑧ 법·제도 정비

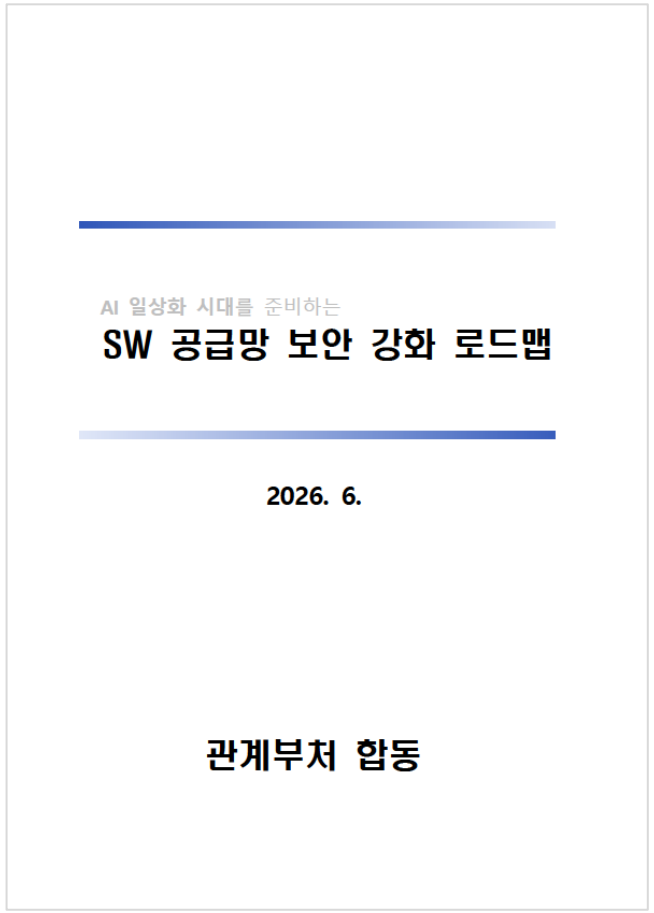
⑨ 글로벌 협력 확대

02

전문 요약: 세부 추진 과제

■ 전문(원문) 다운로드

본 자료는 핵심만 요약한 고객 안내용이며, 자세한 내용은 원문을 참고하세요.


AI 일상화 시대를 준비하는

SW 공급망 보안 강화 로드맵

2026. 6.

관계부처 합동

전문 다운로드

「AI 일상화 시대를 준비하는 SW 공급망 보안 강화 로드맵」

관계부처 합동(과기정통부·국정원) · 2026.6.24

다운로드 ↓

가. SW 공급망 위협 예방 역량 강화

1. 공급망 전주기의 보안 내재화 지원

SW 생애주기별 공급망 보안 기준·가이드 개발

- 설계·개발·테스트·배포 전 주기에 적용하는 '안전한 SW 개발 방법론' 제시 (美 NIST SSDF 참고)
- 실무 중심의 가이드라인 2.0 개발 - 기존 1.0(인식 제고)을 현장 적용형으로 개선
- 기존 개발보안 가이드라인 개정 – SW 공급망 보안 요소 보완·고도화
  (SW개발보안가이드, 언어별 시큐어코딩 가이드 등)

SW 보안 수준 시험·점검 제공

- 정적·동적 분석·공개SW 사용현황 등 SW 공급망 보안점검 테스트베드 구축 (개발보안허브·NCSC 활용)
- 판교·부산 지역정보보호클러스터 활용 → 광역권 단위로 점진적 확대
- (온라인 지원) 비대면 점검('27~) + SW 개발 보안 포털(가칭): 대응방안·질의응답·취약 SW 정보 제공
- (AI 점검 인프라) 고성능 AI 모델 활용 취약점 점검·전문가 조치 지원('27~)

SW 공급망 보안점검 시험환경(예시) - 점검항목

1. SBOM 생성 및 보안취약점 점검 지원
2. 개발공급기업 보안 내재화 점검 지원
3. IoT 기기, 융합산업 제품 등 공급망 보안점검 및 컨설팅 지원
4. 의료기기 인허가, EU CRA법 등 글로벌 규제 점검 지원

