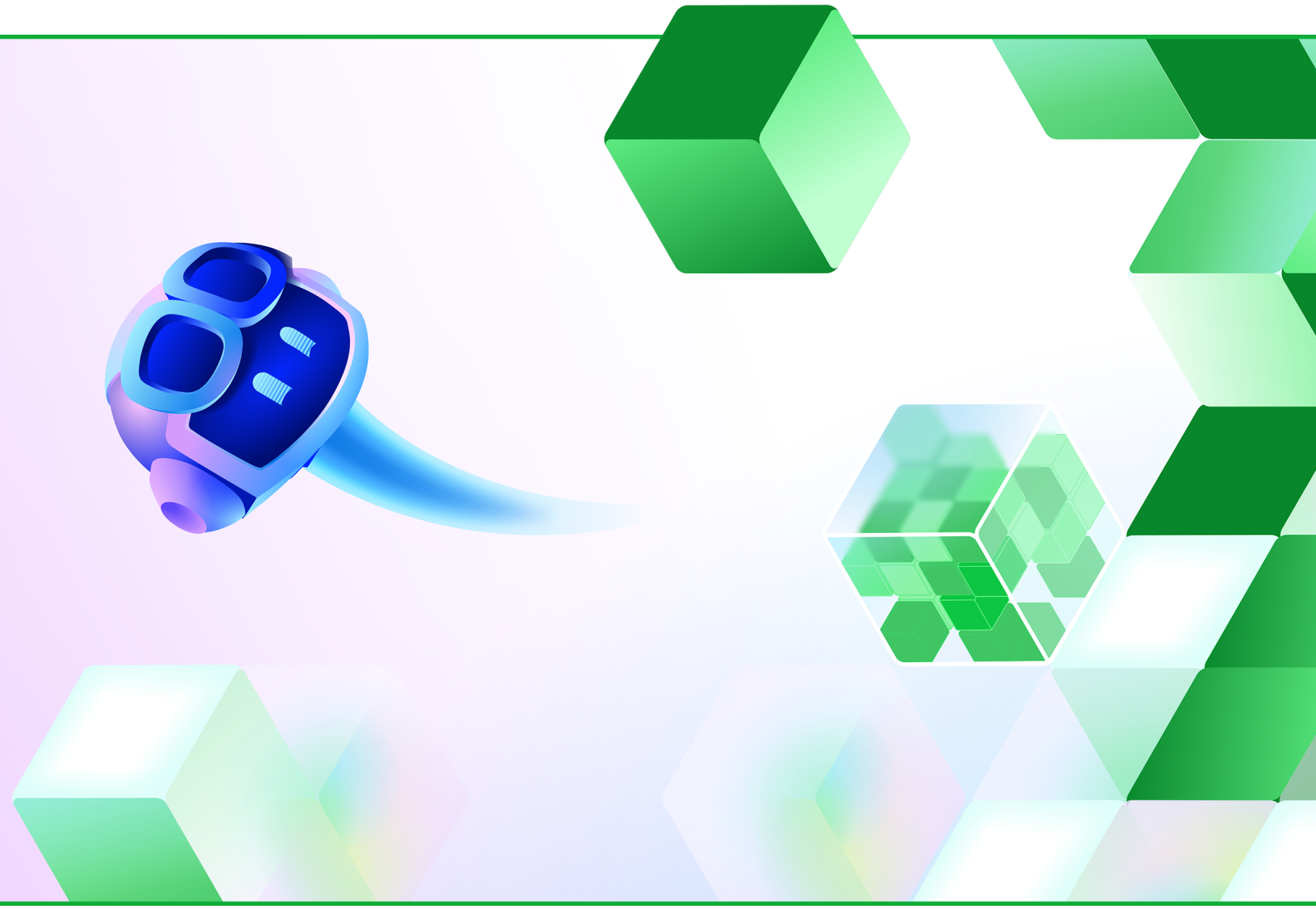
AI 기반 DevSecOps를 위한 엔터프라이즈 가이드



글: GITHUB 작성

머리말

DevSecOps는 소프트웨어 개발 수명 주기(SDLC)의 모든 단계에 보안을 통합하여 시프트 레프트를 현실로 만드는 방법론이자 실행 방식입니다. DevSecOps의 핵심은 보안 작업을 조정하는 것이며, 경우에 따라서는 과거에는 별도로 수행되었던 엔지니어링 및 보안 역할을 DevOps 워크플로에 직접 적용하는 것입니다. 따라서 DevSecOps는 보안 사고로 인한 비용과 영향을 줄이고, 팀이 보안을 강화한 소프트웨어를 더 빨리 출시할 수 있도록 지원합니다 실제로, IBM의 2023년 데이터 유출 비용 보고서에 따르면, DevSecOps를 적극적으로 도입한 조직은 그렇지 않은 조직에 비해 168만 달러의 비용을 절감할 수 있다고 합니다.

시프트 레프트의 과제

지난 10년 동안 보안 전문가들은 시프트 레프트 방식을 채택하도록 권장되어 왔지만, 같은 IBM 보고서에 따르면 조직의 내부 보안팀이 보안 침해를 파악한 경우는 33%에 불과했습니다. 이는 SDLC 전반에 걸쳐 보안을 통합하는 것이 얼마나 어려운지를 보여줍니다. 시프트 레프트를 채택하기 위해서는 코드가 생산 단계에 들어가기 전에 보안 취약점을 찾아낼 수 있을 뿐 아니라, SDLC에 원활하게 통합할 수 있는 도구가 필요합니다.

AI가 어떻게 시프트 레프트를 구현하는 방법

AI를 효과적으로 사용하면 취약점이 처음부터 작성되는 것을 방지하고, 개발자가 테스트하고 개선할 수 있는 안전한 코드 제안을 제공하고, 잠재적 취약점에 대한 컨텍스트를 제공할 수 있습니다. 이 모든 것이 개발자의 일반적인 워크플로 내에서 이루어집니다.

이 가이드가 AI 기반 DevSecOps 전략을 수립하는 데 어떻게 도움이 되는가

