Как сделать разработку безопасной без сноса несущих конструкций?

визитка

Алексей Бегаев
основатель АО “ИНСЕК”

сайт

inseq.ru

Типовые недостатки процессов разработки

- отсутствие автоматизации тестирования и развертывания
- иллюзия безопасности
- противостояние DevOps и Security команд
- отсутствие единообразия кода
- отсутствие политики выпуска релизов
- несоответствие нормативным требованиям
- сложность в подборе мер для соответствия нормативным требованиям

Secure Development Pipeline System

- Внедрение комплексной системы безопасной разработки на основе популярных решений с открытым исходным кодом
- Автоматическое тестирование безопасности приложения (DAST, SAST, IAST)
- Внедрение CI/CD конвейеров
- Формирование культуры информационной безопасности в команде
- Учет требований нормативных документов и лучших практик в цикле безопасной разработки
- Использование ролевой модели

Совместимые анализаторы

Анализаторы секретов

- Git-secrets
- gitLeaks
- Spectral
- Gittyleaks
- Git-all-secrets

Анализаторы зависимостей

- OWASP Dependency-Check
- Bundler-audit
- gemnasium

Статические анализаторы кода

- AKBC-3
- AppChecker
- Svace
- PHP-scan
- SonarQube

Динамические анализаторы кода

- AKBC-3
- Блесна
- ИСП SyDr
- OWASP ZAP
- Acunetix

Фаззинг-тестирование

- СПИН-Фаззер
- ИСП Fuzzer
- AFL
- AFL++