기업의 안전한 개발·공급 환경 전환 지원

- (컨설팅) 개발 인프라·관리체계 진단 등 전문 보안컨설팅 추진('26~)
  - 개발 인프라 구성·보안 정책 적절성·보안 취약점 식별·조치 등 환경분석 및 진단 지원
- (솔루션 도입 지원) 소규모 SW기업 대상 개발환경 개선 지원('27~)
  - 보안 전담 인력이 없는 소규모기업에 클라우드 기반 개발환경 보급·보안 솔루션 도입·전환 지원

2. SW 공급망의 투명성 제고, 3. 보안 중심 개발 문화 정착

SW 공급망 투명성 제고

SBOM 기반의 SW 공급망 보안 관리 모델 적용·확산

- SW 공급망 보안 모델 구축을 통한 보안 위협 추적·관리 지원('26~)
- 우선 지원 대상 - 주요국 제도화 대상 수출기업 및 파급력 높은 분야
  - 수출기업: 美 FDA 의료기기 인허가 시, 美 상무부 커넥티드카·자율주행 SBOM 관리의무
  - EU 사이버복원력법(CRA) - '디지털 요소가 있는 기기' SBOM 관리의무
  - 파급력 높은 분야: 보안 SW, 금융·교통 등 사회기반 SW, 건강·의료 등 민감정보 관리 SW
- 산업별 특성(주 사용 공개SW·언어·규제)을 고려한 보안 모델 발굴·모범사례 확산

SW 공급망 보안기술 고도화

- (SBOM 기술) 접근성·활용성 제고 위한 기술 고도화('26~)
  - 신뢰도: SBOM 정확도·적용범위 검증, 수정 이력 관리
  - 자동화: 생성·검증·분석·대응조치까지 자동화
  - 보관·유통: SBOM 내 민감정보(취약점 등) 안전 유통
- (신기술 대응) AI 등 SW 공급망 보안 모델 연구·실증 추진('27~)
- (보안 운영 재설계) 경직된 프로세스(사람 중심의 SW 취약점 탐지 및 수동 대응)
  → AI 중심 자율체계로 전환

보안 중심 개발 문화 정착

이해관계자별 맞춤형 인식제고

- 보안이 '동반기술'로 인식될 수 있도록 보안 중심의 개발 문화 확산 지원
- 경영진·개발자·운영인력 등 전 구성원 대상 맞춤형 인식 제고 활동 확대
- SW 인재 양성 교육 과정에 공급망 보안 기본 교육 반영('26~)
- 산·학·연·관 협력을 통해 캠페인, 컨퍼런스 등 홍보 활동 추진('26~)

SW 공급망 보안 전문기업·인력 양성

- (전문기업 육성) SW 공급망 보안 전문서비스 기업 육성·지정('27~)
  - 정보보호 전문서비스 기업 제도 개편
  - 취약점 분석 평가 및 보호 대책 수립 등 수행 기업 지정
- (전문인력 양성) 사이버보안 인재 양성 사업 연계 교육과정 개발·양성('26~)
  - 자동차, 의료기기 등 SW 공급망 보안 규제 강화 특정 산업의 경우, 특화 교육 및 프로그램 마련

4. 공급망 위협정보 모니터링·탐지 강화, 6. 신속 피해확산 차단

보안취약점 발굴·조치 활성화

- 버그바운티·CVD/VDP 등 취약점 발굴 채널 확대
- 국민 사생활·국가경제 중요성이 높은 디지털 제품군 보안 실태점검 추진('26~)
- (미흡기업) 후속 조치 미비 기업·제품 공공분야 도입 제재 강화('27~) - 보안 패치 및 조치 완료 시까지 공공조달 일시 제한

위협 정보 탐지 ·발굴 다각화

- AI 기반 실시간 모니터링·자동화 체계 개발·전환('28~)

- AI 기반 탐지체계 운영을 통해 은닉된 위협 발굴('26~)
- Date Lake에 축적된 다양한 위협 정보 간 연관 분석 및 AI 기반 실시간 분석 기능 접목
- 신속한 복원력 확보를 위한 AI 기반 방어체계 구현('27~)

- 美 CVE 프로그램 종료 대비 대체 위협정보수집 채널 확대('26~)

안보위해 제품 대응 체계 마련

- 민·관·군 '안보위해 평가 협의체' 운영, 자가점검 체크리스트('27~), 공공분야 납품 시 안전성 확인 강화('28~)

신속한 피해확산 차단

- SW 공급망 침해사고·위협정보 발견 즉시 민·관 전파 절차 마련('26~)
- NCTI·KCTI·C-TAS 등 위협정보 공유 시스템 활용, SW 공급망 위협 경보·확산방지 체계 운영('28~)

5. 공급망 보안 위험관리 체계 구축

공공·민간 양측의 SBOM 관리와 취약점 대응 체계를 구축합니다.