IBM 보고서는 DevSecOps가 기업이 데이터 유출로 인한 평균 비용을 줄이는 데 가장 큰 도움이 되었다고 결론지었습니다. 우리는 이전에 DevSecOps와 모범 사례 그리고 조직이 SDLC 전반에 걸쳐 보안 관행을 통합하는 데 도움이 되는 팁에 대해 작성한 적이 있습니다. 이제 AI가 DevSecOps 전략을 구현할 때 조직이 직면하는 핵심 과제를 완화하는 데 어떻게 도움이 되는지 살펴보겠습니다. 위험을 효율적으로 해결하고, 증가하는 보안 인텔리전스에 대한 수요를 충족하며, 최신 규제 표준을 준수하는 것입니다.

목차

DevSecOps 구현에 있어 3가지 핵심 과제 및 AI가 이를 해결할 수 있는 방법

DevSecOps 채택률이 높을수록 비용 절감 이점이 높아지지만, 기존 워크플로에 보안 도구를 사용하는 것이 아니라 보안을 SDLC에 통합하는 것이 어렵습니다.

소프트웨어 개발에 AI가 빠르게 도입되면서 DevSecOps 구현의 마찰을 줄일 수 있는 기회가 생겼습니다. Gartner**에 따르면 2027년까지 엔터프라이즈 소프트웨어 엔지니어의 50%가 머신러닝 기반 코딩 도구를 사용할 것으로 예상됩니다.** 이러한 도구의 도입은 DevSecOps 워크플로 전반에 걸쳐 AI 사용을 강화하여 보다 효율적이고 능동적인 보안 관행을 위한 기반을 마련할 것입니다.

DevSecOps 전략을 구현할 때의 핵심 과제를 살펴보고, 잠재적인 근본 원인을 논의한 다음, 조직이 사전 보안 예방 조치를 채택하는 데 도움이 될 수 있는 AI 및 자동화 솔루션을 살펴보겠습니다.

45%

(추정) 2025년까지 공급망 공격으로 인해 영향을 받을 글로벌 기업의 비율

86%

2023년 애플리케이션을 통한 인증 정보 악용 및 개인 인증 정보 악용을 통해 발생한 모든 데이터 유출 사고의 비율

#1

DevSecOps 전략은 기업이 데이터 유출로 인한 평균 비용을 줄이는 데 도움이 되는 최고의 요소입니다.

