GUARD CONF

Современные DevOps-практики: от идеи до релиза



Кирилл Довгаль

Руководитель
продукта GitFlic

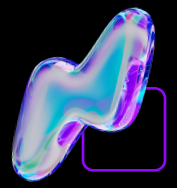


Инструментов больше. Проще не стало



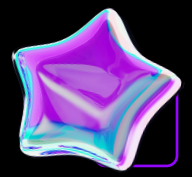
Инструменты

Git, CI/CD, Kubernetes, сканеры, мониторинг:
каждый инструмент работает



Связи

Связывают инструменты между собой люди



Новое приложение

Каждый раз требует одного и того же: проект и конвейер,
окружение, доступы и проверки, метрики и логи

Проблема в процессе

GUARDCORE

Конвейеры

У команд разные конвейеры, общий стандарт существует только в виде инструкции

Заявки

Доступы, секреты и проверки выдаются через очередь заявок

Проверки

Подключены не везде, результаты разбросаны, у исключений нет срока и владельца

Владельцы

Владельца и работающую версию системы ищут вручную

Связи

Связи между системами держатся на знаниях отдельных специалистов

Вывод

Это ограничение процесса, а не инструментов

Решение это ADP

GUARDCORE

Портал

На базе Backstage: каталог, шаблоны, самообслуживание

Dex и ALD Pro

Единый вход

AM/ Grafana

Метрики (дополнительно)

Dependency-Track

Учет состава ПО (дополнительно)

GitFlic

Код, CI/CD, реестр образов

Argo CD

Развертывание по GitOps

«Боцман»

Kubernetes-кластеры и проекты

Astra Linux SE

Серверная Astra Linux Special Edition: операционная система платформы

Разработка без лишних заявок

Шаблоны: Go, Java, Python, C#, TypeScript, React

Роли

Роль на сервис назначается в портале
и сразу применяется в GitFlic и «Боцмане».
Портал регулярно перепроверяет назначения

Единый вход

Пользователи и группы берутся из ALD Pro,
вход идет через Dex

Инфраструктура

Базу, кеш и брокер разработчик заказывает
в форме создания сервиса

Изменения

Новые версии шаблонов и каталога CI
приходят запросом на слияние,
изменения видны до принятия



От коммита до релиза

GUARDCONF

Изменение → Сборка → Проверки → Выпуск → Эксплуатация

Изменение
запрос на слияние в GitFlic, проверяющие, условия слияния

Конвейер
lint → test → build → scan → deploy

Среду выбирает тег git
v*-dev.N → dev, v*-rc.N → staging, vX.Y.Z → prod (задание запускается вручную)

Эксплуатация
на странице сервиса видны поды, метрики, логи и показатели DORA

Откат
отмена коммита развертывания, после чего Argo CD возвращает предыдущую версию

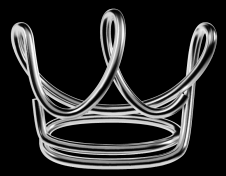
Кому подходит ADP

GUARDCORE



Разработчик

Решает типовую задачу без заявки



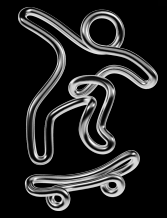
Платформа

Платформенная команда меняет один шаблон вместо правок в каждом проекте



ИБ

Получает проверки в каждом конвейере с сохраненным результатом



Руководитель

Видит системы, их владельцев и историю выпусков

Toyota Chofer на Backstage: более 100 команд, более 1600 облачных приложений, более 40 шаблонов. Проекты выходят за недели, а не за кварталы. Затраты в 2022 году снизились более чем на $10 млн



Источник: Backstage Adopter Spotlight: Toyota, 20.03.2023

DevSecOps: проверки внутри конвейера

GUARDCONF

Исходный код	Зависимости	Контейнеры	Конфигурации	Стенд
Анализ кода и поиск секретов в CI	SBOM для каждой сборки. Dependency-Track отслеживает уязвимости сторонних компонентов	Trivy и Hadolint: уязвимости образов и ошибки Dockerfile	KICS и проверки Helm: манифесты и конфигурации до применения в кластере	DAST: динамический анализ развернутого приложения

При настроенных порогах сборка и выпуск блокируются.
Результаты проверок сохраняются и сводятся в GitFlic ASOC

А хотите еще эффективнее управлять процессом?

GUARDCORE

Основа та же. Меняется исполнитель

Уже работает на ADP

01

Автоматизация операций

Шаблоны, сборка, проверки и развертывание

→

02

Кибернетизация процесса

Правила и данные, обратная связь и аудит

→

03

Подключение ИИ-исполнителей

Задача, полномочия, проверяемый результат

+ИИ

Агент готовит изменение.
Проверки, полномочия и правила выпуска остаются прежними.

ИИ под контролем

GUARDCONF

Агент готовит изменение

Проверки, полномочия
и правила выпуска
остаются прежними



Изменение агента проходит тот же путь, что и изменение человека:
запрос на слияние → ревью → конвейер → блокирующие проверки →
выпуск в prod вручную → откат

**На действия ИИ распространяются те же правила проверки
и журналирование, что и на действия обычного пользователя**

Будущее разработки в процессах

GUARDCONF

Платформа

Ускоряет разработку
за счет стандартизации
и самообслуживания.
Эффект подтверждает
замер до и после

ИИ

Полезен внутри
управляемого процесса,
но решения остаются за людьми

Безопасность

Становится
частью конвейера



GUARDCONF

Спасибо за внимание!



Кирилл Довгаль

Руководитель
продукта GitFlic



GUARDCORE



Начнем с демо?



