SYNOPSYS®

Webinar

다양한 AppSec 도구의 넘쳐나는 결과들로부터 가장 중요한 보안문제에 집중하는 방법

- ASPM으로 AppSec 프로그램의 효율성 확보

남문현부장

Sales Engineer, Synopsys Korea

Oct 2023

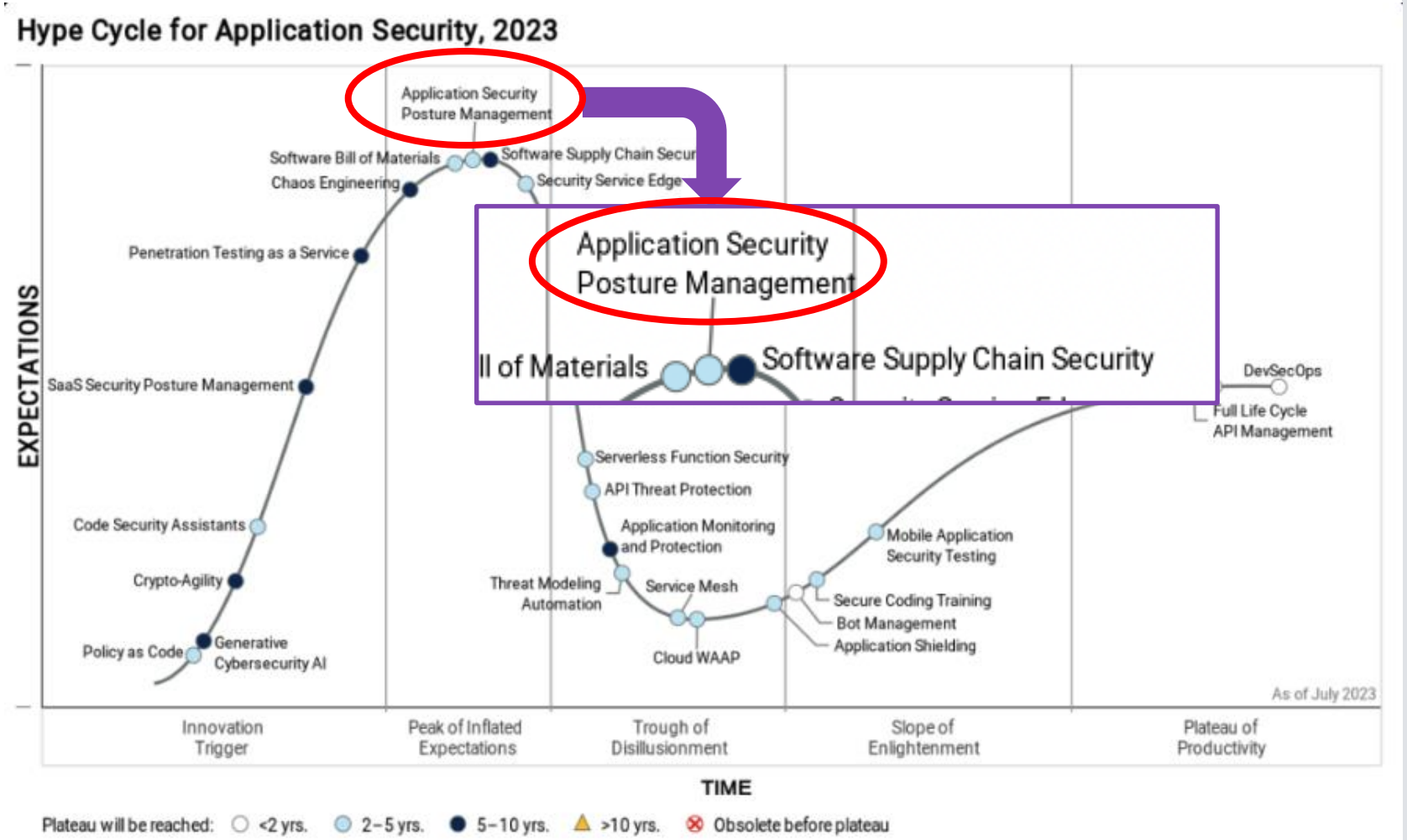
목차

- 애플리케이션 보안 상태 관리(Application Security Posture Management, ASPM)의 등장
- 시장의 변화와 추세
- AppSec이 직면한 도전과제
- ASPM의 기능과 역할
- Synopsys ASPM 솔루션: Security Risk Manager(SRM)

애플리케이션 보안 상태 관리(Application Security Posture Management, ASPM)의 등장

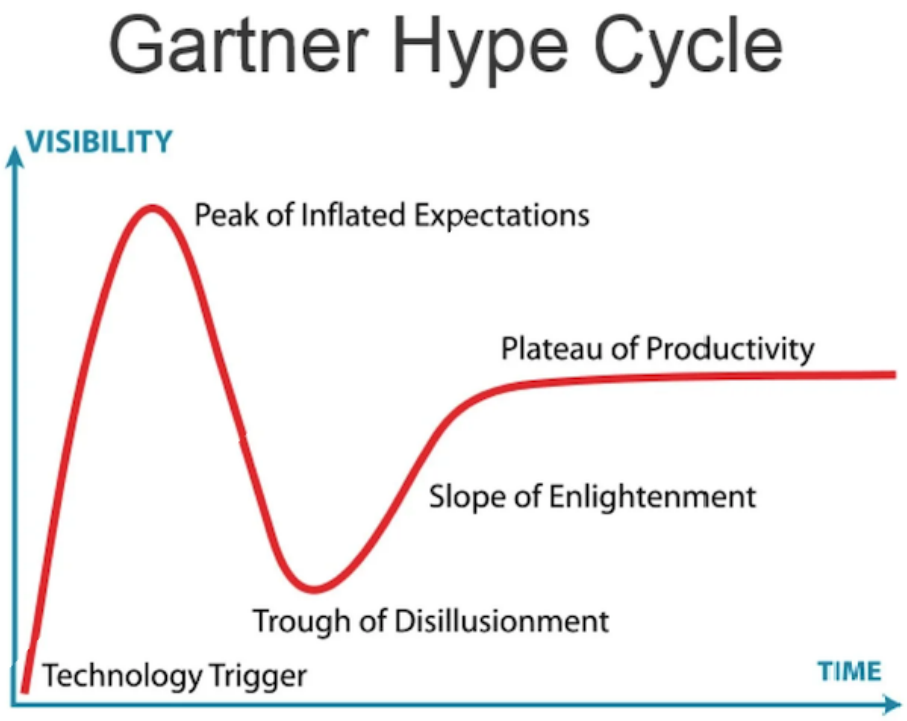
ASPM의 등장

2023년 애플리케이션 보안의 하이프 사이클



*"By 2026, **over 40% of organizations** developing proprietary applications **will adopt ASPM** to more rapidly identify and resolve application security issues." (Gartner)*

Gartner 하이프 사이클?