과제 1: 소프트웨어 공급망의 보안 위험 개선

금융 투자만으로는 보안 위험을 해결할 수 없습니다. 보안에 대한 투자가 증가했음에도 불구하고, 개선율은 수년간 정체되어 있습니다. Gartner는 2025년까지 전 세계 조직의 45%가 어떤 식으로든 공급망 공격의 영향을 받을 것으로 예측하고 있습니다.

2023년 Verizon 데이터 유출 조사 보고서에 따르면, 애플리케이션과 자격 증명 남용은 전체 데이터 유출 사고의 86%를 차지합니다. 또한 IBM 보고서에 따르면, 2022년 3월부터 2023년까지 도난 또는 손상된 자격 증명으로 시작된 침해 사건은 해결하는 데 가장 오랜 시간이 걸렸으며, 정확히 328일이 걸렸습니다. 심지어 마감 기한을 맞추기 위해 81%의 개발자가 취약한 코드를 출시해야 한다는 압박을 느낀다고 Osterman Research 백서에 인용되어 있습니다.

자격 증명 악용을 방지 할 수 있는 열쇠는 무엇입니까? Multi-Factor Authentication과 자동화된 보안 제어와 같은 보호 기능을 통해 플랫폼이 기본적으로 안전하게 유지되도록 하는 DevSecOps 전략을 채택하세요. IBM 보고서에 따르면, DevSecOps는 기업이 데이터 유출로 인한 평균 비용을 줄이는 데 가장 큰 도움이 되는 요소입니다.

AI와 자동화를 통한 신속한 문제 해결 방법

보안 조치를 AI로 대체하는 것이 아닙니다. 오히려 조직은 AI를 사용하여 마찰을 줄이고 보안 프로그램을 강화할 수 있습니다. 미래 지향적인 엔지니어링 리더들이 DevSecOps 플랫폼을 선택할 때 고려하는 몇 가지 AI 및 자동화 기능을 살펴보겠습니다.

- **수정 알림 자동화 및 코드 수정 제안.** 코드 스캐닝 자동 수정 기능은 풀 리퀘스트에서 취약성 경고가 있는 AI 생성 코드 수정을 제안할 수 있습니다.
- **비정형 보안 암호 보호.** 사전 정의된 파트너 패턴에 대해서만 식별되고 보호된 보안 암호를 스캔하는 대신, Secret Scanning과 같은 기능은 코드에서 비밀번호와 기타 일반적이거나 비정형 보안 암호를 감지할 수도 있습니다.
- **자동 생성 사용자 지정 패턴.** Secret Scanning은 AI를 사용하여 사용자 맞춤형 패턴을 자동 생성하고 조직에 고유한 토큰 유형을 감지할 수도 있습니다.

알고 계셨나요?

자동화된 보안 기능은 코드를 스캔할 수 있지만, 해당 기능이 SDLC의 어느 단계에 포함되는지에 따라 조직의 보안 태세가 달라질 수 있습니다. 예를 들어, 코드가 공개된 후에 스캔하여 유출된 보안 암호가 감지되면 보안 경고를 발동할 수 있습니다. 반면, 푸시 보호 기능은 코드가 조직의 리포지토리로 푸시되기 전에 보안 암호를 스캔할 수 있습니다.

푸시 보호와 같은 사전 예방적 보안 기능을 지원하는 플랫폼은 수천 건의 보안 암호 유출을 방지할 수 있습니다. 예를 들어, 내부 데이터에 따르면 GitHub Advanced Security의 푸시 보호 기능은 2022년 4월부터 12월까지 100가지 보안 암호 유형에 걸쳐 11,000건 이상의 보안 암호 유출을 방지했습니다.

과제 2: 보안 인텔리전스에 대한 긴급한 요구 충족

애플리케이션 보안 전문가

소프트웨어 개발자

ISC2(국제 정보 시스템 보안 인증 컨소시엄)의 2023년 인력 연구에 따르면, 전 세계적으로 **4백만 명의 보안 전문가**가 더 필요합니다. 개발자와 보안 전문가의 비율이 수요를 더욱 악화시키고 있습니다. **개발자 100명당 보안 연구자 1명이 조직에 속해 있습니다.** 수많은 개발자가 충분한 보안 전문가 없이 많은 코드를 생성한다면, 취약점이 간과되어 잠재적인 보안 침해가 발생할 수 있습니다.