'26~

공공 분야

- 공공분야 SBOM 관리체계 개발('26~)
  - SBOM 항목 도출·표준화, 생성·공유·교환 방식, 접근통제, 통합관리 절차 마련
- SBOM 신뢰성 보장방안 마련('27~)
  - 취약점 영향도 분석(VEX) 등 기밀성·무결성·가용성 확보 기술
- SBOM 통합 관리 시스템 구축('26~)
  - 등록·관리, 위험 실시간 모니터링·공지
  - 보안기능 시험 및 보안적합성 검증필 제품 SBOM 관리
- 취약점 정보 DB 구축('28~)
  - SBOM 통합 관리 시스템과 연계해 취약점 조치 정보 등록·공유·이력 관리

민간 분야

- 고위험 취약점 포함 여부 상시 관리체계 도입·운영('26~)
  - 중대(Critical) 취약점·신규/은닉형 악성코드 등을 고위험으로 분류·관리
- SBOM 데이터 수집·SW 공급망 위험 경보 시스템 구축·운영('27~)
- SW 자산식별·위험요소 분석 기반 보안 조치 수행('28~)
- C-Clean 서비스 지원('28~)
  - 기업·이용자 PC 대상 취약 SW 실시간 탐지·제거 및 패치 안내

■ 고위험 취약점 점검 및 경보 시스템 – 예시

출처: 관계부처 합동 'SW 공급망 보안 강화 로드맵'(2026.6) 〈그림 11〉 재구성

다. 정책•제도적 기반 조성

7. 정책 추진체계 구축, 9. 글로벌 협력 확대

범정부 정책협력체계 구성

- (가칭) 범정부 정책협력체계 구성 - 사이버보안 유관부처·전문기관(KISA·금융보안원 등) 참여('26~)
  - 분야별로 산재된 사이버보안 제도 및 부처·유관기관 간 협업 강화 방안 마련

민간 자율 활동 지원

- 민·관 합동 포럼 및 산업별 자율협의체 운영 — 보안 수칙 개발·확산·점검('26~)

글로벌 협력 확대

- 美 CISA·GGEF 등과 위협정보 공유 및 공동 가이드라인 협력체계 강화('26~)
  - 국경 없는 공급망 위협에 대한 취약점 등 위협정보 지속 공유·공동 대응
- 해외 규제(CRA·FDA 등) 대응 지원 및 인증 상호인정(MRA) 확대 추진('26~)
  - 국가별 인증제도 특성 분석 기반 분야별 무역장벽 극복 컨설팅 제공

다. 정책•제도적 기반 조성

8. 법·제도 정비

개발·공급부터 사후관리까지, 민간·공공 제도를 정비합니다. (로드맵상 추진 계획 - 연도는 시행 예정 시점)

공공 분야

- 정보시스템 보안 절차·위험관리 절차서 마련('27~)
  - 공공분야 정보화사업 추진 시 SBOM 제출·취약점 대응 절차 도입
  - 공공분야 도입 SW > SBOM 제출 및 보안취약점 관리 담당관 지정 등 지침 개정
- 보안적합성 검증 개선('26~)
  - 보안요구사항 개선·검증 대상 제품 점증 확대('27~)
  - 국가용 보안요구사항 기능단위 세분화
  - SBOM 제출 및 SW 공급망 보안 검증 요건 > '안전한 SW 개발 방법론' 준수 확인('27~)

민간 분야

- SW 공급망 보안관리 검증·우수기업 확인서 시범운영('27~)
  - (가칭) SSS Verified — 자율 신청 기반, 美·EU 상호인정 추진
- 기존 정보보호 인증제도(ISMS·CSAP·IoT)에 SW 공급망 보안 평가요소 반영·정규 제도화 추진
- 사후관리 책임성 제도 개선('27~)
  - SW 생명주기 전체의 지속적 보안을 위한 인센티브 근거 마련 + 취약점 미조치 시 시정권고

03

우리 조직은 무엇을 준비해야 하는가

■ 규제 타임라인 — 2027년, 준비는 지금부터

국내 제도화는 2027년에 집중 시행되며, 특히 수출 기업은 해외 규제가 사실상의 진입 조건이 됩니다.