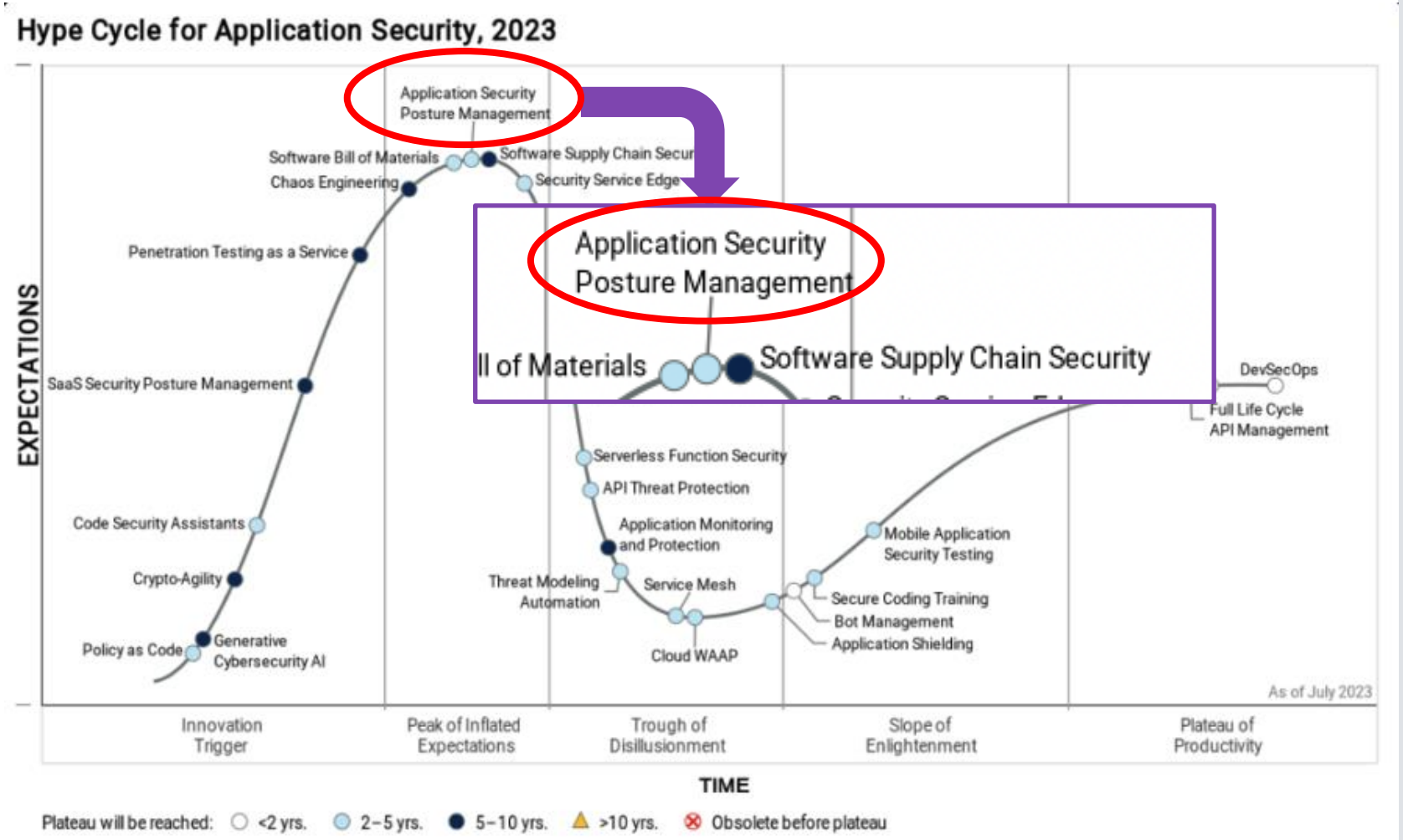


Source: https://en.wikipedia.org/wiki/Gartner_hype_cycle

번호	단계	설명
1	기술 촉발(Technology Trigger)	잠재적인 기술 혁신이 시작됩니다. 초기 개념 증명 사례와 미디어의 관심은 상당한 홍보 효과를 불러일으킵니다. 사용 가능한 제품이 존재하지는 않고 상업적 실행 가능성이 입증되지 않은 경우가 많습니다
2	부풀려진 기대의 정점(**Peak of Inflated Expectations**)	초기 홍보는 수많은 성공 사례를 만들어내지만, 종종 수많은 실패를 동반하기도 합니다. 일부 기업은 조치를 취하지만 대부분은 그렇지 않습니다.
3	각성의 골짜기(**Trough of Disillusionment**)	실험과 구현이 실패함에 따라 관심은 줄어들게 됩니다. 기술 생산자가 흔들리거나 실패합니다. 살아남은 공급업체가 얼리어답터들이 만족할만큼 제품을 개선해야만 투자가 계속됩니다.
4	깨달음의 언덕(**Slope of Enlightenment**)	기술이 기업에 어떻게 이익을 가져다 줄 수 있는지에 대한 사례가 구체화되고 더 널리 이해되기 시작합니다. 기술 공급업체에서 2세대와 3세대 제품들이 등장합니다. 더 많은 기업이 파일럿에 자금을 지원하지만 보수적인 기업은 여전히 신중한 태도를 유지합니다.
5	생산성의 안정기(**Plateau of Productivity**)	주류 채택이 시작됩니다. 공급업체의 실행 가능성을 평가하는 기준이 보다 명확하게 정의됩니다. 기술의 광범위한 시장 적용 가능성과 관련성이 분명한 성과를 거두고 있습니다. 만약 이 기술이 틈새 시장 이상을 가지고 있다면 이 기술은 계속해서 성장할 것입니다.

ASPM의 등장

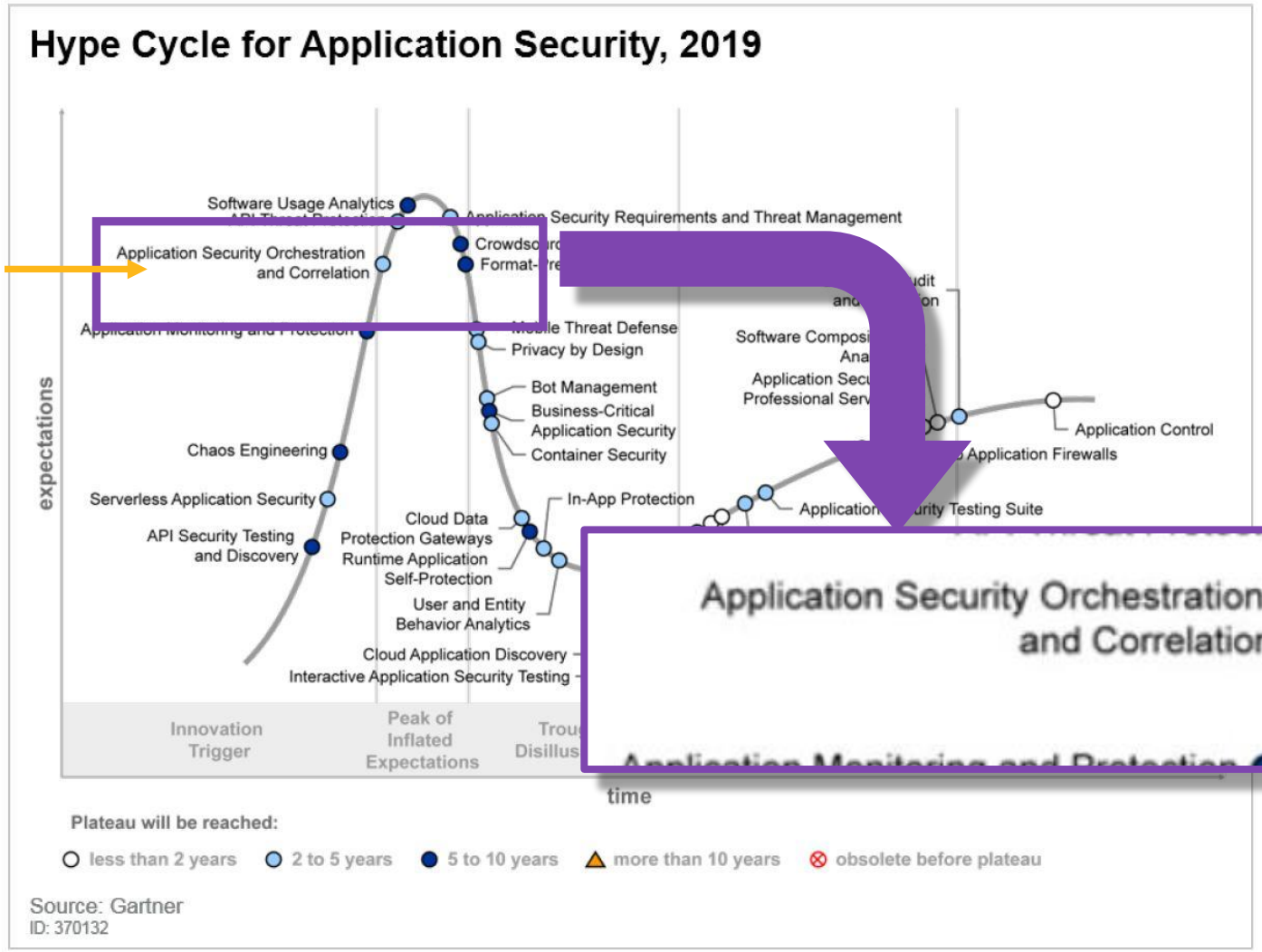
2023년 애플리케이션 보안의 하이프 사이클



*"By 2026, **over 40% of organizations** developing proprietary applications **will adopt ASPM** to more rapidly identify and resolve application security issues." (Gartner)*

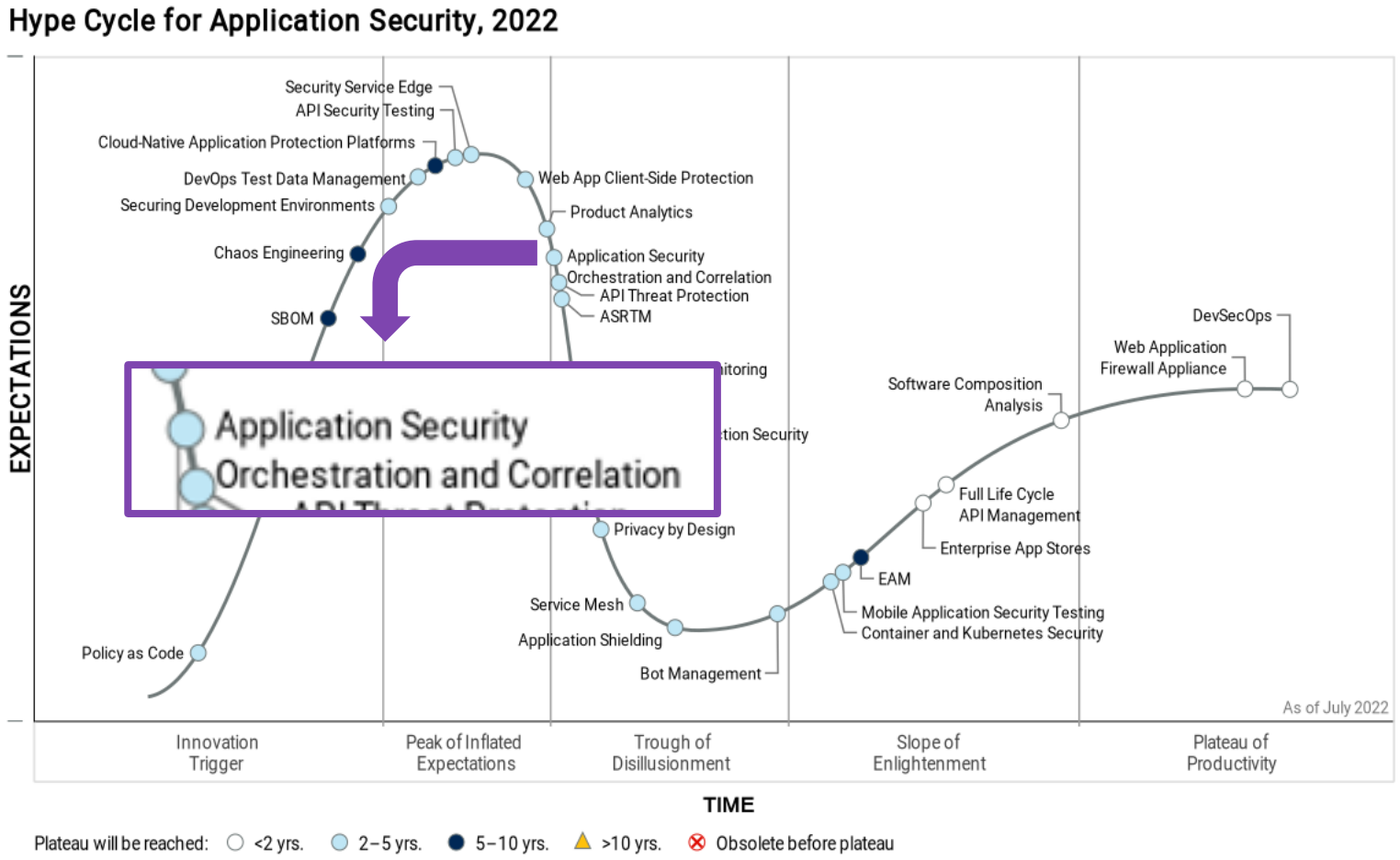
Application Security Orchestration and Correlation(ASOC)

애플리케이션 보안 조율 및 상관관계



ASOC

2022년 애플리케이션 보안의 하이프 사이클



Gartner, Hype Cycle for Application Security, 2022, Joerg Fritsch, 11 July 2022

ASOC의 3가지 주요 이점

ASOC는 AppSec 프로세스에 3가지 주요 이점을 제공:

1. 효율성: 모든 데이터를 한 곳에서 관리
2. 확장성: AppSec의 일관성
3. 책임성
   - 소프트웨어 테스트는 언제 진행되었는가?
   - 어떤 이슈가 발견되었는가?
   - 이슈는 해결되었는가?