또한, AI 코드 작성 도구를 사용할 것으로 예상되는 엔터프라이즈 소프트웨어 엔지니어가 늘어남에 따라 검토해야 할 코드가 더 많아질 것으로 예상되어 보안 전문가에 대한 수요가 더욱 증가할 것입니다. 그러나 조직은 보안 전략에 AI 보안 관행을 구현함으로써 새로운 환경에 발맞출 수 있습니다.

AI와 자동화가 보안 인텔리전스를 강화하는 방법

- **AI는 개발자가 처음부터 안전한 코드를 작성하는 데 도움이 될 수 있습니다.** AI 코드 작성 도구는 개발자가 코드를 작성하는 과정에서 보안과 엔지니어링을 결합하여 올바른 보안 결정을 내리는 데 도움이 될 수 있습니다.
- **AI는 위협을 찾아내는 수동적인 노력을 강화할 수 있습니다.** 예를 들어, 자문 데이터베이스에는 보안 연구자들이 선별한 일반적인 취약성 노출과 오픈 소스 보안 자문 내용이 포함되어 있는 경우가 많습니다. 강력한 보안 플랫폼에는 공격에 대한 데이터 로깅과 원격 측정 소스를 적극적으로 모니터링하는 보안 사고 대응 팀 외에 활발한 포상금 사냥꾼 커뮤니티가 있을 수도 있습니다. 이러한 노력을 가속화하여 보안 연구자들이 더 빨리 조사를 수행할 수 있도록 하고, 새로운 취약성을 감지하는 데 도움을 주며, 수동 프로세스를 자동화할 수 있습니다.

- **AI는 개발자에게 보안 교육과 지침을 제공할 수 있습니다.** 개발자가 보안 경고를 받으면, AI 코딩 도구와 같은 제품을 작업 공간에서 바로 사용하여 문제를 파악할 수 있습니다. 즉, 개발자들이 웹에서 답을 찾기 위해 워크스페이스를 떠나지 않고도 코딩 과정에서 보안 문제에 대해 배울 수 있습니다. 개발자들은 AI 도구를 사용하여 코드베이스에 맞는 취약성 사례를 생성함으로써 보안 개념에 익숙해질 수 있습니다. 이처럼 실용적이고 직접적인 학습 경험을 통해 개발자들은 보안 문제가 코드에서 어떻게 나타나는지 이해할 수 있습니다.

집단 지능형 보안 정보를 대규모 결과로 전환하는 3단계 방법

Linux Foundation의 Global Spotlight 2023 보고서에 따르면, 전 세계 조직의 90%가 오픈 소스 소프트웨어(OSS)를 사용하고 있습니다. 또한, Linux Foundation은 OSPO 또는 OSS 이니셔티브를 구현할 계획인 기업의 72%가 향후 12개월 이내에 이를 구현할 것으로 예상하고 있습니다.

OSS 보안을 유지하는 것은 집단적인 문제이며 집단적인 책임입니다. 즉, 소프트웨어에 의존하는 대규모의 다양한 개발자, 조직, 개인, 오픈 소스 관리자, 보안 전문가 모두가 이해관계자가 된다는 의미입니다. 이것이 왜 중요한가요? **오픈 소스는 더 큰 규모의 보안 인텔리전스 풀을 생성합니다.**

다음은 집단적인 보안 인텔리전스를 대규모의 결과로 전환하는 세 가지 팁입니다.

1. **엔지니어링 팀에 실무 중심의 보안 학습 및 개발을 제공합니다.** 위에서 언급한 바와 같이, AI 페어 프로그래머는 특정 코드에 맞춰 취약성 사례를 생성함으로써 개발자들이 더 많은 보안 개념을 배울 수 있도록 도와줄 수 있습니다. Secure Code Game과 같은 무료 대화형 교육 세션은 개발자들에게 실제 코드에서 취약한 패턴을 발견하고 수정하는 방법, 워크플로에 보안을 구축하는 방법, 코드에 대해 생성된 보안 경고를 이해하는 방법을 가르쳐 줍니다.

