

DevSecOps - безопасность

DevSecOps является методологией, которая интегрирует практики безопасности в процесс разработки программного обеспечения, обеспечивая безопасность на всех этапах цикла разработки и эксплуатации. Эта модель подчеркивает совместное участие команд безопасности, разработки и операций с целью создания более безопасных приложений и инфраструктур.

Объединение DevSecOps и CI/CD

DevSecOps стремится встроить безопасность в каждую стадию конвейера CI/CD. Он не только обеспечивает укрепление конвейера, например, путем стандартизации доступа и ролей, но и гарантирует, что инструменты сборки, такие как Jenkins, укреплены против угроз безопасности. Это включает в себя проверку артефактов, анализ кода и проверку соответствия.

Этапы и меры безопасности

Во время различных этапов разработки:

- 1. **Кодирование:** Проведите сканирование кода на наличие уязвимостей или встраиваемых секретов, таких как ключи доступа.
- 2. **Сборка:** Интегрируйте инструменты безопасности и метки для идентификации артефактов.
- 3. **Тестирование:** Проверьте, соблюдаются ли стандарты безопасности и проходит ли система тесты на безопасность.
- 4. **Развертывание:** Регистрируйте компоненты безопасности и проводите проверки целостности, чтобы обнаружить любые несанкционированные изменения.
- 5. **Мониторинг:** Устанавливайте и следите за стандартами безопасности, выполняйте непрерывные аудиты и валидацию.

Внедрение DevSecOps в CI/CD позволяет командам быть уверенными в том, что приложения и инфраструктура соответствуют стандартам корпоративной безопасности, уменьшая риск сбоев и улучшая общую эффективность и гибкость. Это обеспечивает баланс между инновационными темпами DevOps и строгими требованиями безопасности, позволяя организациям быть более гибкими и реактивными при обеспечении безопасности на уровне, соответствующем масштабам организации.