ASOC 도구의 요구 기능

1. 광범위한 상용 및 오픈소스 AppSec 테스트 도구와 통합되어야 합니다.

2. 이러한 도구에서 얻은 결과를 정규화하고 상호 연관시켜야 합니다.

3. 반드시 오케스트레이션 기능을 제공해야 합니다.

ASPM 도구의 요구 기능

서로 다른 환경 전반에 걸친 통합

모든 보안 테스트, 개발자 도구, 이슈 추적기 전반에 걸쳐 데이터 통합

이슈의 우선순위 지정 및 분류심사 가속화

발견 건수를 줄이고 가장 중요한 보안 작업을 파악

정책 관리 중앙 집중화

스캔 전/후 작업의 정의 및 시행

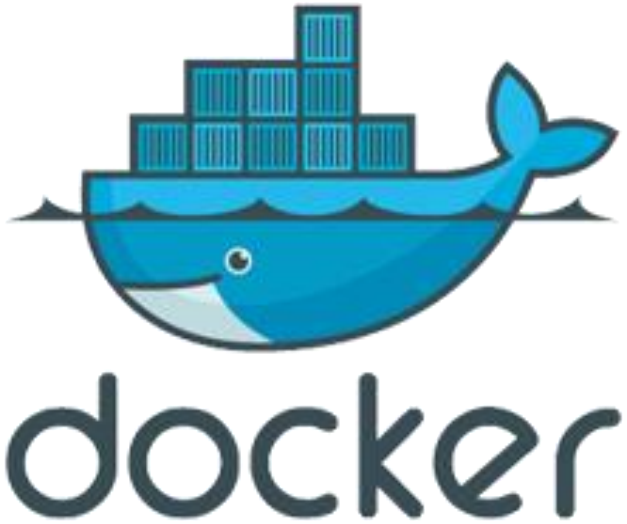
소프트웨어 위험에 대한 정확한 시각 제공

소프트웨어 차지 공간 전체에 대한 표준 준수 상태 요약

시장의 변화와 추세

갈수록 더 복잡해지는 소프트웨어

- 소프트웨어 설계의 변화
  - 마이크로서비스, 서버리스 등
- 더 빨라진 배포 방식
  - 10s -> 100s -> 1000s 빌드(매일)
- 어느 때보다 다양해진 배포방식
  - 컨테이너, 클라우드, IoT 장치들



갈수록 더 복잡해지는 소프트웨어

Facebook 매일 50,000 에서 60,000번의 Android 빌드를 제공합니다

Amazon은 매초마다 새로운 소프트웨어를 프로덕션 환경에 배포하는 것으로 알려져 있습니다

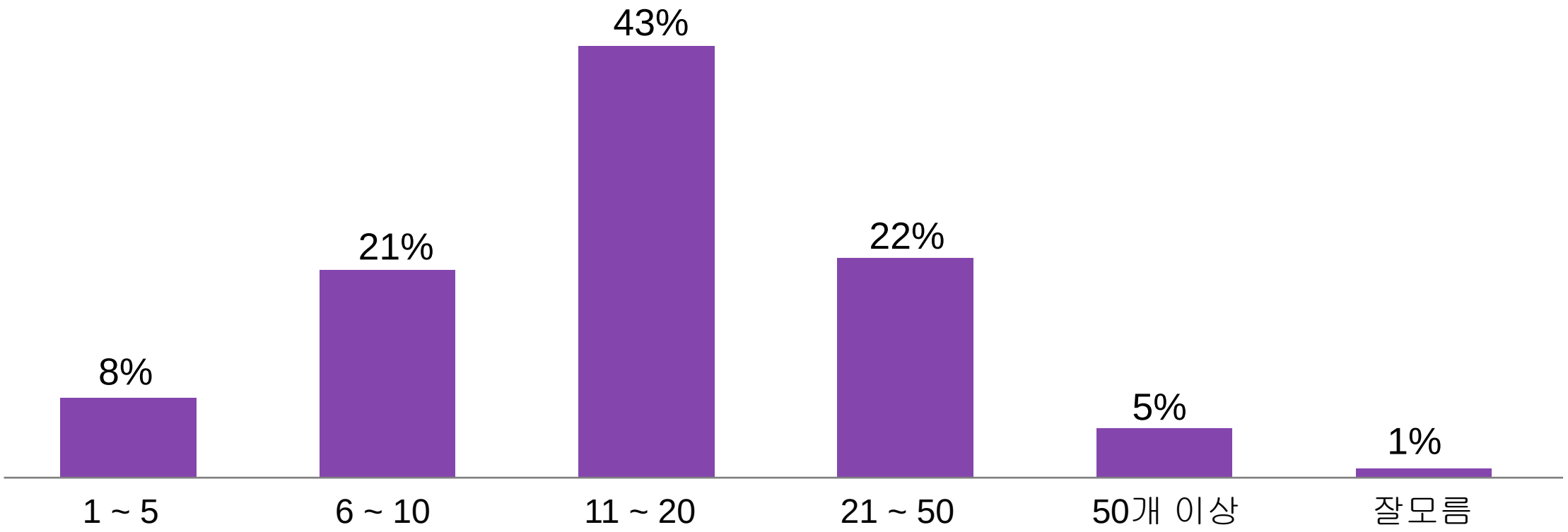
Etsy는 지속적인 전달(CD) 방식을 사용하여 단일 모놀리식 애플리케이션을 하루 60회 이상 배포합니다

Netflix의 DevOps 팀은 매일 100번씩 새로운 릴리스를 배포합니다

다양한 AppSec 도구들의 사용

현재 귀사에서 사용하고 있는 개별 애플리케이션 테스트 도구는 몇개입니까?

(378명의 응답자에 따른 비율)



Source: Cracking the Code of DevSecOps - Enterprise Strategy Group June 2021

DevOps속도를 저하시키는 오래된 도구와 방법

파이프라인 정체

대규모 모놀리식 AppSec 테스트 도구는 빌드, 테스트 및 릴리스 파이프라인을 정체시킬수 있습니다. 해답은 더 작은 규모의 해당 목적에 접합한 테스트가 상황에 따라 적시에 지능적으로 실행되도록 하는 것입니다.

출력 과부하

결과 관리

더 많은 도구 + 더 많은 테스트 = 더 많은 결과. 보안팀은 개발자가 부담을 느끼지 않고 가장 중요한 문제에 집중할 수 있도록 상호 연관시키고, 중복을 제거하고, 우선순위를 지정해야 합니다.

데이터 과부하

애플리케이션 보안과 DevOps의 속도

"우리는 전력질주 중입니다"

개발자

"너무 빨라요!"

AppSec

"우리는 기다릴 수 없습니다"