2. **퍼블릭 자문 데이터베이스를 활용하여 비공개 리포지토리를 보호합니다.** 엔지니어링 리더는 퍼블릭 자문 데이터베이스의 보안 인텔리전스를 활용하는 플랫폼을 선택해야 합니다. 이러한 플랫폼은 조직의 코드에 영향을 미치는 취약성이나 멀웨어에 대한 자문 보고서가 게시될 때 경고 알림을 생성할 수 있습니다.
3. **AI를 통해 OSS 패키지의 이해와 모델링을 가속화합니다.** OSS에는 수천 개의 패키지가 있으며, 그 패키지에는 개발자에게 익숙하지 않은 API가 포함되어 있는 경우가 많습니다. 그러나 이러한 패키지를 이해하고 모델링하는 것이 OSS 생태계를 안전하게 유지하는 방법입니다. 보안 및 엔지니어링 팀은 API를 수동으로 모델링하는 대신 AI 도구를 사용하여 더 많은 패키지를 식별하고 더 많은 취약점을 감지할 수 있습니다. GitHub의 보안 연구팀이 AI 모델링을 사용하여 새로운 취약점을 발견한 방법을 알아보세요.

GitHub: 안전한 소프트웨어를 구축, 확장, 제공하기 위한 AI 기반 개발자 플랫폼

1억 명 이상의 개발자와 Fortune 100대 기업 중 90% 이상이 소프트웨어 프로젝트를 구축, 유지, 기여하는 데 GitHub를 사용하고 있습니다. 개발자들에게 최신 AI 혁신 기술을 제공하여 개발 워크플로에 직접 보안을 포함시키는 것까지, GitHub는 엔지니어링 팀이 안전한 소프트웨어를 구축하고 제공할 수 있도록 필요한 모든 것을 제공합니다.

팀이 GitHub를 선택하는 이유 알아보기.

과제 3: 점점 더 엄격해지는 규정 준수 및 규제 기준 충족

조직들은 데이터와 사용자의 보안과 기밀성을 보장하는 규정 준수 및 규제 요건에 직면하고 있습니다. 이러한 표준은 심각한 데이터 유출과 사이버 공격의 위험을 최소화하기 위해

고안되었으므로, 규정 준수를 입증하면 기업이 개인 데이터 보호에 전념하고 있다는 것을 고객에게 확신시킬 수 있습니다.

다음은 이러한 규제 표준 중 몇 가지를 간략하게 소개한 것입니다.

이름	표준
안전하고, 신뢰할 수 있으며, 믿을 수 있는 AI에 관한 행정 명령	미국 바이든 행정부가 2023년 10월에 발표한 이 행정명령은 미국이 AI를 설계, 개발, 배치하기 위한 로드맵을 제공합니다. 이 행정 명령은 신뢰할 수 있는 AI 시스템의 개발과 사용을 강조합니다. 또한, AI 개발 및 배치에 있어 연방 정부, 민간 부문, 학계, 기타 이해관계자 간의 파트너십을 장려합니다.
국가 사이버 보안 개선에 관한 행정 명령	2021년 5월에 바이든 행정부가 서명한 이 행정 명령은 사이버 보안 관행을 강화하고, 더 높은 수준의 소프트웨어 공급망 보안을 설정하는 표준, 지침, 절차를 개발할 것을 요구합니다.
HIPAA(건강보험 양도 및 책임에 관한 법률)	이 미국 법은 보호 대상 건강 데이터를 취급하는 모든 미국 기업이 건강 데이터에 안전하게 전자적으로 접근할 수 있도록 하고, 미국 보건복지부가 정한 개인정보 보호 규정을 준수하도록 규정하고 있습니다.
GDPR(일반 데이터 보호 규정)	이 EU(유럽연합) 규정은 기업이 개인 데이터를 수집하고 처리하는 방법에 대해 엄격한 규칙을 적용하고 있으며, EU 회원국 내에서 발생하는 거래에 대해 EU 시민과 거주자의 개인 데이터와 프라이버시를 보호하도록 의무화하고 있습니다(기업 자체가 EU에 기반을 두고 있지 않더라도).
PCI DSS(Payment Card Industry Data Security Standard)	PCI 보안 표준 위원회가 관리하는 이 표준은 주요 카드 협회의 브랜드 신용 카드를 취급하는 조직을 위한 글로벌 정보 보안 표준입니다.

