개발팀 생산성 저해하는 위협 3가지, 해결방안 3가지

생산성은 어느 산업에서나 성공을 가늠하는 중요한 이슈입니다. 소프트웨어 제품을 만드는 일에서도 마찬가지인데요, 효율적으로 생산하는 것뿐만 아니라 사이버 공격으로부터 안전하게 만드는 것도 중요합니다. 소프트웨어 팀의 생산성을 끌어올리는 방법에 대해 고민하고 있다면 아래 내용을 눈여겨볼 필요가 있습니다. 팀의 생산성을 저해하는 대표적 위협과 그를 해결하는 방법에 관해 설명하고자 합니다.



1. 속도를 내야 한다는 압박

프로젝트 매니저가 소프트웨어 개발팀에 비현실적이고 불가능한 데드라인을 제시할 때가 있습니다. 특히 고객 요구사항이 있을 때 매니저들이 개발자를 압박하곤 합니다. ‘예상 시점’을 제시하면서 말이죠. 그러나 그 예상 시점이란 거의 마감 시간이나 마찬가지인 경우가 많습니다. 그러면 개발자는 스트레스를 받게 되고, 업무를 수행할 수 있는 최고 수준의 능력을 발휘하지 못하게 됩니다.

궁극적으로는 고객의 기대치를 관리하는 것입니다. 고객에게 늦어질 수 있는 작업이라는 걸 인식시키는 게 필요합니다. 더 나은 제품 퀄리티를 위해서 정밀한 테스트가 이루어진다는 점을 인식시키세요. 커뮤니케이션과 그에 따른 상호 간의 이해가 개발팀의 업무 환경을 완전히 다르게 만들어낼 수 있습니다.

2. 저급한 품질의 코드

저급한 코드란 여러 가지 형태로 나타납니다. 다른 개발자들이 읽기 힘들어서 필수적인 수정을 못 하게 만드는 코드인 경우가 대표적입니다. 또는 개발팀이 마감 시간을 맞추느라 시간에 쫓겨서 충분한 테스트나 디버깅을 못 한 채 소프트웨어를 배포해버리는 경우를 의미하기도 합니다.

저급한 품질의 코드는 생산성을 떨어뜨리고 개발 기간이 늘어나는 데 영향을 줍니다. 코드 품질을 좋게 만들려면 코드의 표준을 지키고, 코드를 꼭 테스트하며, 프로젝트를 지속적으로 관리할 프로젝트 매니저를 한 명 선정하는 것이 필요합니다.

3. 유행 지난 기술

새로운 기술들은 직원들이 더 효율적으로 업무를 수행할 수 있도록 해 주고, 프로젝트 시간을 절약해 주기도 하며, 일반적으로 고객을 만족시키고, 경쟁사보다 사업을 활발히 수행할 수 있도록 지원하기도 합니다. 성공적인 개발팀은 최신 기술을 이용하여 더 빠르고 안전하게 업무를 수행합니다.

다국적 회계법인인 Price Waterhouse Cooper (PWC)가 북미와 유럽 등 여러 국가를 대상으로 약 12,000명을 조사하였습니다. 조사에 참여한 사람들은 C레벨 수준의 역할에서 어드민까지, 여러 업계에 종사하는 사람이었습니다. PWC는 90%의 C레벨 임원진은 직원들이 일하는 데 필요한 기술을 사용하고 있다고 믿고 있었습니다. 그러나 실무자들의 53%만이 그렇다고 답했습니다.

또한 92%의 임원진이 가장 중요한 프로젝트를 수행하는 데 제공되는 기술들에 만족한 반면, 실무자들의 63%만이 그에 동의했습니다. 이 결과를 보면, 경영진과 실무자들 사이 간극이 있음을 알 수 있습니다. 사용된 기술이 실패할 경우, 임원진은 문제를 다른 사람에게 넘겨서 해결하고자 합니다. 그러나 담당자들은 유행 지난 구식 기술의 문제를 처리해야만 합니다.

4. CI/CD 파이프라인

CI/CD 파이프라인은 CI와 CD로 구성됩니다. CDI는 Continuous integration의 약자로, 한국말로는 ’지속적 통합’으로 해석됩니다. 소프트웨어 개발 과정에서 빈번하게 코드 체크를 하면서 사소한 코드 수정을 계속해가는 작업이라고 할 수 있습니다. 또한 개발자들이 코드를 개발할 때 사용하는 여러 가지 도구와 플랫폼들을 통합하는 것을 요구합니다.

CD는 Continuous delivery, 즉 ‘지속적 배포’를 의미합니다. 테스트 및 개발 등 생산 프로세스의 하부 구조를 형성하는 다양한 환경에 애플리케이션 패키지를 자동으로 배포하는 것입니다. 코드 변경이 하위 구조 환경으로 이동하는 방식을 자동화합니다. 한마디로 지속적 배포는 소프트웨어가 언제든지 신뢰 가능한 수준으로 출시될 수 있게 보증한다고 할 수 있습니다.

CI/CD 방법론을 익히면 개발팀이 더 좋은 코드를 만들고 더 효율적인 커뮤니케이션을 할 수 있게 됩니다.