개발자

안전하지 못한 **Software**

사이버 공격과 데이터 유출

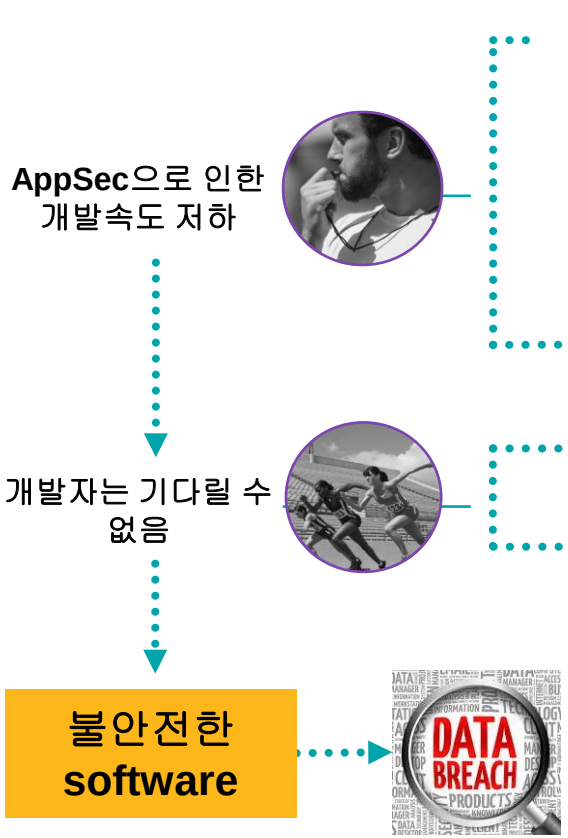
Ponemon 연구 2021

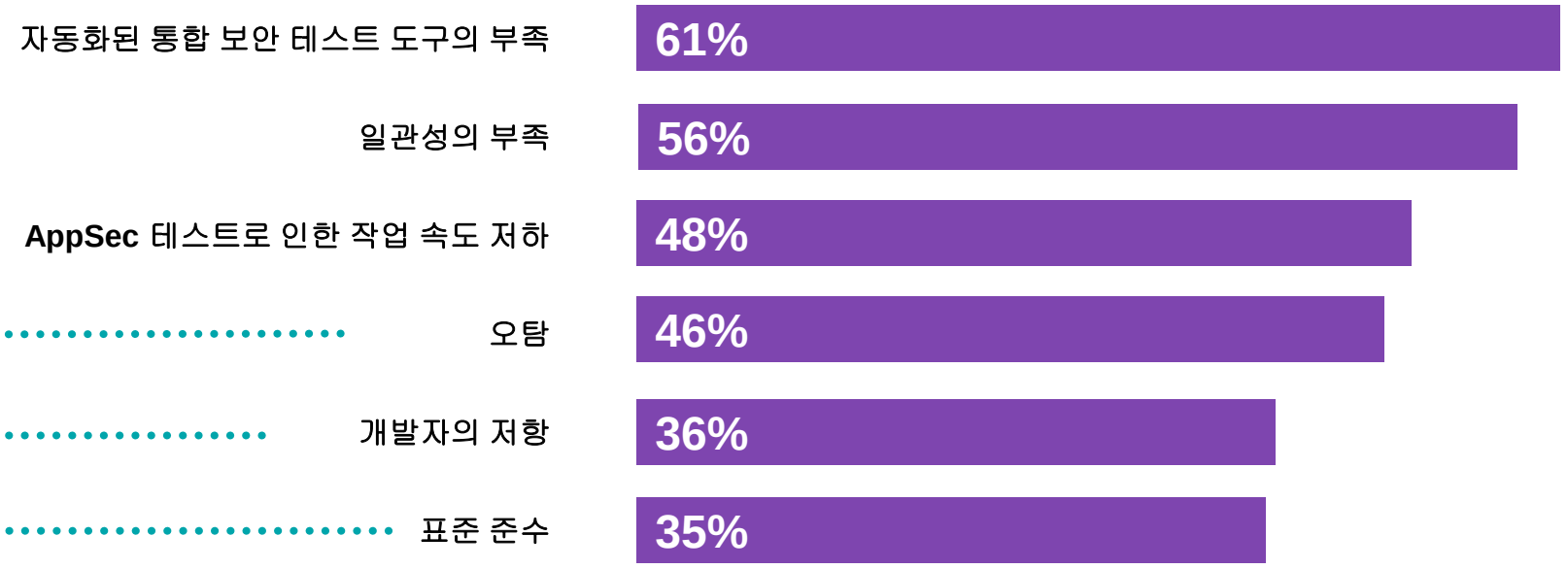
- $4.24M USD
  - 2021년 평균 데이터 유출 비용
  - 2020년 대비 10% 증가
- 2021 연말까지 전세계적으로 연간 $6조 USD 예상

AppSec이 직면한 도전과제

AppSec의 가장 큰 과제는?

AppSec 테스트의 자동화, 통합 및 일관성 부족

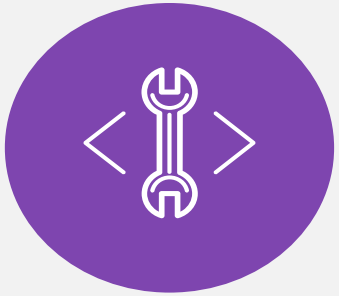




350명의 기업 IT 의사 결정권자를 대상으로 한 설문, 2020년 4월

451 Research

AppSec 투자에도 불구한 SDLC 보안의 실패



64%

최소 6개 이상의 AST 도구 사용 중

35%

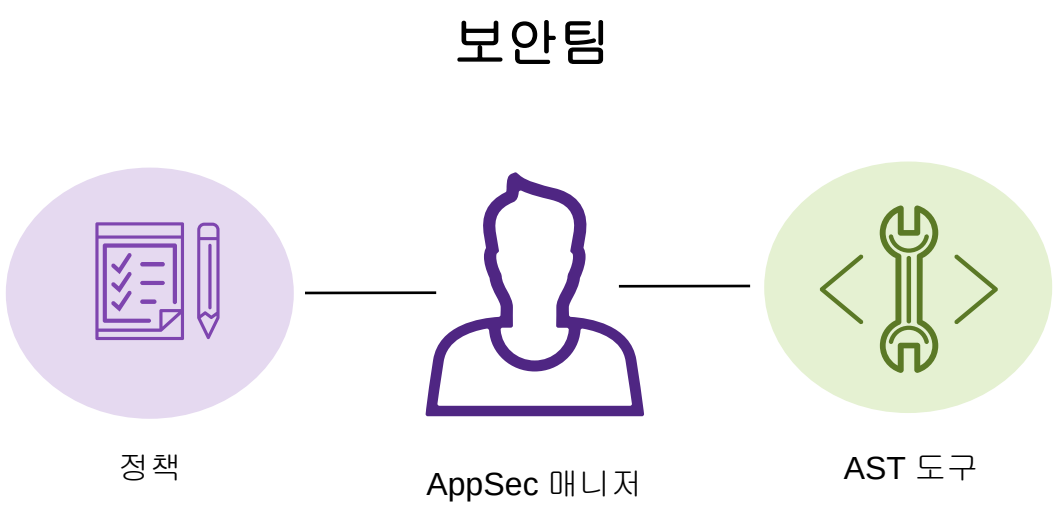
알고 있는 취약점을 가진 코드를 그대로 배포

45%

테스트 또는 보안 검사 없이 소프트웨어 출시

Source: Enterprise Strategy Group

AppSec ROI 달성을 위해 필요한 것?



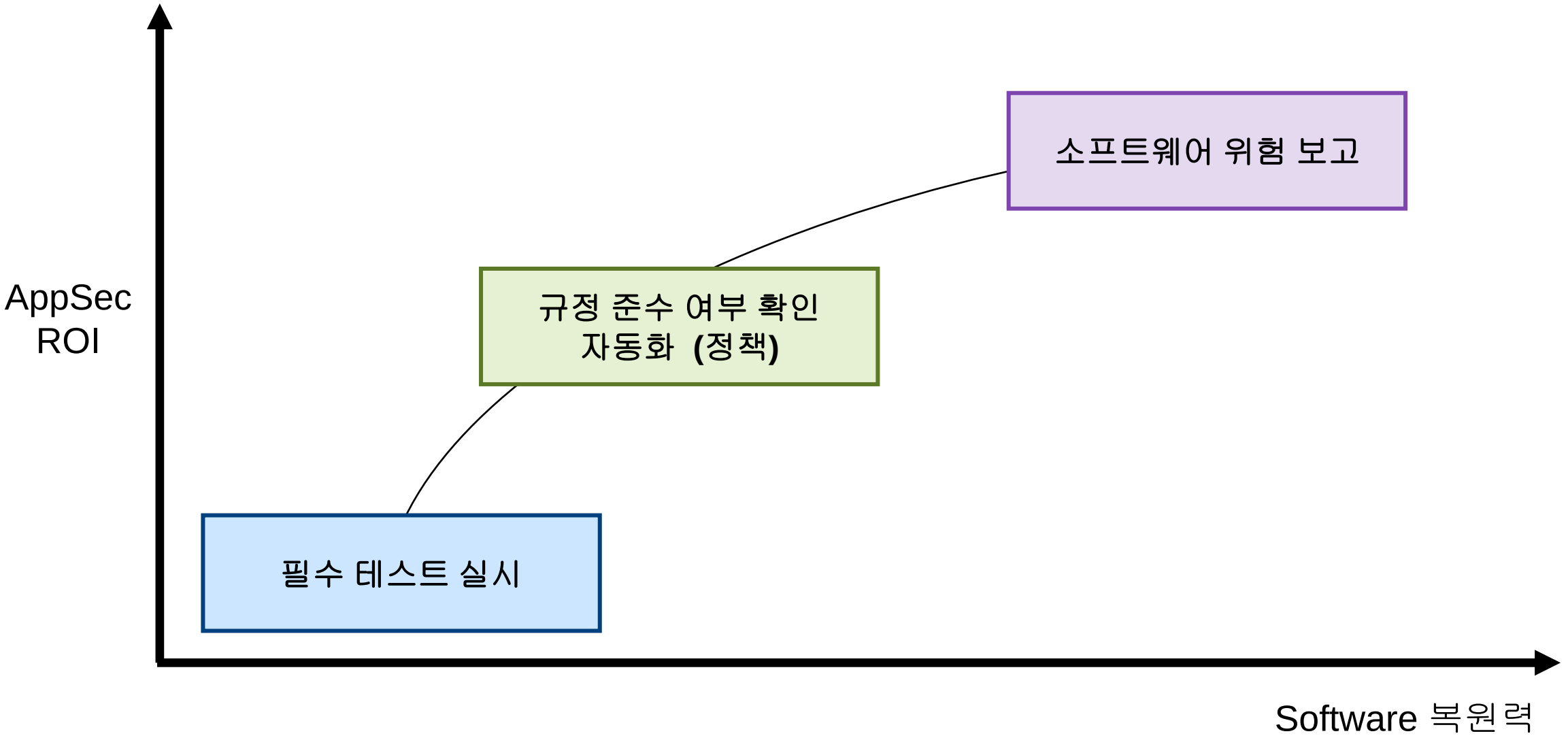
개발자가 애플리케이션 보안 테스트(AST) 도구들과 보안 업무절차을 따르게 하려면 어떻게 해야 합니까?

보안정책이 잘 지켜지고 있는지 어떻게 알 수 있습니까?