AI와 자동화가 규정 준수를 간소화하는 방법

이러한 표준을 준수하면 경쟁 우위를 확보할 수 있으므로, 조직은 규정 준수 여부를 평가 및 유지하고 감사에 대한 상세한 보고서를 제공할 수 있는 효과적인 솔루션이 필요합니다. 다음은 **보안 도구가 지원해야 하는 주요 규정 준수 작업과 AI와 자동화가 그 과정을 간소화하는 데 어떻게 도움이 되는지에 대한 설명입니다.**

- **가시성.** 환경에 대한 거시적 수준의 가시성을 제공하는 대시보드는 조직의 보안 태세의 전반적인 상태와 추세를 측정하는 데 매우

중요합니다. 대시보드는 SDLC에서 경고를 쉽게 찾을 수 있도록 함으로써 위험 추적, 개선 및 예방을 지원합니다. 또한 대시보드는 어떤 팀이 개선에 가장 효과적인지, Secret Scanning 푸시 보호와 같은 자동화 및 AI 기능으로 어떤 종류의 취약성을 예방하고 있는지 강조할 수 있습니다. 그뿐만 아니라, 조직의 리포지토리에서 코딩 스캔을 기본적으로 활성화하면 코드베이스를 자동으로 모니터링할 수 있습니다.

- **보고.** 최고의 솔루션은 팀이 업계 표준을 준수할 수 있도록 자동화하는 데 도움을 줄 뿐만 아니라, 감사관과 공유할 수 있는 취약성 및 규정 준수 문제에 대한 상세한 보고서를 제공합니다. 상세한 감사 로그, 규정 준수 보고서, 통합에 쉽게 액세스할 수 있는 플랫폼은 조직의 내부 및 외부 규정 준수 노력을 지원합니다.
- **규정 준수 관리.** ISO 27701, ISO 27018과 같은 International Organization for Standardization(ISO)의 인증과 STAR (Security, Trust & Assurance Registry)와 같은 Cloud Security Alliance의 인증은 소프트웨어 개발의 데이터 보호 요구 사항을 지원하고, 개발자가 클라우드 서비스의 데이터 보호를 위한 모범 사례를 따르도록 하며, 클라우드 서비스의 보안을 평가합니다. 이러한 인증을 획득하고 유지하는 것은 데이터 보호 및 보안의 높은 기준을 유지하겠다는 약속을 확인하는 것입니다.

네이티브 AI와 자동 보안 기능을 갖춘 플랫폼을 선택하면 조직이 높은 기준을 충족하는 동시에 긍정적인 DevSecOps 경험을 창출할 수 있습니다. 이러한 도구는 사용자 맞춤형 및 자동 분류 규칙을 통해 보안 경고에 우선순위를 부여함으로써 문제 해결을 가속화하고, 조직이 환경에 도입되기 전에 안전하지 않은 종속성을 파악할 수 있도록 하며, 조직에 종속성 라이선스, 변경 사항, 프로젝트 사용 및 취약성에 대한 정보를 제공합니다.

GitHub Advanced Security로 보안 태세 개선

종속성 검토, 코드 및 보안 암호 스캔과 같은 GitHub Advanced Security 기능을 활용함으로써 조직은 제3자 라이브러리와 종속성을 더 잘 관리하고, 보안 기능을 SDLC에 직접 통합하여 워크플로를 최적화하고, 다양한 산업 규정을 준수할 수 있습니다.

오늘 코드를 보호하세요

AI를 활용한 DevSecOps 전략 구현

개발자의 워크플로를 보호하고 DevSecOps를 도입해야 하는 이유는 무엇일까요? 소프트웨어는 코드로 시작되기 때문입니다. 레프트 시프트 전략을 채택하고 SDLC의 모든 단계에 보안을 심층적으로 통합하는 조직은 DevSecOps를 거의 도입하지 않거나 전혀 도입하지 않는 조직에 비해 168만 달러의 비용을 절감할 수 있습니다.

