SINGLETON

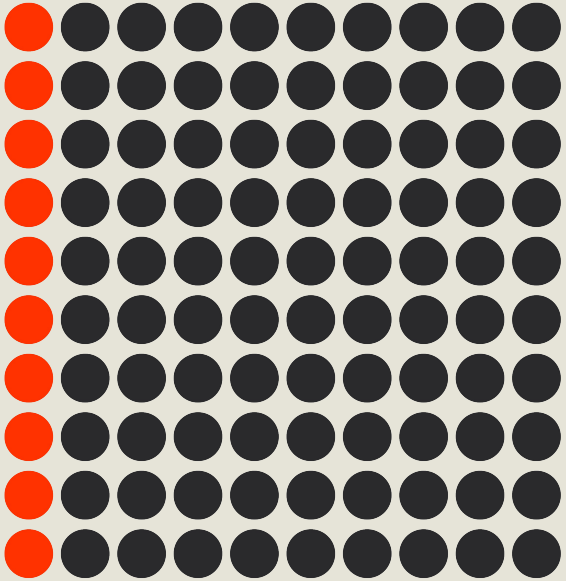
+7(495)792-13-37

p.sorokin@singleton-security.ru

t.me/sorokinpf

Атаки на CI/CD

Неочевидные последствия развитых автоматизаций



whoami

Павел Сорокин

CTO Singleton Security

Pentester и AppSec

@sorokinpf

@NARYL_SEC

О чем доклад

01 Примеры проблем безопасности CI/CD и возможных последствий

02 Почему сделать CI/CD безопасным - не простая задача

03 Что можно сделать для усиления безопасности CI/CD

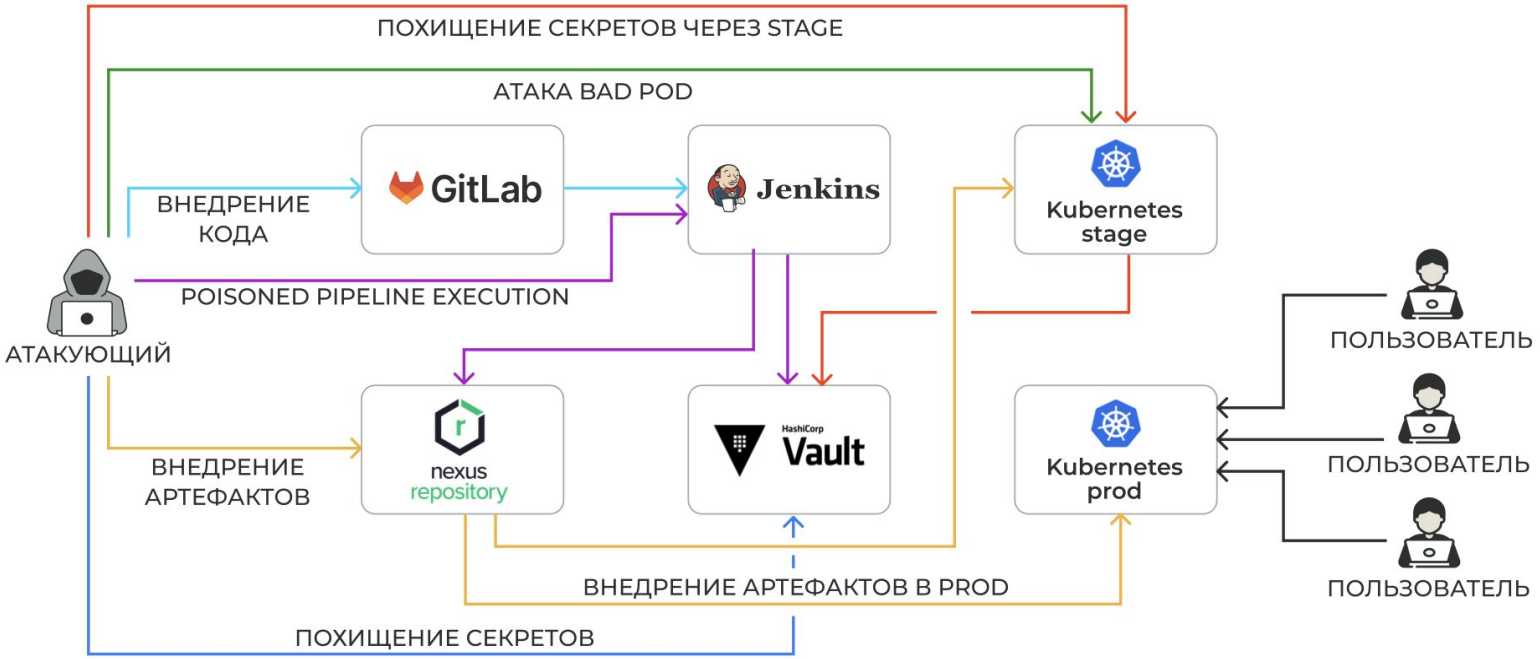
CI/CD - состав

- SCM (github/gitlab/bitbucket)
- CI (gitlab/teamcity/jenkins)
- Secret Manager (vault)
- Runtime (k8s/docker/proxmox/vmware)
- Artifact Repository (artifactory/nexus/harbor)
- etc

Проблемы CI/CD

Черт - в деталях

Проблемы CI/CD - сложность



CI/CD Примеры атак

01. Запуск кода в тестовом кластере или CI job позволял читать "продовые" секреты

02. Небезопасная настройка Gitlab раннера позволяла получить секреты из всех джоб, запускаемых на нём и подменить артефакты в Nexus

03. Побочный эффект от прав доступа на изменения в одном репозитории в гитлабе позволял выполнить задачу на скрытом раннере с привилегированными k8s секретами

Проблемы CI/CD - сложность

01 Большое количество взаимосвязей и интеграций

02 ИБ тяжело контролировать эти интеграции и оценивать их влияние на инфраструктуру

03 Для работы с безопасностью CI/CD требуются специфические навыки

Проблемы CI/CD - вне скоупа пентеста/аудита

01 Как правило перед пентестерами ставят другие цели

02 Иногда в скоуп попадают отдельные компоненты: kubernetes или gitlab

03 Видение текущего состояния системы CI/CD зачастую не полное

Проблемы CI/CD - критичность последствий

01 Выключение "прода"

02 Похищение всех данных

03 Заражение артефактов, передаваемых клиентам

Усиление безопасности CI/CD

Сила - в знании

Усиление безопасности CI/CD

01 Пентест

02 Аудит

03 Планирование

04 Реализация

Пентест CI/CD

01 Доступ в CI/CD уровня инженера

02 Доступ к документации уровня инженера

03 Изучение системы CI/CD

04 Планирование и выполнение атак

05 Разработка рекомендаций

Аудит безопасности CI/CD

01 Доступ к подробной документации

02 Интервью с командами, поддерживающими компоненты CI/CD

03 Детальное изучение работы системы CI/CD

04 Разработка векторов атак, а также выявление слабых мест

05 Разработка рекомендаций, в том числе высокоуровневых

Вопросы?

SINGLETON

p.sorokin@singleton-security.ru

@sorokinpf