	'24	'25	'26	'27	'28~
해외 규제	**英 PSTI 시행** ('24.4) **EU CRA 공포** ('24.12) **美 Cyber Trust Mark** ('24.3)			**EU CRA 시행** ('27.12, SBOM·취약점 관리 의무)	
국내 제도화			**보안적합성 검증** SW 공급망 평가기준 반영 **국내 인증제도 상호인정(MRA) 확대 추진** EU·英 등 사이버보안 관련 제도 강화 대응	**'27~ 집중 시행** • 침해사고 및 보안취약점 발견 이후 보안 패치/신속한 조치 필수 • SSS Verified 시범인증 • 공공 정보시스템 보안 절차 • 위험관리 절차서 • 사후관리 책임성 제도 • SBOM 제출·개발방법론 준수	**정규 인증 제도화** (ISMS·CSAP·IoT 내 공급망 보안 시험평가 요소 반영)

■ 분야별 대응 포인트 — 우리는 어디에 집중해야 하나

개발·공급	도입·운영
개발 단계 보안 내재화 (정적/동적 분석)	정보화사업에 SBOM 제출 및 취약점 대응 요건 대비
SBOM 생성·관리로 구성요소 가시성 확보	보안적합성 검증 강화 대응
오픈소스 취약점·라이선스 관리 체계	공급망 사이버보안 위험관리 절차 준수
출시 후 사후관리(패치·EoS 공지) 프로세스	SW 보안취약점 관리 담당관 지정
(수출)CRA·FDA·SBOM 등 해외 규제 대응	도입 제품의 안보위해성·취약점 상시 점검

■ 지금 점검해야 할 6가지

아래 항목 중 '아니오/모름'이 있다면, SW 공급망 보안 대응을 지금 시작할 시점입니다.

1 개발 단계 보안

정적(SAST)/동적(DAST) 분석이 개발 파이프라인에 내재화되어 있는가?

2 SBOM 관리

우리 SW의 구성요소(오픈소스·서드파티)를 SBOM으로 파악하고 있는가?

3 오픈소스 위험

사용 중인 오픈소스의 알려진 취약점·라이선스를 지속 관리하는가?

4 AI 생성 코드

AI가 생성한 코드의 보안 취약점을 검증하는 절차가 있는가?

5 사후관리

출시 후 보안 패치·취약점 대응·지원종료(EoS) 공지 체계가 있는가?

6 규제 대응

(수출 시) CRA·FDA 등 해외 규제 요건에 대응할 수 있는가?
(공공기관 납품 시) 보안적합성 검증 강화 및 SBOM·취약점 요건에 대응할 수 있는가?

04

스패로우의 대응 전략

■ 개발부터 운영까지 — SW 공급망 보안 전방위 지원

◈ 사업 영역

Application Security
애플리케이션 보안

SW Supply Chain
SW 공급망 보안

◈ 주요 제품

Sparrow Enterprise	애플리케이션 보안 테스팅 통합 솔루션
Sparrow SecureHub	SBOM 공유 및 관리 플랫폼
Sparrow MCP	AI 생성 코드 보안 어시스턴트

