УДК 004.056

АНАЛИЗ МЕТОДОВ И АЛГОРИТМОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ТЕХНОЛОГИИ DEVSECOPS

Баландин А.К. (Университет ИТМО),
Научный руководитель – Ищенко А.П.
(Университет ИТМО)

Введение. В различных IT компаниях всё больше в разработке используют методологию DevOps. Её целью является объединение разработки, обеспечения качества, развертывание и интеграция кода. DevSecOps – развитие методологии DevOps, где помимо автоматизации затрагиваются вопросы обеспечения не только качества и надёжности кода, но и как результат – безопасность программного обеспечения или услуги на всех этапах жизненного цикла приложения.

Основная часть. В ходе работы над проектом были выполнены следующие задачи:

1. Проведен анализ отличий DevSecOps от DevOps, а именно алгоритмов и методик, которые делают цикл разработки в рамках DevSecOps, безопасным
2. Анализированы выявленные алгоритмы для определения целей их использования и эффективности
3. Определены инструменты, которые позволяют имплементировать выявленные алгоритмы

Методология DevOps — набор инструментов, который позволяет создать конвейер непрерывной интеграции и непрерывной доставки: автоматических систем тестирования, инфраструктуры для написания и развёртывания кода, программ для передачи кода между разными командами.

DevSecOps – это практика интеграции тестирования безопасности в каждый этап процесса разработки программного обеспечения.

Практика DevSecOps дает несколько преимуществ.

- Раннее обнаружение уязвимостей в программном обеспечении
- Сокращение времени выхода на рынок
- Соответствуйте нормативным требованиям
- Безопасная разработка новых функций

Основные подходы Sec (обеспечения безопасности) в DevSecOps.

- Сдвиг влево– это процесс проверки уязвимостей на ранних этапах разработки программного обеспечения.
- Сдвиг вправо- указывает на важность сосредоточения внимания на безопасности после развертывания приложения.
- Используйте автоматизированные инструменты безопасности
- Повышайте осведомленность о безопасности - каждый член команды, участвующий в разработке приложений, должен нести ответственность за защиту пользователей программного обеспечения от угроз безопасности.

Команды DevSecOps используют следующие инструменты DevSecOps для оценки недочетов в безопасности во время разработки программного обеспечения, их обнаружения и оповещения о них.

- Статическое тестирование безопасности приложений (SAST) - Инструменты статического тестирования безопасности приложений (SAST) анализируют и находят уязвимости в исходном коде.
- Анализ состава программного обеспечения – это процесс, который автоматизирует обеспечение видимости использования программного обеспечения с открытым исходным кодом (OSS) с целью управления рисками, обеспечения безопасности и соответствия лицензиям.
- Интерактивное тестирование безопасности приложений (IAST) – используются для оценки потенциальных уязвимостей приложения в рабочей среде. IAST состоит из специальных мониторов безопасности, которые запускаются из приложения.
- Динамическое тестирование безопасности приложений (DAST) - Инструменты, которые имитируют хакеров, тестируя безопасность приложения извне сети.

Выводы. В результате работы было проведено исследование методологии DevSecOps, и в частности алгоритмов обеспечения безопасности, которые используются в рамках методологии. Рассмотренные алгоритмы были сопоставлены с инструментами, которые помогают имплементировать их во время разработки программного обеспечения и на всех этапах жизненного цикла приложения или программного обеспечения.

Список использованных источников:

1. «Что такое DevSecOps?», [Электронный ресурс] URL: https://aws.amazon.com/ru/what-is/devsecops/ (дата обращения: 10.01.2023)

2. «Что такое DevSecOps и какова его роль в CD?», [Электронный ресурс] URL: https://www.jetbrains.com/ru-ru/teamcity/ci-cd-guide/what-is-devsecops/ (дата обращения: 10.01.2023)

3. Джим Бёрд «DevOpsSec», 2016 г

Баландин А.К. (автор) Подпись

Ищенко А.П. (научный руководитель) Подпись