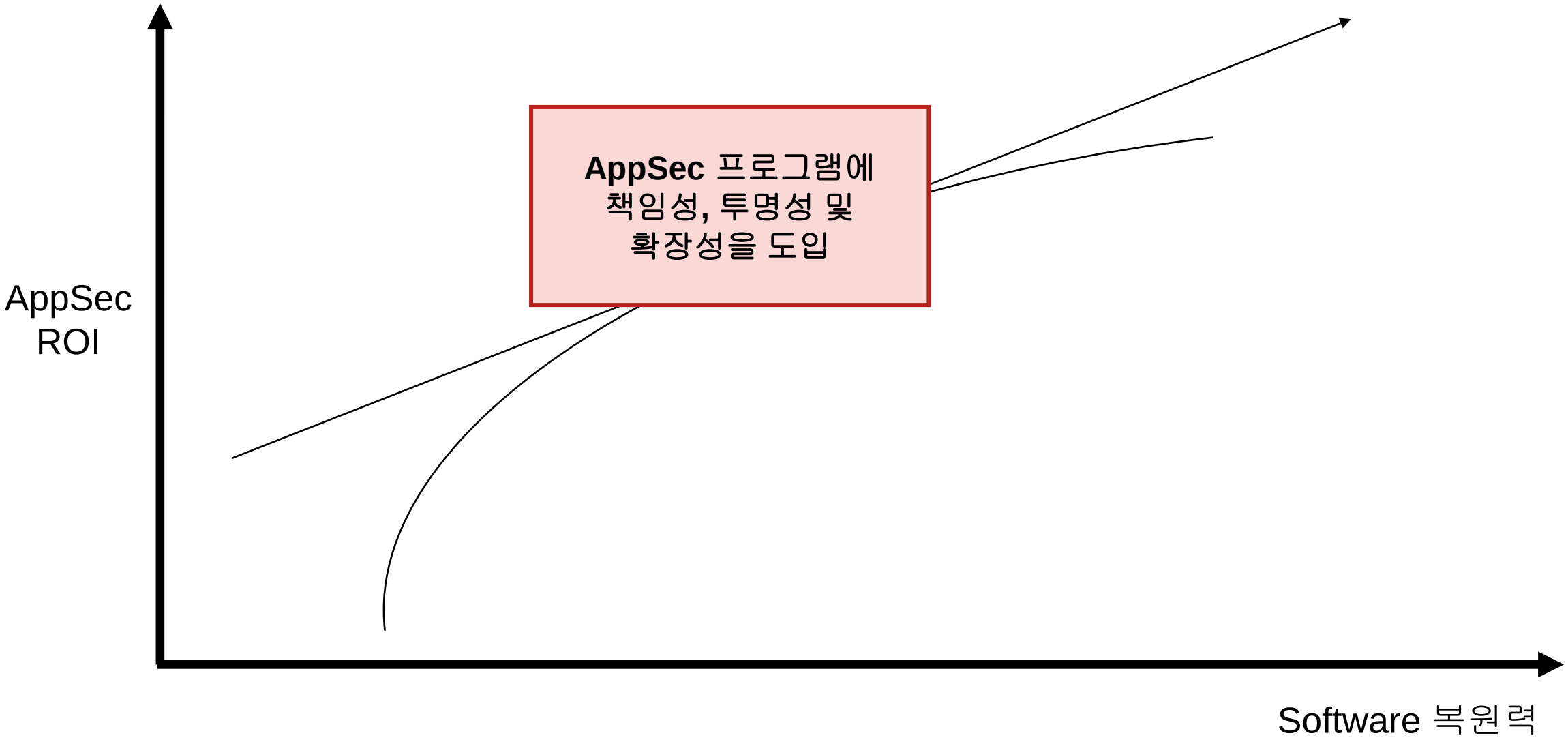
애플리케이션의 보안 위험은 얼마나 됩니까?

AST 투자를 어떻게 확장할 수 있습니까?

AppSec 프로그램이 성숙되기 위해 필요한 능력



AppSec 프로그램이 성숙되기 위해 필요한 능력

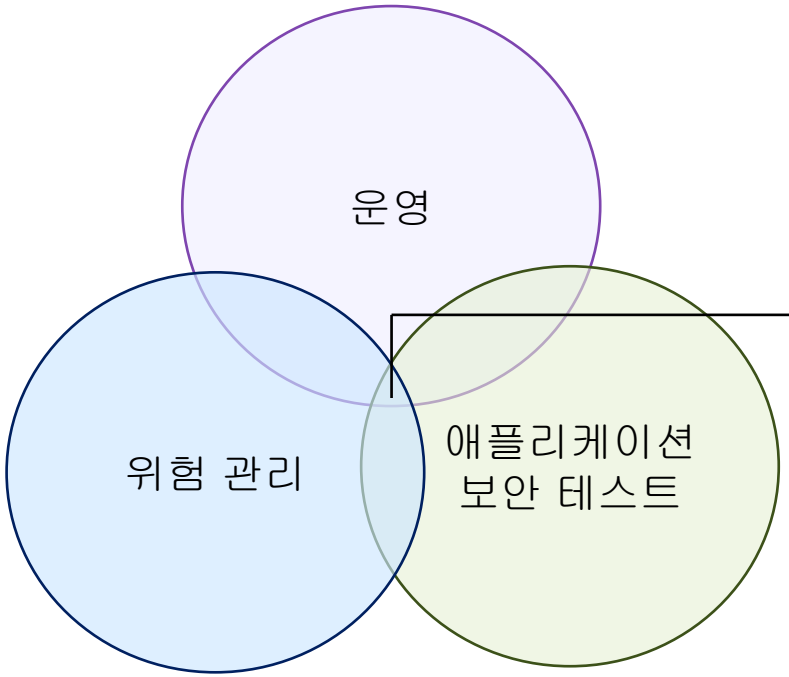


ASPM의 기능과 역할

Application Security Posture Management

애플리케이션 보안 위험상태 관리

ASPM은 어디에 적합한가?



ASPM 솔루션은 소프트웨어 개발, 배포 및 운영 전반에 걸쳐 보안 데이터, 가시성 및 제어 기능을 통합할 수 있는 기능을 제공합니다

"By 2026, **over 40% of organizations** developing proprietary applications **will adopt ASPM** to more rapidly identify and resolve application security issues." *(Gartner)*