◈ 핵심 경쟁력

1 안전한 SW 개발·공급을 위한 Full Line-up 보유

정적·동적 분석, SW 구성요소 분석 등 SW 개발 전반의 보안 취약점을 분석하는 통합 플랫폼과 SBOM 생성·안전한 유통 제품 보유

2 다수의 정부지원사업 수행

- SBOM 실증사업·전자정부진단사업 등 정부지원사업 수행사로 선정
- SW 보안약점 진단원, 모의해킹 인력 등 우수한 개발·보안 역량 보유

3 다양한 인증 및 특허 획득

- 29건의 국내외 애플리케이션 보안 특허 보유
- GS·CC·CSAP·ISO26262 등 다양한 인증 보유

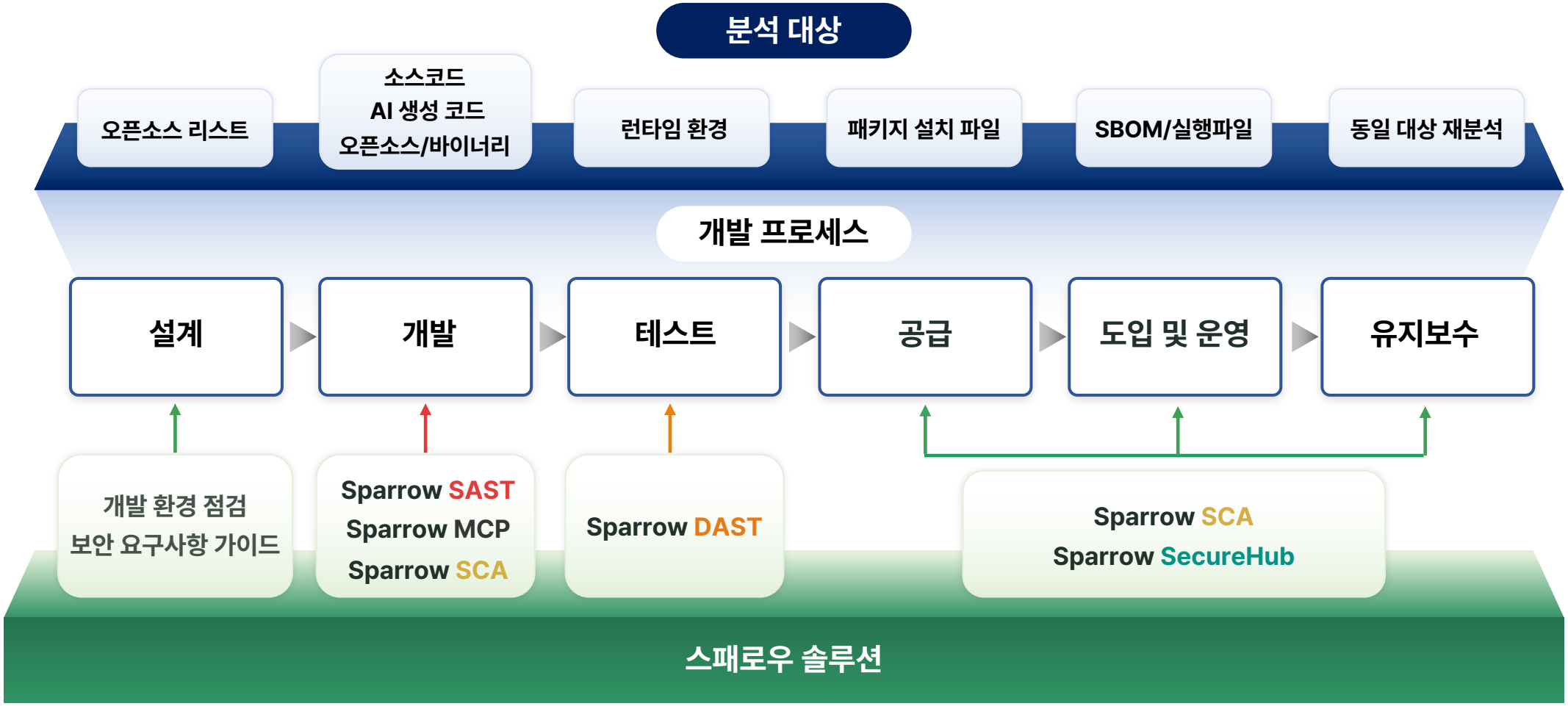
■ 로드맵이 요구하는 것 ↔ 스패로우의 대응

예방 · 복원 · 기반 — 로드맵 3대 전략 전부에 스패로우가 대응합니다.

	사전 · 예방	사후 · 복원력	기반 · 제도
로드맵 요구	**개발 전 단계 보안 내재화** **안전한 개발 & 책임있는 공급**	**SBOM 기반 SW 공급망 가시화** **SW 공급망 참여자 간 보안정보 공유·협력**	**보안적합성·법제도 정비** **국내 인증제도와 상호인정(MRA)**
스패로우 대응	• 정적(SAST)·동적(DAST) 분석으로 취약점을 개발 단계부터 차단 • AI가 생성한 코드의 취약점까지 개발과 동시에 검증 • 오픈소스 리스트를 식별 및 사전 검토 수행	• SBOM 기반 SW 공급망 위험 추적·관리 • SW 구성요소 가시화 · SBOM 생성 • SW 공급망 내 공급자↔수요자 SBOM 공유·상호 검토·협업	• CRA·FDA·보안적합성이 요구하는 SBOM·취약점 관리 요건 충족 지원 • '안전한 SW 개발 방법론' 준수 근거 확보