- Honggfuzz
- Boofuzz

Анализаторы контейнеров

- Clair
- Trivy
- Anchore
- Dagda

Тестирование в реальном времени

OpenRASP

AKVS

trivy

PHP Scan online code scanner

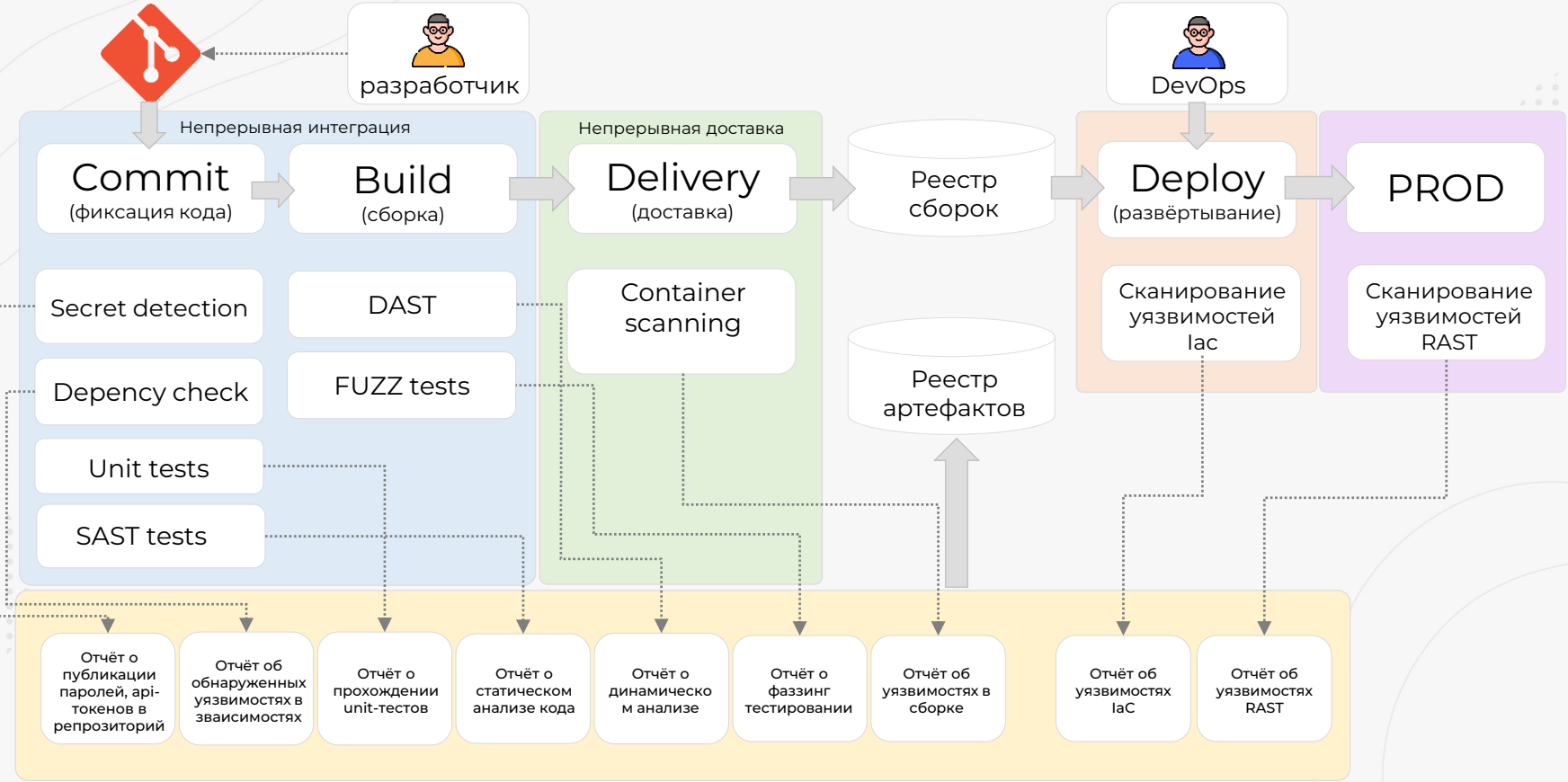
sonarqube

ZAP

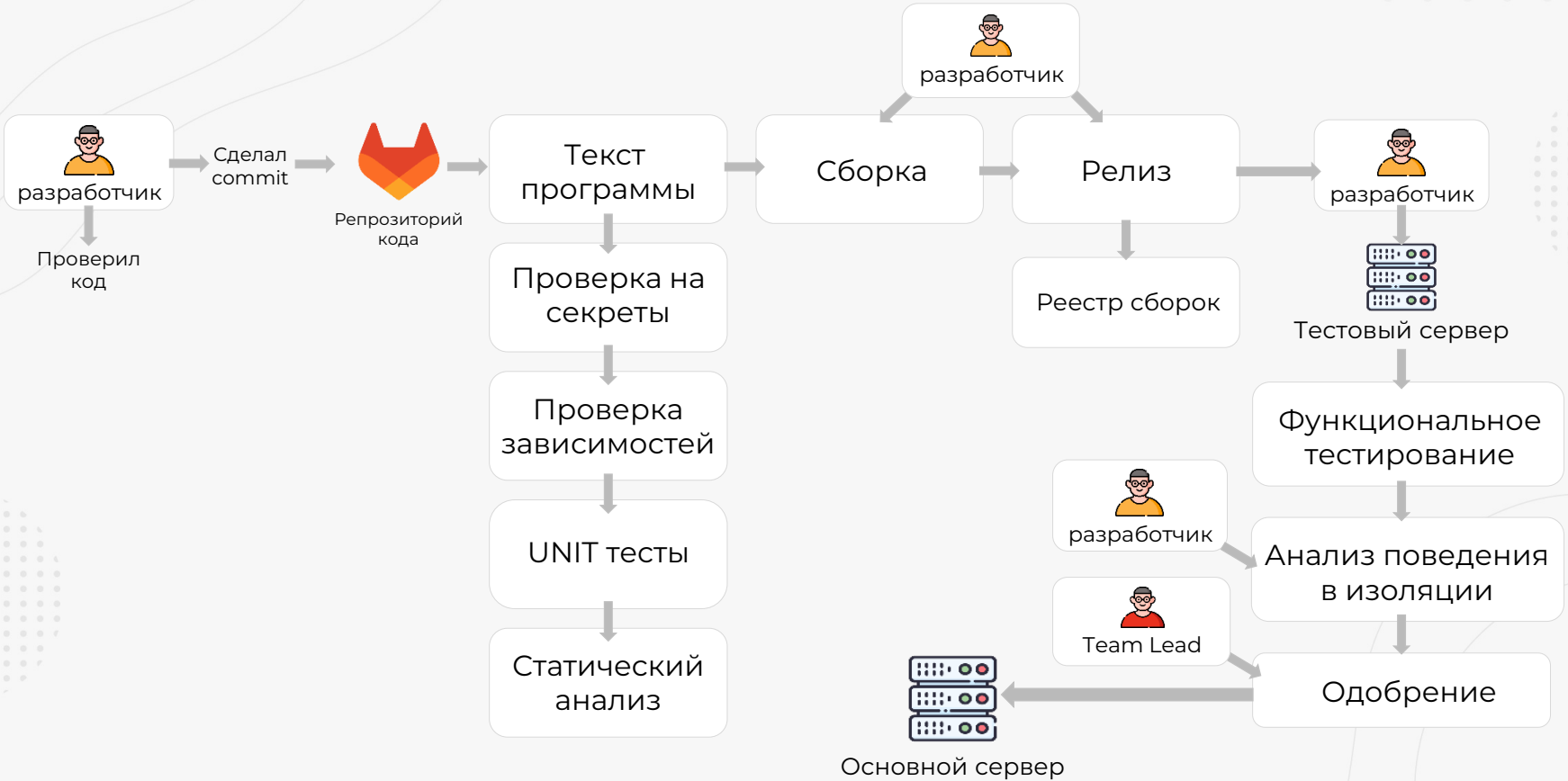
AFL/AFL++

DEPENDENCY-CHECK

Архитектура конвейера

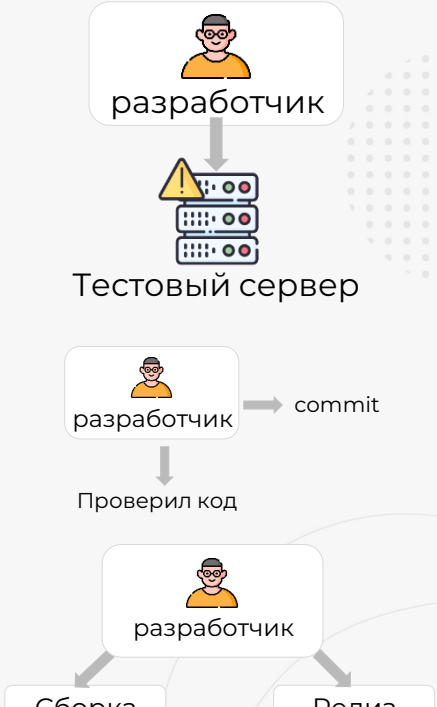


Исходное состояние типового конвейера



Возможные недостатки

- Не происходит автоматическое развёртывание приложения на сервер
- «Монолитный» конвейер
- Недостатки сетевой безопасности
- Использование паролей по умолчанию
- Нерегулярный аудит безопасности
- Нет разделения процессов по ролям