ASPM 솔루션의 필요 기능

서로 다른 환경 전반에 걸친 통합

모든 보안 테스트, 개발자 도구, 이슈 트래커 전반에 걸쳐 데이터 통합

이슈의 우선순위 지정 및 분류심사 가속화

발견 건수를 줄이고 가장 중요한 보안 작업을 파악

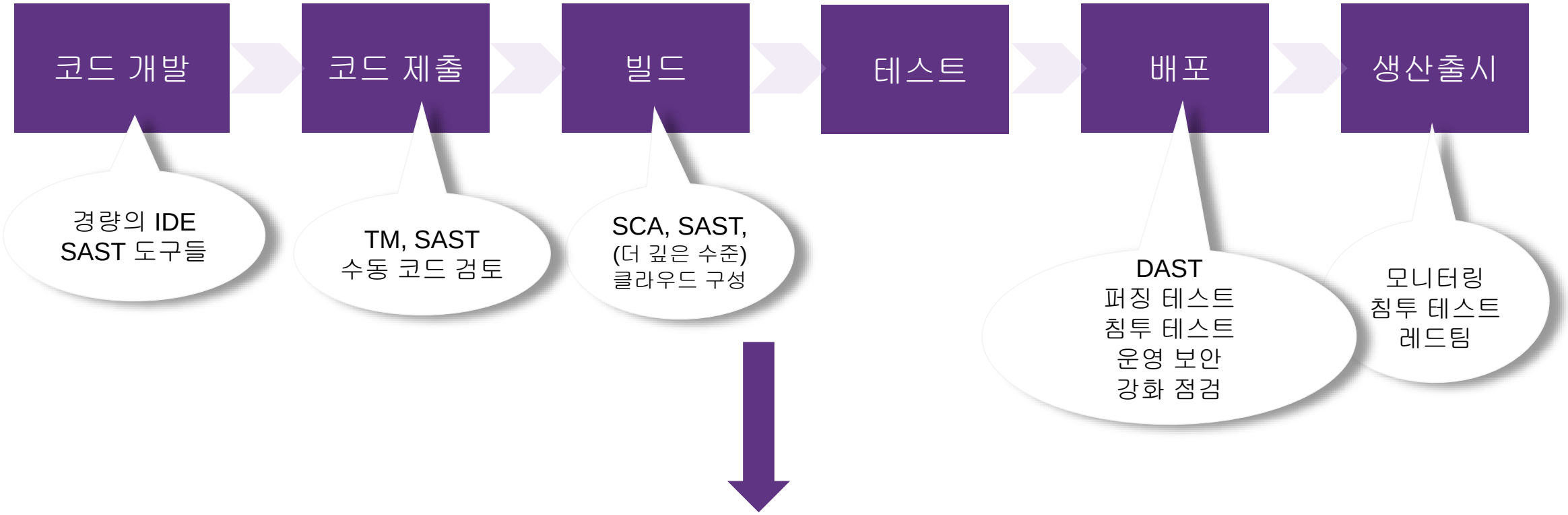
정책 관리 중앙 집중화

스캔 전/후 작업의 정의 및 시행

소프트웨어 위험에 대한 정확한 시각 제공

소프트웨어 차지 공간 전체에 대한 표준 준수 상태 요약

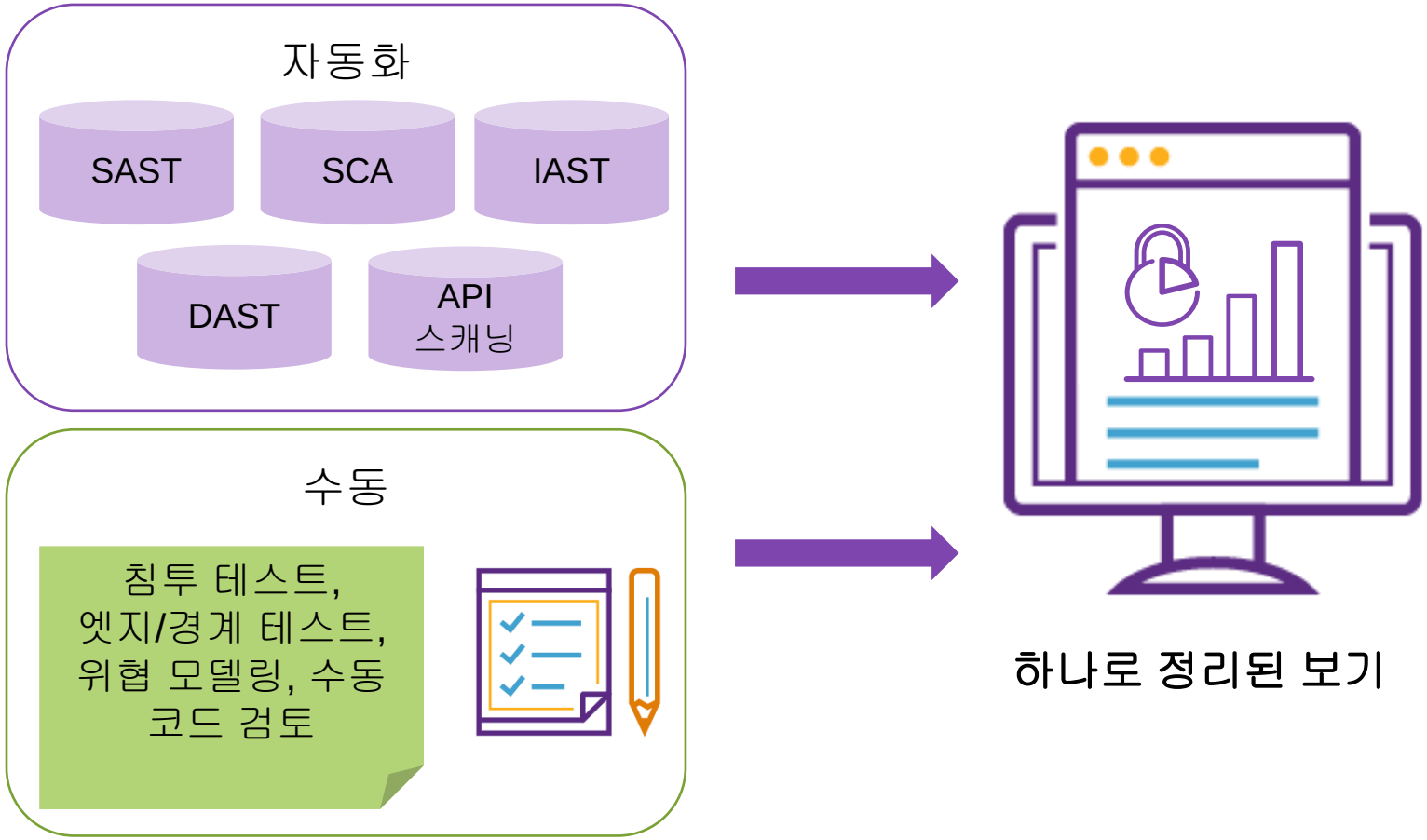
보안 상태 관리를 위해서는 종합적인 관점 필요



소프트웨어는 어떻게 구성되어 있는가? 무엇을 언제 테스트 했는가? 어떤 것이 수정되었는가? 발견된 이슈는 무엇인가? 노출/악용 가능성은 어느 정도인가? 소프트웨어가 규정을 준수하고 있는가?

테스트 소스 통합 및 데이터 상호 연관

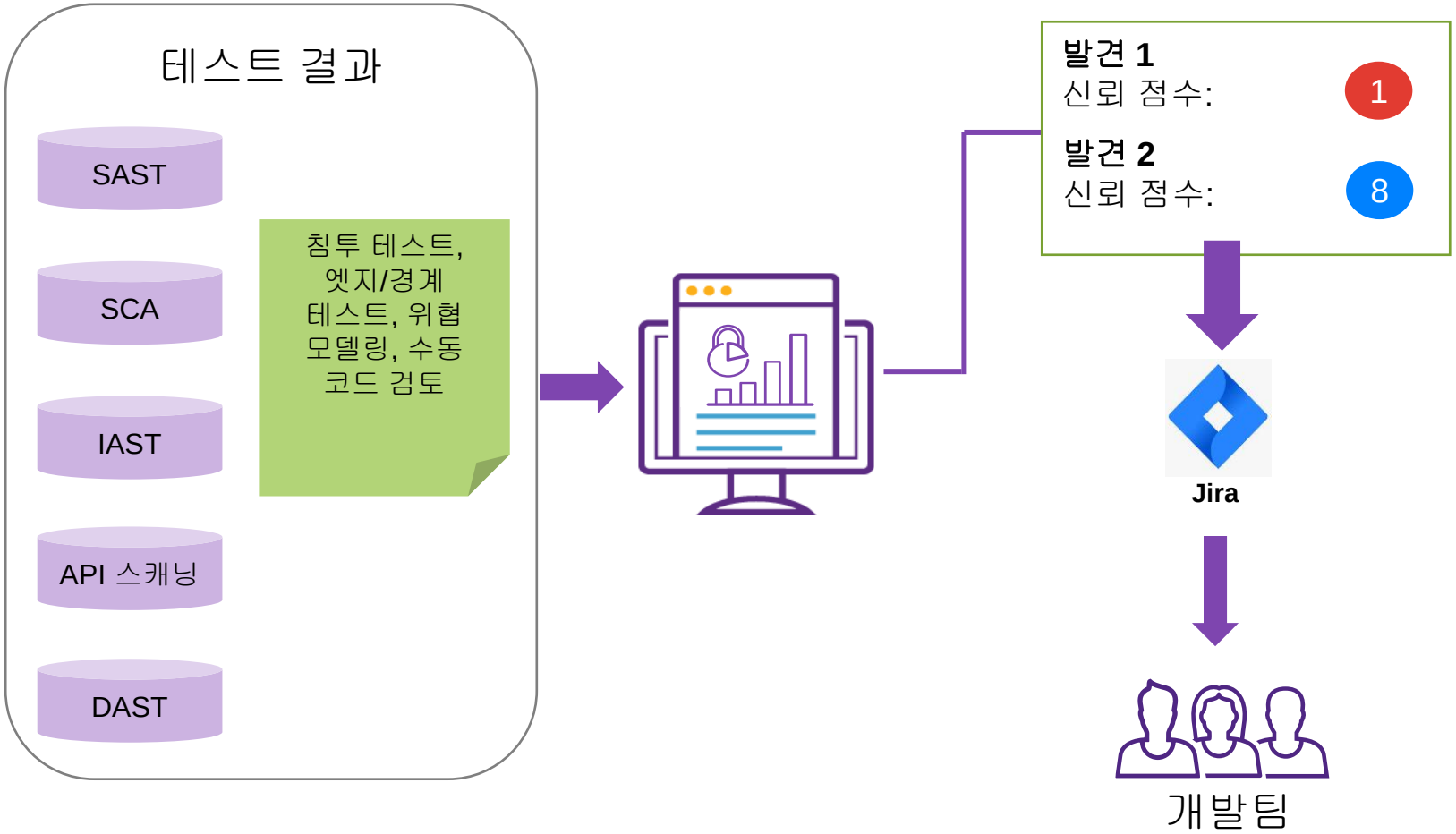
단일 기록 시스템으로 실행 가능한 인사이트 확보



영향이 큰 보안 활동을 식별하고 **수동 및 자동화된 AST와 개발자 도구 전반에 걸쳐 내용을 요약**

우선 순위 지정 및 업데이트 적용 시간 단축

위험도에 따라 보안 이슈 에스컬레이션



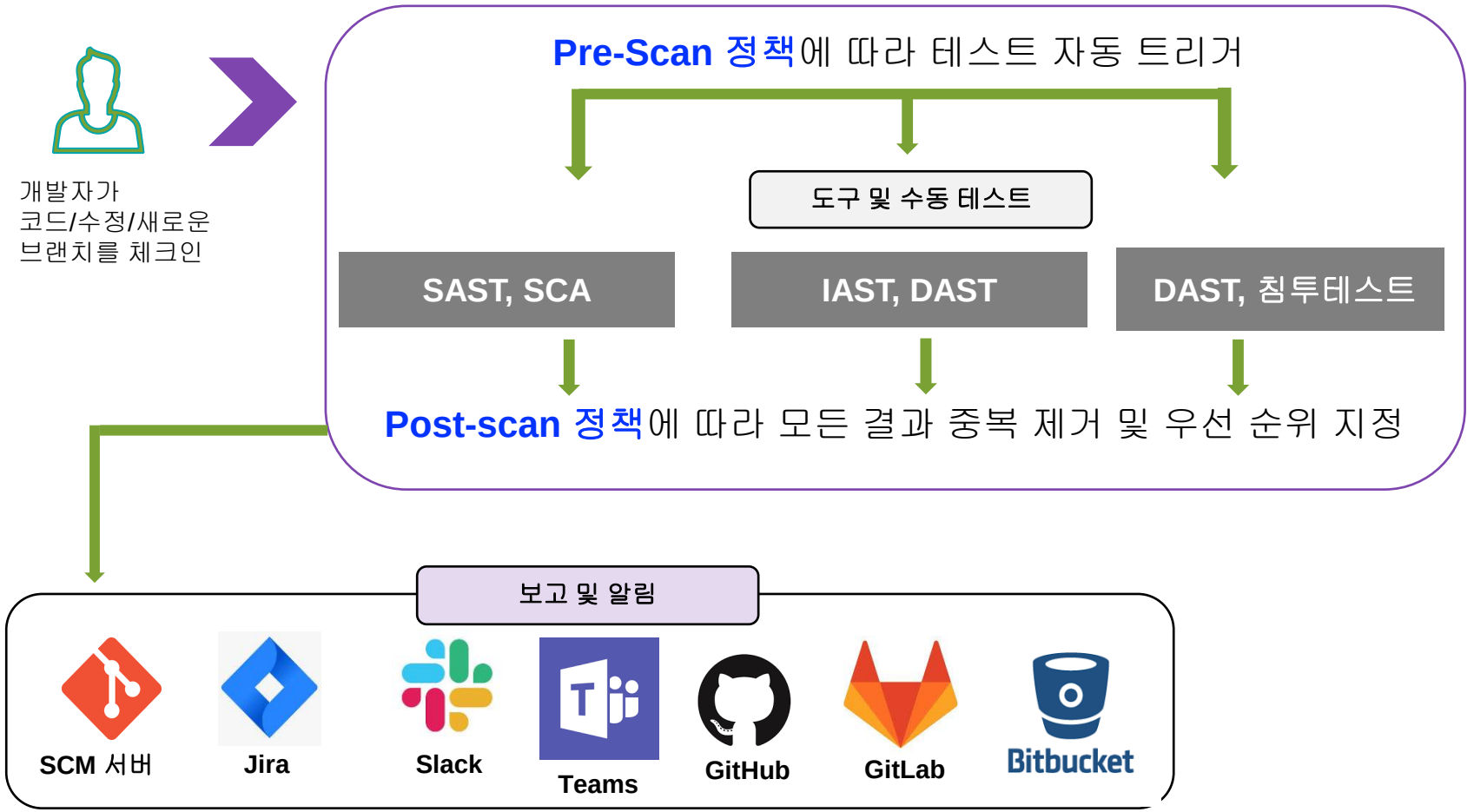
심각한 결함을 개발자 이슈 추적기 및 **IDE**에 직접 동기화하여 보안 적용도를 높이고 교육 피로도를 줄입니다