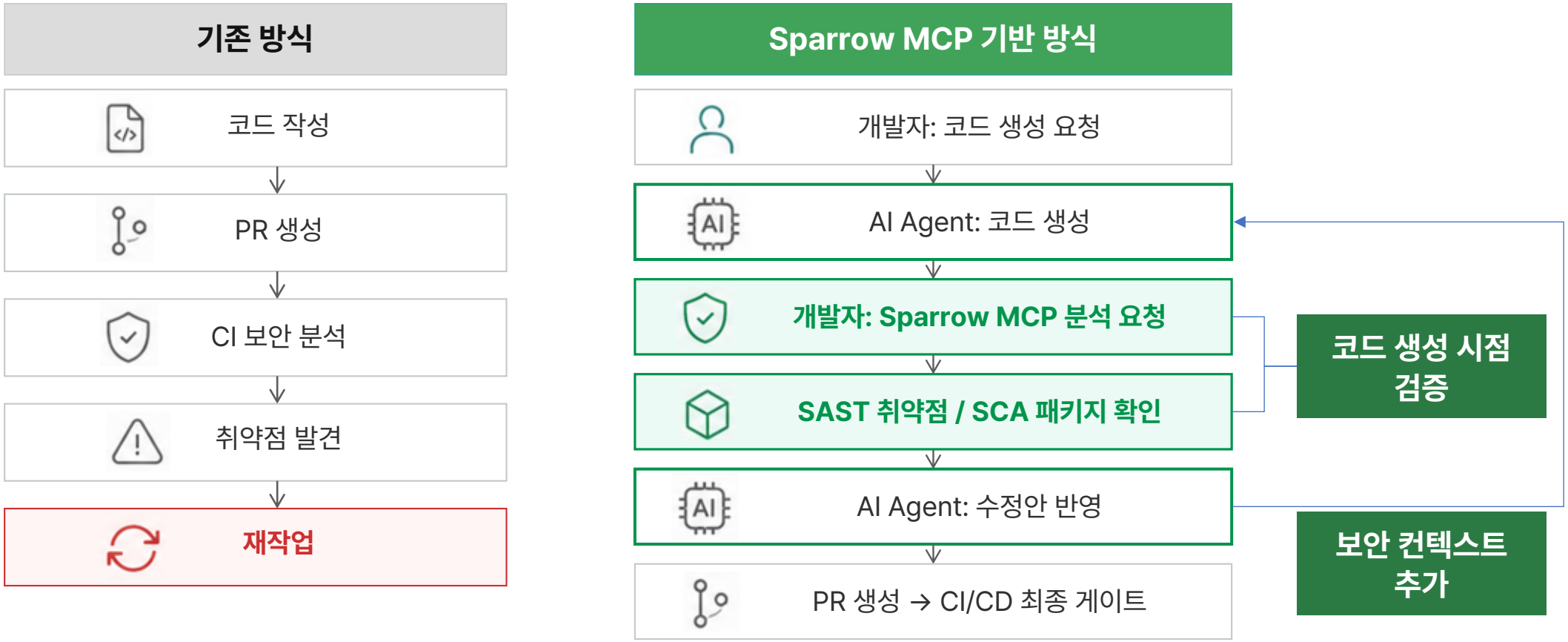
■ 스패로우 대응 - 1 전 생애주기 커버

설계부터 유지보수까지, 각 단계의 분석 대상과 스패로우 기능을 한 흐름으로 연결합니다.



■ 스패로우 대응 - 2 AI 생성 코드 보안(Sparrow MCP)

보안 검증을 코드 생성 시점으로 앞당겨 AI 개발 워크플로우에 보안을 내재화합니다.



보안 검증 시점을 PR 이후 → AI 코드 생성 시점으로 앞당깁니다.

■ 스패로우 대응 - 3 SBOM Lifecycle 관리 체계

SBOM 기반 신속한 취약점 대응과 지속적인 모니터링 체계 구축으로 SW 공급망 보안 정책에 대응이 가능합니다.