그러나 위에서 논의한 바와 같이, 성공적인 DevSecOps 전략을 실행하는 데는 낮은 수정률, 보안 전문가에 대한 수요 증가, 증가하는 규정 준수 및 규제 표준 충족 필요성 등 여러 가지 문제가 있습니다.

AI와 자동화가 DevSecOps를 현실로 만드는 데 도움이 될 수 있는 분야는 다음과 같습니다.

- **수정 작업의 신속화.** AI 코드 작성 도구는 개발자가 처음부터 더 안전한 코드를 작성하는 데 도움이 될 수 있으며, 보안 도구는 수정 작업 경고를 자동화할 수 있습니다. 이 두 가지 기능을 결합하면 개발자의 수정 작업 워크플로를 간소화하고 생산성을 높이는 AI 생성 코드 수정 제안이 포함된 경고를 제공할 수 있습니다.
- **집합적 보안 인텔리전스 강화.** 보안 연구자들이 AI를 사용하여 더 빠르게 조사하고 새로운 취약점을 감지할 수 있도록 합니다.
- **개발자 보안 교육 개선.** 개발자가 코딩 과정에서 보안 문제에 대해 배울 수 있는 AI 페어 프로그래머와 코드베이스에 맞게 조정된 실습 예제를 활용합니다.
- **모니터링, 보고, 규정 준수 관리 개선.** AI와 자동화 도구를 사용하면 감사 로그를 쉽게 가져오고 보안 경고에 우선 순위를 지정할 수 있으므로 조직은 높은 규정 준수 표준을 충족하고 유지하면서 DevSecOps 경험을 개선할 수 있습니다.

AI와 자동화 보안 도구는 개발자의 책상에서 코드를 보호하는 데 중요한 역할을 할 수 있습니다. 그 결과, 위험 감소, 더 빠른 탐지 및 수정, 더 안전한 소프트웨어의 더 빠른 배포가 가능합니다.

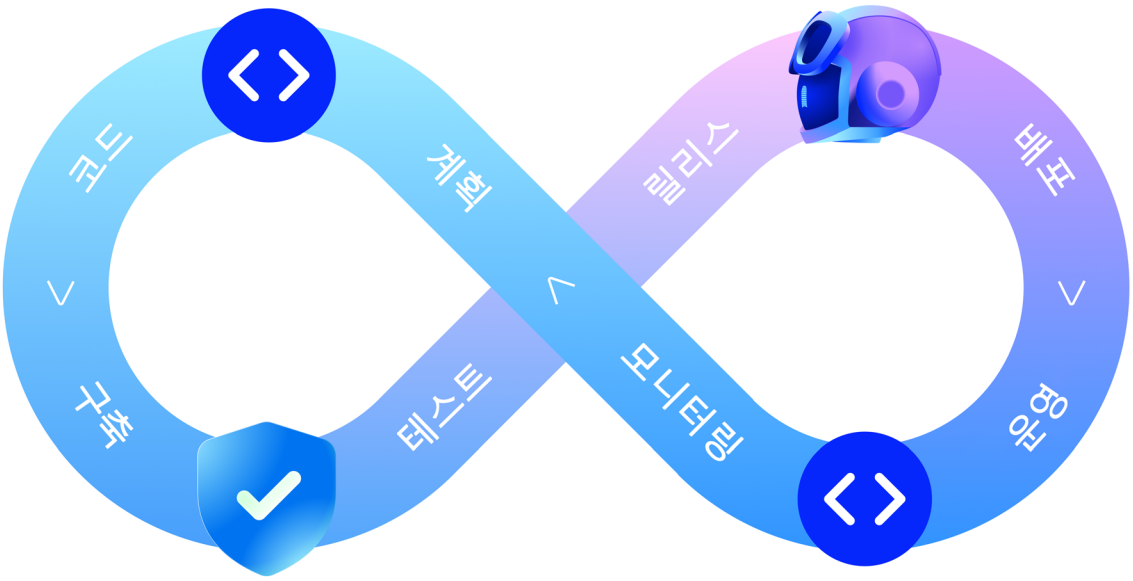
GitHub가 도와드립니다.

GitHub Advanced Security를 사용하면 조직의 보안 태세를 개선하고, 워크플로를 최적화하며, 다양한 규정과 표준을 사전에 준수할 수 있습니다. AI 기반 보안 기능은 엔지니어링 팀에 원활한 DevSecOps 경험을 제공하여 기업이 제품을 더 안전하고 빠르게 제공할 수 있도록 합니다.