정책이 확장가능한 제어 구현의 핵심

*Source: Cybersecurity Collaborative, "**CISO's Guide to Developing an Effective Application Security Program, 2022**"*

대규모 거버넌스 구축

중앙 제어 지점에서 보안 표준절차 적용



정책 및 작업을 한 곳에서 밀어 넣어 일관성 있는 테스트 및 수정 작업을 조율

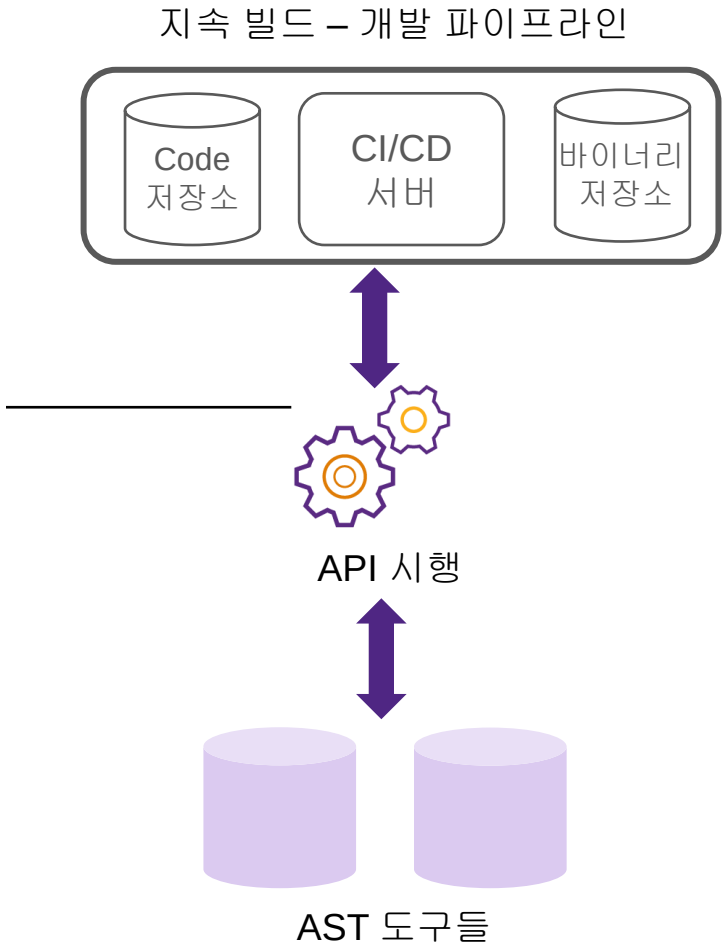
정책유형 – Pre-Scan 정책

Pre-Scan 정책

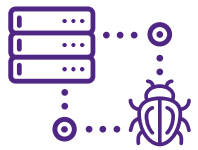
동적 앱 별 기준
(비지니스 중요도, 다운타임 위험)

필요한 테스트 유형
(자동 또는 수동, 기간)

테스트 실행 조건
(코드 변경 범위, 결함)



정책유형 – Post-Scan 정책



보안 이슈들

Post-Scan 정책

정책 앱 별 기준
(위험 프로파일, 규정 준수 기준)

이슈 분류
(이슈 유형, 심각도, 악용 가능성)

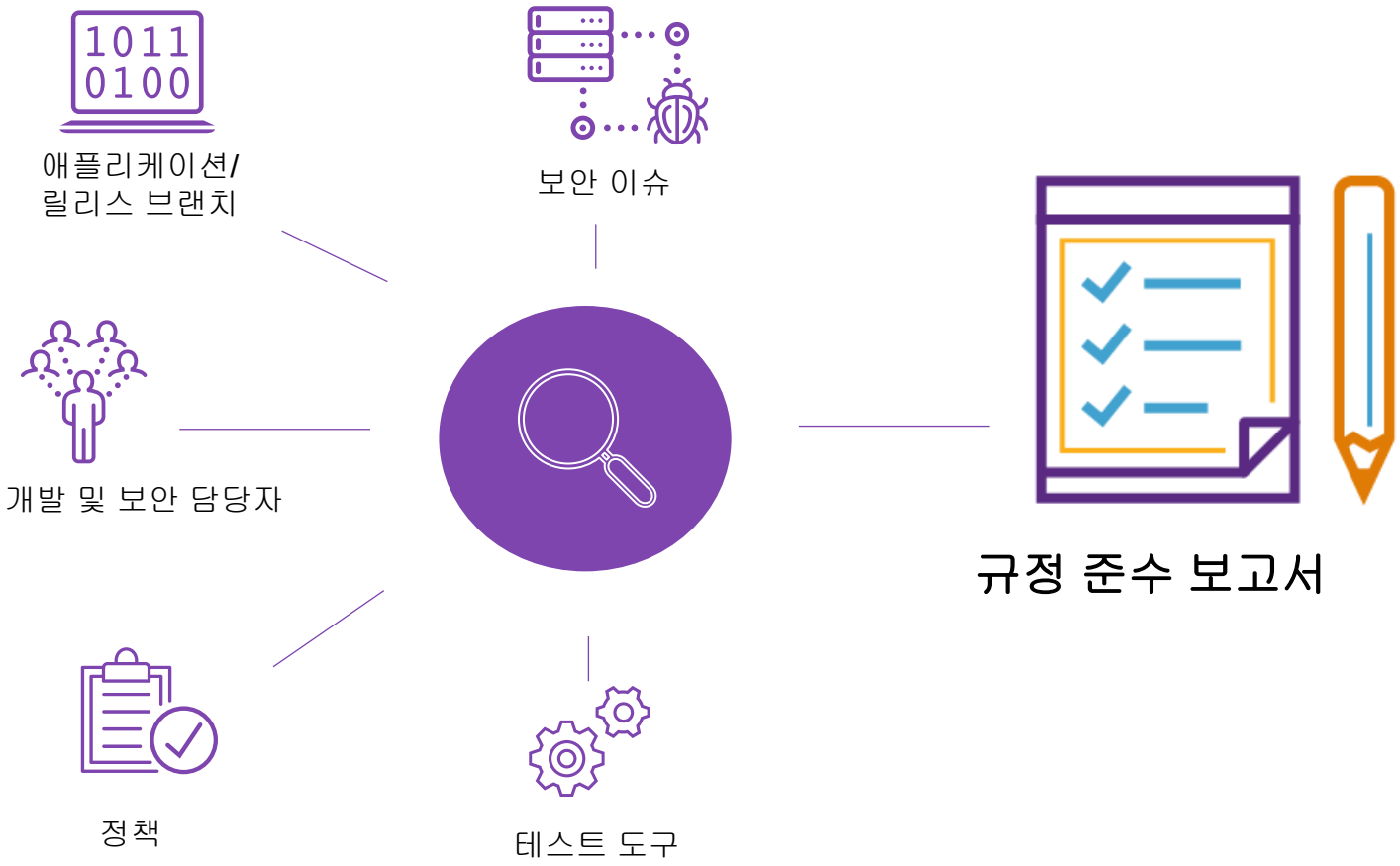
수정 SLA
(수정 사항 제출 일정)