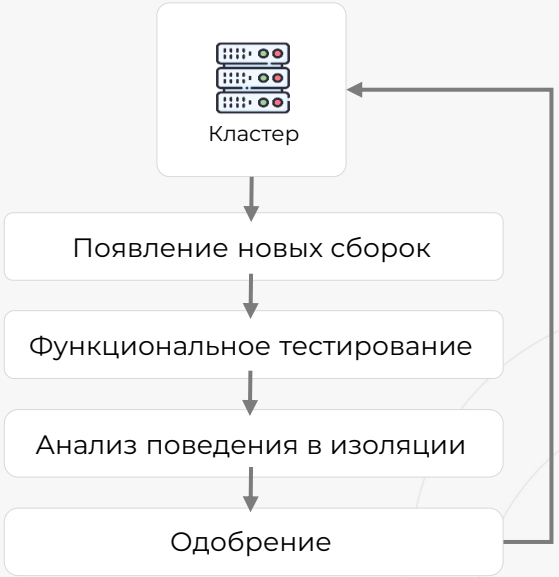


Решение

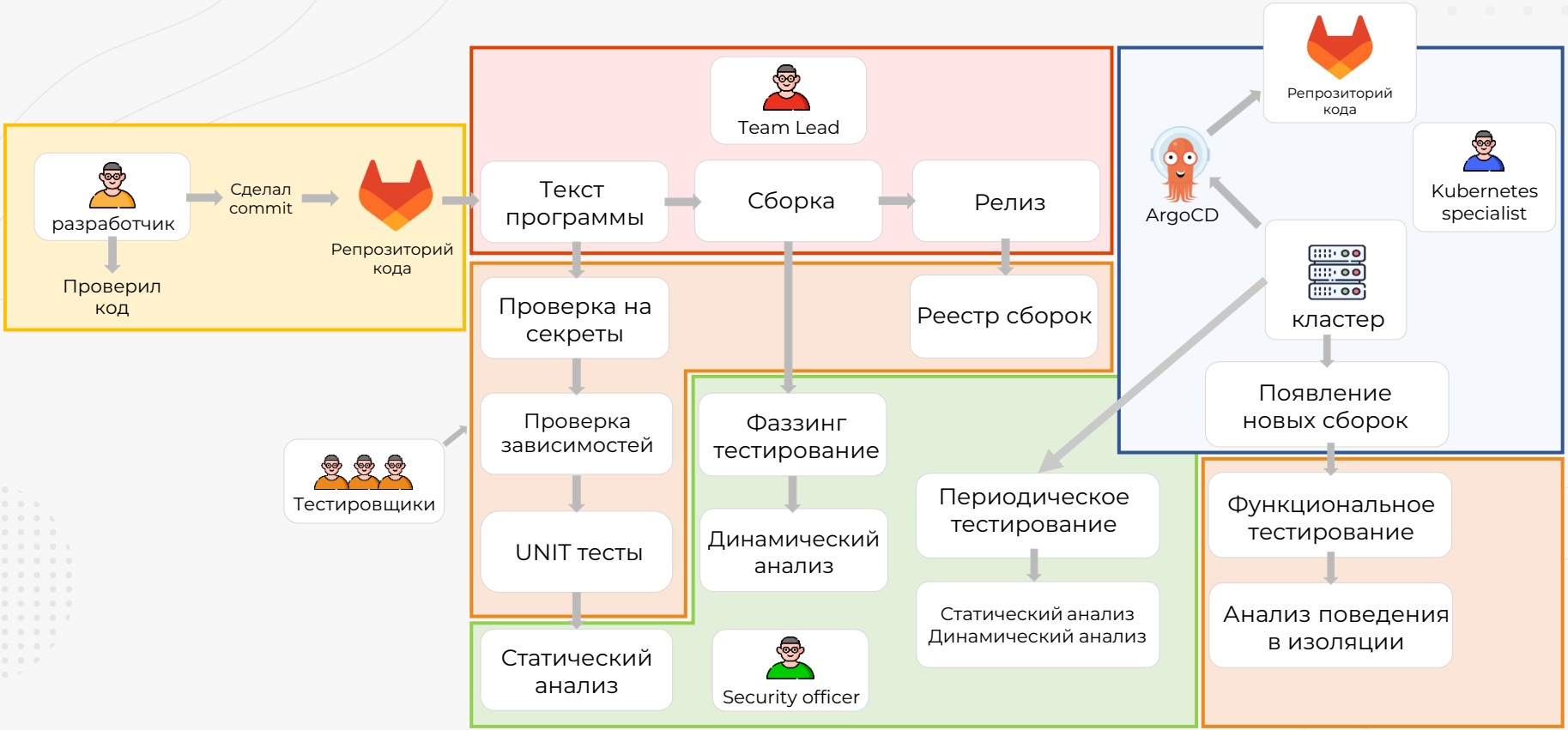
Внедрение ArgoCD в процесс развертывания для мониторинга реестра

Добавление задач для тестирования кода на актуальные уязвимости

Добавление событий (Argo Events) для тестирования новых сборок



Разделение процессов по ролям



Secure Development Pipeline System это

- Комплексная система безопасной разработки на основе популярных решений с открытым исходным кодом
- Упрощённое внедрение автоматического тестирования безопасности приложения (DAST, SAST, IAST)
- Возможность гибкой подстройки под ваши процессы
- Материалы для формирования культуры безопасной разработки в комплекте
- В комплекте документация по разработке безопасного ПО в полном соответствии с ГОСТ Р 56939-202X