GitHub Advanced Security에 대해 자세히 알아보기

SDLC의 모든 단계에서 AI 기반 보안 통합: 다이어그램

SDLC 전반에 걸친 보안 통합은 DevSecOps 전략을 구현할 때 마찰을 줄이는 데 도움이 될 수 있습니다. 아래 다이어그램은 GitHub 플랫폼이 어떻게 보안, AI, 자동화 도구 및 리소스 제품군을 제공하여 DevSecOps 경험을 향상시키는지를 보여줍니다.



계획 수립

GitHub Issues와 GitHub Projects는 통합된 도구 세트를 제공하여, GitHub 내에서 바로 프로젝트를 계획, 구성, 추적, 관리할 수 있도록 함으로써, 모든 프로젝트 관리 과정을 간소화합니다. 예를 들어, 프로젝트 매니저는 GitHub Project 보드를 만들어 보안 관련 이슈와 풀 리퀘스트의 추적을 자동화할 수 있습니다.

코드 작성

GitHub Copilot은 안전한 관행을 권장하고, 오류를 조기에 발견하며, 일반적인 코딩 오류를 최소화함으로써 개발자가 처음부터 더 안전한 코드를 작성할 수 있도록 도와줍니다. AI는 코드 작성을 지원하는 데 사용되며 철저한 보안 검토와 좋은 코딩 관행을 대체해서는 안 된다는 점을 유의해야 합니다.

구축

Codespaces는 기본적으로 안전하게 설계된 일관된 사전 구성된 빌드 환경을 여러 팀의 개발자에게 제공합니다.

테스트

GitHub Advanced Security 및 GitHub Packages는 함께 사용하면 테스트 과정을 간소화할 수 있습니다. 예를 들어, GitHub Advanced Security 기능은 개발자가 코드 변경 사항을 병합하기 전에 보안 문제를 해결하고, 보안 암호를 리포지토리에 푸시하기 전에 감지하며, 의존성에서 잠재적인 보안 위험을 찾아 해결하는 데 도움이 됩니다. 한편, GitHub Packages는 개발자들이 소프트웨어 패키지를 호스팅할 수 있도록 함으로써 테스트를 위한 실제 환경을 보다 쉽게 복제할 수 있게 해 줌으로써 테스트의 효율성을 향상시킵니다.

릴리스

GitHub Advanced Security 기능은 배포되기 전에 코드에 민감한 정보가 포함되어 있지 않은지 확인합니다. 개발자들은 비밀 스캐닝의 AI 기능을 사용하여 조직에 고유한 비밀 유형을 보호하기 위한 사용자 맞춤형 패턴을 생성할 수 있습니다.

배포

GitHub Actions 및 GitHub Mobile은 향상된 보호 기능과 빠른 응답 기능을 제공하여 보다 안전한 배포 프로세스를 만듭니다. 예를 들어, 조직은 코드가 푸시되거나 풀 리퀘스트가 이루어질 때마다 GitHub Actions를 사용하여 린터, 정적 분석 도구 또는 보안 취약점 스캔을 자동으로 실행할 수 있습니다. GitHub Mobile은 배포 기능을 제공하지 않지만 배포 프로세스를 모니터링하고 배포 중에 수동 개입이 필요한 경우 신속하게 대응하는 데 사용할 수 있습니다.

운영 및 모니터링

GitHub Actions, Dependabot와 같은 도구를 사용하면 조직이 보안 취약점을 효율적이고 시기적절하게 식별, 수정, 예방할 수 있습니다. 예를 들어, GitHub Actions는 보안 점검 및 스캔 실행과 배포 프로세스를 자동화하여 테스트를 거친 안전한 코드만 배포되도록 할 수 있습니다 GitHub Advanced Security의 의존성 검토 및 Dependabot은 의존성 변경, 프로젝트 통합 및 취약성을 모니터링합니다. GitHub Advanced Security의 코드 스캔 자동 수정 기능은 풀 리퀘스트에서 취약성 경고와 함께 AI로 생성된 코드 수정을 제공할 수 있습니다.