내부 **AppSec** 정책

발견 1
위험 점수: 7.8
수정 기한: 14 일
심각도: Critical

중요한 소프트웨어 위험 이해

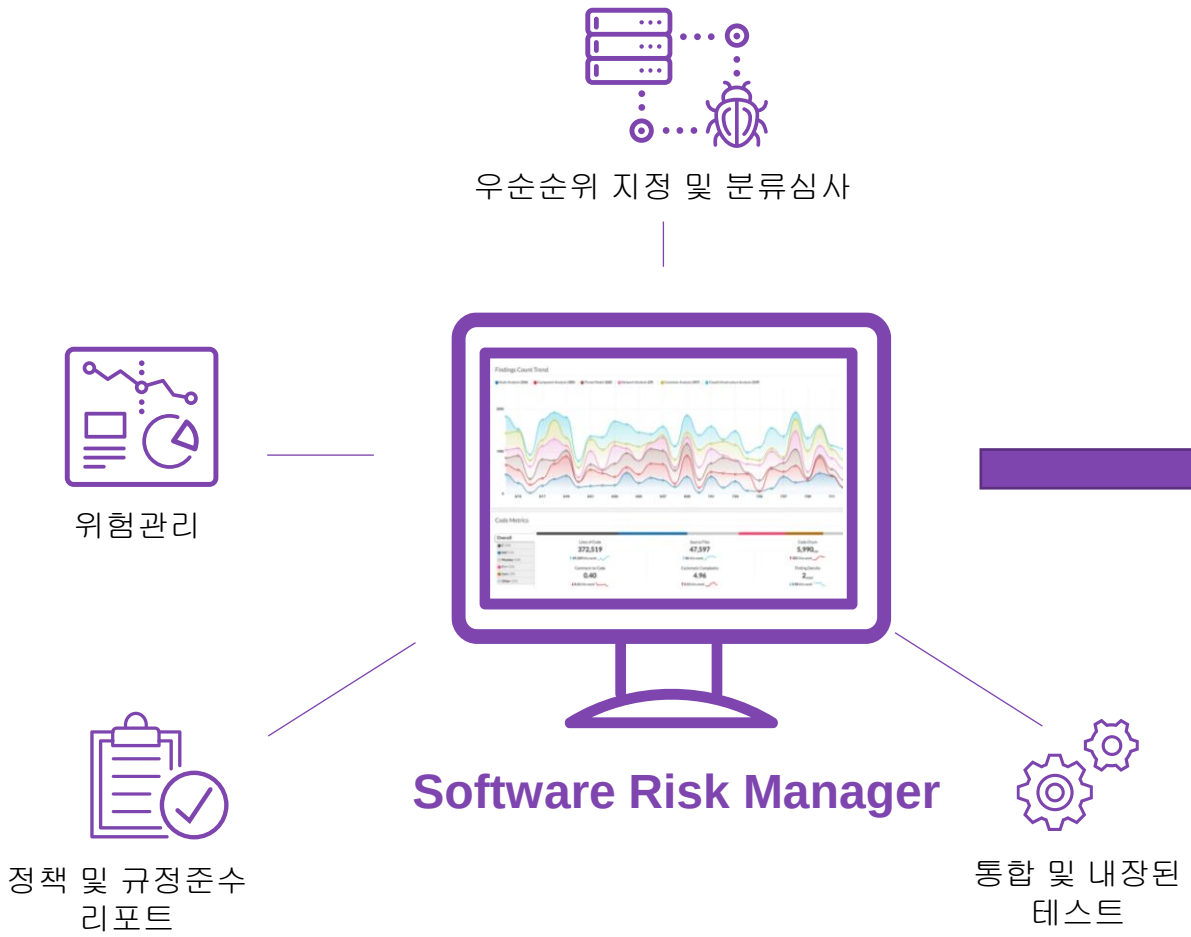
규정 준수 위반에 따른 매핑 및 감사 결과 도출



SDLC 전반에서 규정 준수를 지속적으로 모니터링하고 **코드** 라인까지 위험을 파악

Synopsys ASPM 솔루션: Security Risk Manager(SRM)

Security Risk Manager(SRM)



위험관리
- 전반적인 위험 상태
- 감사(audit) 기능

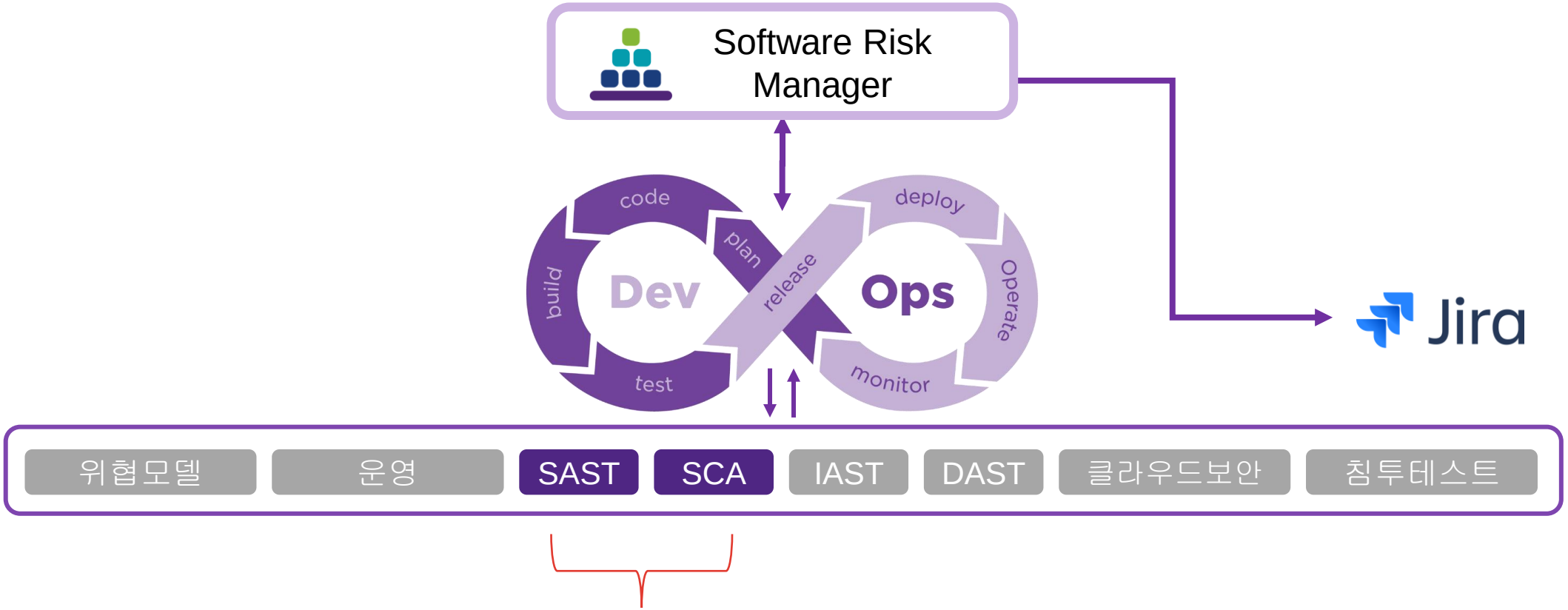
정책 – 테스트 및 수정 조율(Orchestration)
- Pre-scan
- Post-scan

우선순위 지정 및 분류심사
- 정규화 / 중복제거
- 위험수치

통합 – 135이상 및 계속 추가
- 수동 및 자동 AST
- 개발, 배포 및 운영

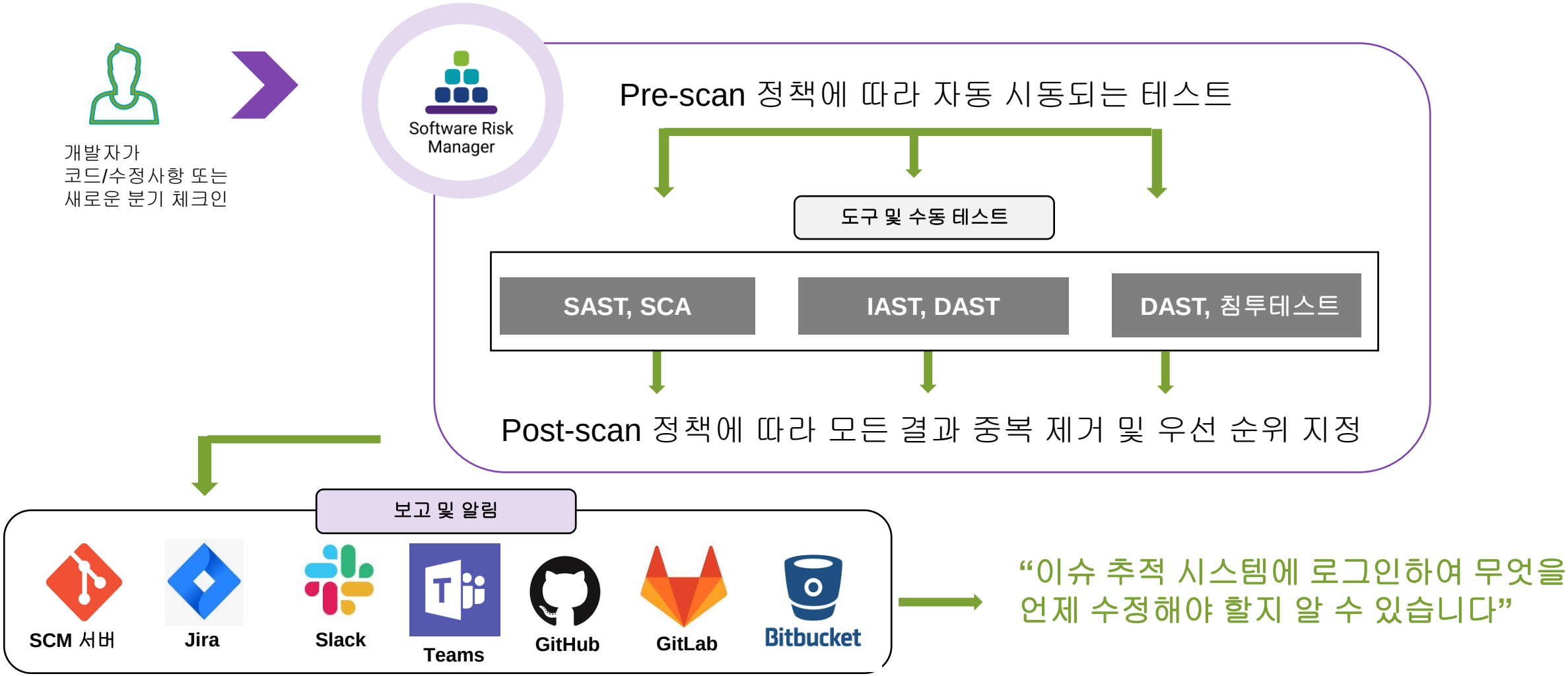
내장된 테스트 – 시장을 선도하는 스캔 엔진을 포함한 유일한 ASPM 솔루션
- SAST
- SCA

내장된 보안 테스트를 통해 위험확인이 빨라집니다



80%이상의 테스트 요구사항을 충족하고, 이슈와 소프트웨어 자산을 동적으로 발견

Software Risk Manager, 그리고 개발자!



Synopsys AppSec 솔루션

Gartner® Magic Quadrant™ 7년 연속 리더

Figure 1: Magic Quadrant for Application Security Testing

Gartner® Magic Quadrant™
7년 연속 리더

2023 Gartner® Magic Quadrant™ for Application Security Testing

Thank You


SYNOPSYS®