01 생성 (Generate)

분석 대상에서 SBOM 자동 추출
· 다중 포맷 (CycloneDX · SPDX)
· 소스·바이너리·컨테이너 모두 지원

02 보강 (Enrich)

SBOM에 외부 정보를 결합
· 취약점·라이선스·EOL·공급사 정보
· 메타데이터 보강으로 의사결정용 SBOM

03 증명 (Attest)

SBOM에 디지털 서명·무결성 보장
· Sigstore · Cosign · in-toto · SLSA
· "변조되지 않았다" 를 데이터로 증명

04 공유 (Share)

SecureHub 기반 안전한 전달
· 링크·이메일·API 채널
· 권한·다운로드 이력·승인 워크플로우

05 검토 (Review)

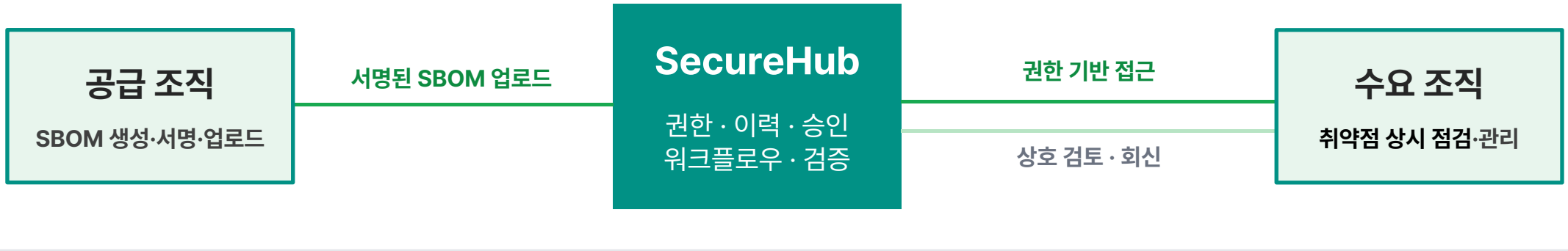
공급사 ↔ 수요자 상호 검토
· VEX 기반 영향 합의
· 정책 위반·라이선스 충돌 확인

06 관리 (Manage)

버전·이력·변경 추적 + 정책 자동화
· 신규 CVE 발생 시 영향 SBOM 식별
· 폐기 / 갱신 정책 운영

■ 스패로우 대응 - 4 SBOM 공유 전략(Sparrow SecureHub)

SW 공급망 참여자들 모두 안전하고 신뢰할 수 있는 SBOM 공유 환경을 실현합니다.



안전한 전달

· 프로젝트 접근 링크 / 이메일 공유
· 권한 기반 접근 (Role / 조직)

워크플로우

· 검토 요청
· 컴포넌트 목록 · 취약점 현황 조회

감사 추적

· 등록 / 공유 이력
· 조직 구성 추가 / 변경 및 SBOM 서명
· 규제 대응 감사 로그 자동 생성

협업

· 공급 조직 ↔ SW ↔ 수요 조직 한 화면
· VEX·취약점 응답을 포함한 SBOM 검토

■ 스패로우 솔루션 활용 – SW 공급망 전 주기 보안 활동 예시

개발·공급 기업과 도입·운영 기업이 각 공급망 단계에서 수행할 활동입니다.

개발 · 공급 기업

기획 · 설계 → 개발 → 테스트 → 배포

기획·설계	· 개발 환경·언어·오픈소스 사용 현황 등 환경 조사 · SW 제품, 서비스 개발자 및 관련자 대상 보안 교육 (시큐어코딩·공급망 보안)
개발	· 시큐어코딩 준수 및 AI 생성 코드 보안 검증 · 오픈소스 라이브러리 사용 전 보안성 확인 · 빌드 과정의 자동화된 보안 테스트
테스트	· 정적·동적 분석으로 보안 취약점 점검 · 전문 인력 모의해킹으로 위협 요소 제거
배포	· SW 구성요소 식별 및 SBOM 생성 · 도입·운영 기업에 점검 보고서·SBOM 전달

도입 · 운영 기업

도입 → 구축 → 운영 → 모니터링 → 모니터링

도입·구축	· 점검 보고서로 보안 요구사항 이행 여부 확인 · 외부 도입 SW의 SBOM 제출 요구 및 검토
운영·모니터링	· SBOM 기반 CVE 등 취약점 포함 여부 상시 점검 · 신규 취약점 발견 시 개발사 조치 요청·이력 관리
폐기	· SBOM에 EoL 추가로 교체·제거 계획 사전 수립 · 변경된 SW 자산 정보 반영해 SBOM 업데이트

SPARROW

| AI가 짠 코드까지, SW 공급망을 끝까지 책임집니다

sparrow.im

sales@sparrow.im

02-6263-7400