5. 시큐어 데브옵스(Secure DevOps)

오늘날 점점 디지털화되는 세계에서 사이버 보안은 모든 산업군이 직면하는 과제입니다. 소프트웨어 기업에 사이버 보안은, 고객이 소프트웨어 패키지를 구매한 후 발생하는 단순한 문제가 아닙니다. 사이버 보안은 소프트웨어 개발의 모든 측면에 스며들어 있습니다. 따라서 소프트웨어 기업은 설계, 빌드, 테스트, 배포, 지원 및 유지보수 등 모든 개발 단계에서 보안을 따져봐야 합니다.

개발자들은 빨리 코드를 배포하기 원하지만, 배포된 코드가 안전하지 않다면 속도가 빠른 건 무용지물입니다. 한편 개발자들이 보안을 통제할 수 있다고 믿다가 더 큰 문제를 야기하는 경우도 발생합니다. 시큐어 데브옵스는 개발과 보안 사이의 균열을 해소할 수 있습니다.

개발 주기 초기에 보안 테스트를 자동화하면 개발자는 코드 결함을 미리 발견하게 됩니다. 시큐어 데브옵스는 궁극적으로 소스 코드를 배포하는 속도를 더 빠르게 할 수 있습니다.

6. 취약성 테스트를 위한 적절한 솔루션

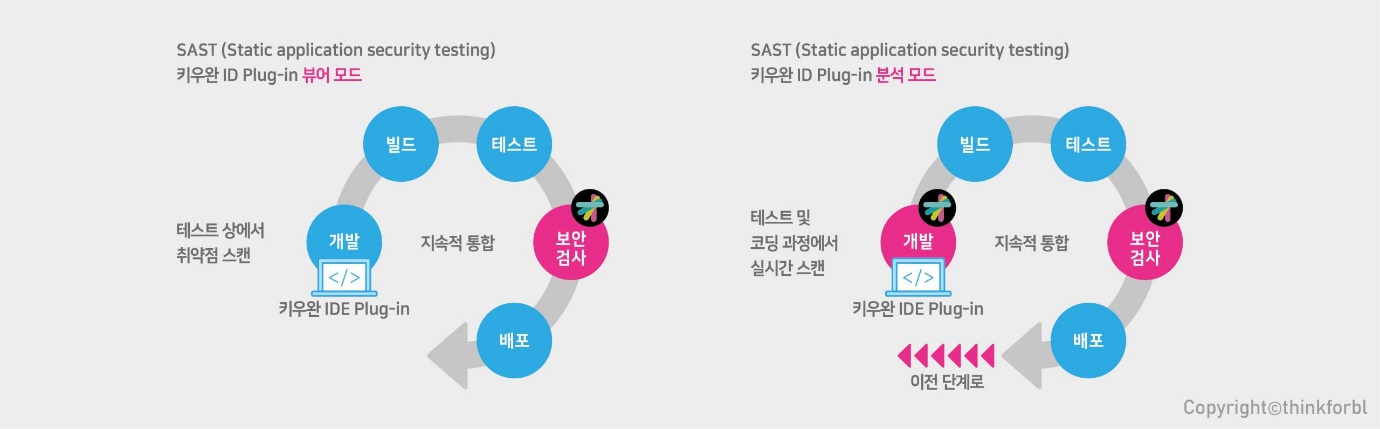
사이버 보안에 대한 위협의 강도가 높아질수록, 취약성 평가는 소프트웨어 앱 보안에서 아주 중요한 과정이 됩니다. 특히 자동화된 취약성 테스트는 수동 테스트에 비해 뚜렷한 이점이 있습니다.

자동화된 취약성 테스트는 일회성 또는 연속 검색의 형태를 취할 수 있고, 검사에서는 SaaS 모델 또는 on-premise 모델을 사용할 수 있습니다. 한 마디로 다양한 형태의 테스트가 가능합니다.

한편 자동화된 취약성 테스트는 불량 코드를 검색하고 차단할 수 있게 해주기 때문에, 개발팀이 코드를 최대한 효율적이고 안전하게 만드는 걸 돕습니다.

키우완의 코드 보안 솔루션은 SAST 기술을 사용합니다. 코드를 스캔하여 소스 코드를 분석하고 코드가 사이버 공격에 취약한 지점이 어딘지를 파악하는 방식입니다. 키우완은 OWASP(Open Web Application Security Project) 및 CWE(Common Pulse Enumeration)와 같은 엄격한 보안 표준을 준수합니다. 또한 모든 중요한 언어를 인식하기 때문에 모든 데브옵스 도구와 통합될 수 있습니다.

일회성 검색은 보안 검사를 수행하기에 적합하고, 연속 검색은 무제한 검색 기능을 제공하며 보안을 지속적으로 모니터링하는 데 좋습니다. 그리고 플러그-인 기능으로 개발환경과 통합될 수 있습니다. 그리고 소프트웨어와 CI에 통합되어 라이프사이클 관리 형태를 제공할 수 있습니다.



키우완 같은 SAST 보안 솔루션은 취약점을 개선하고 라이센스 컴플라이언스를 모니터링하면서 보안을 자동화합니다. 즉 적절한 솔루션을 사용하는 것이 개발팀이 만든 소스코드의 취약점을 없애고 안전하게 소프트웨어를 배포할 수 있는 단초라고 할 수 있겠습니다.

이상으로 개발팀의 생산성을 떨어뜨리는 요소엔 어떤 것이 있는지, 그 해결방안은 무엇인지 알아보았습니다! 더 많은 정보를 원하신다면 [Kiuwan Blog 원문](https://www.kiuwan.com/software-development-team-productivity/)에서 확인하실 수 있습니다.