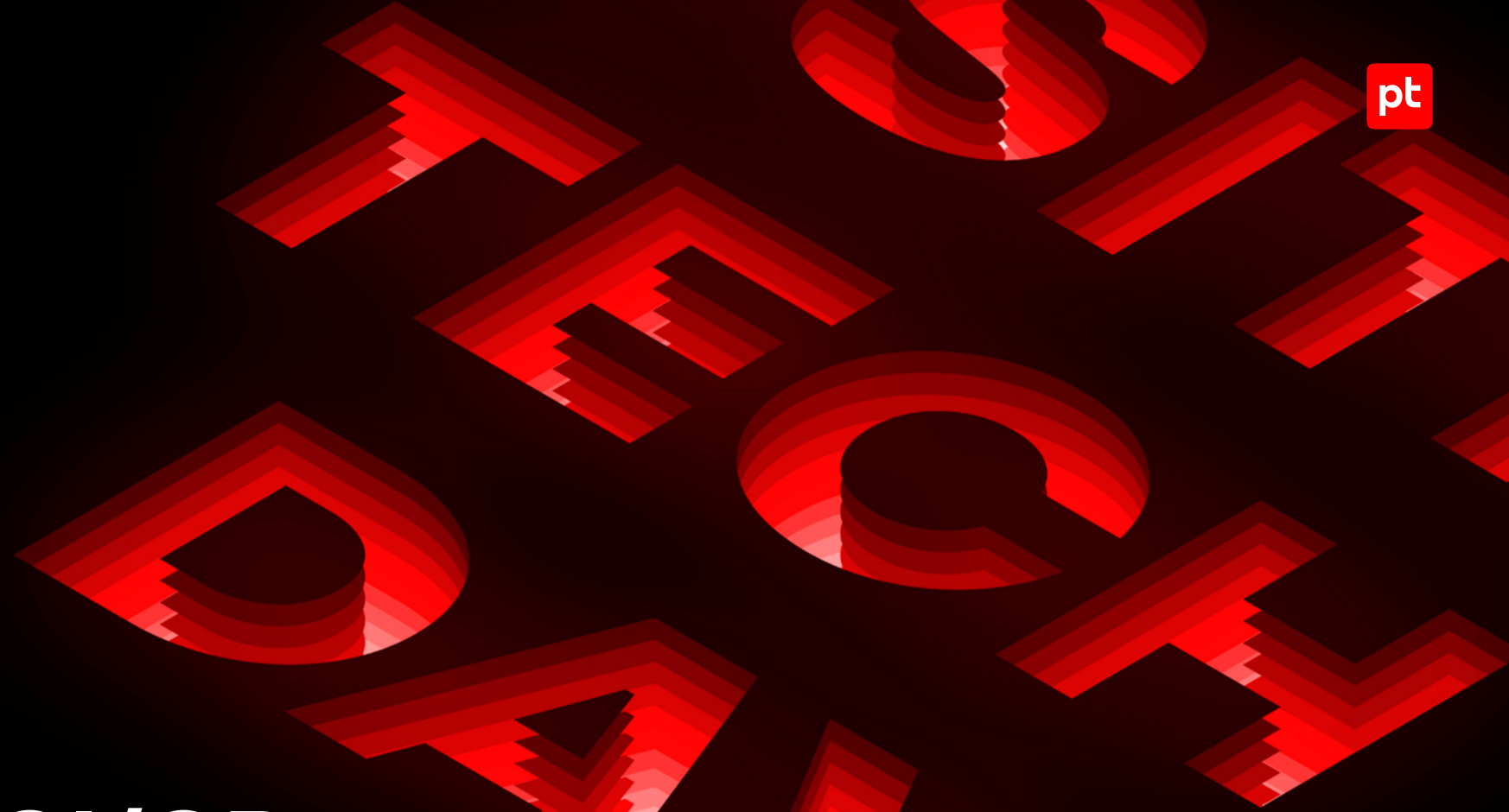
Максим Залысин
Head of DevOps



Конвейер CI/CD на стыке функциональности и безопасности

Спикер

Максим Залысин, Positive Technologies

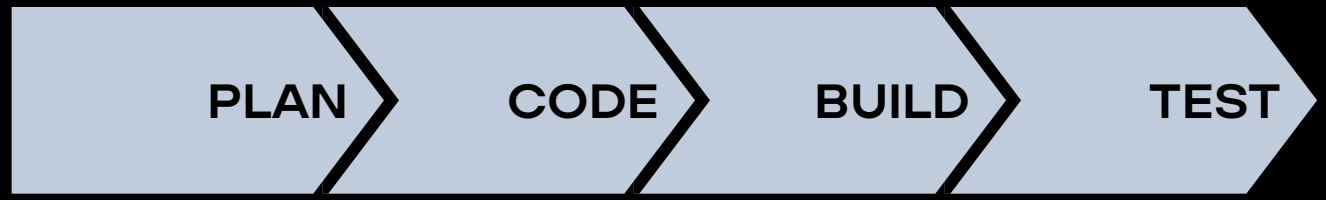
Head of DevOps
или
Руководитель департамента технологий и процессов разработки

- немножко менеджер
- немножко админ
- немножко разработчик
- немножко безопасник

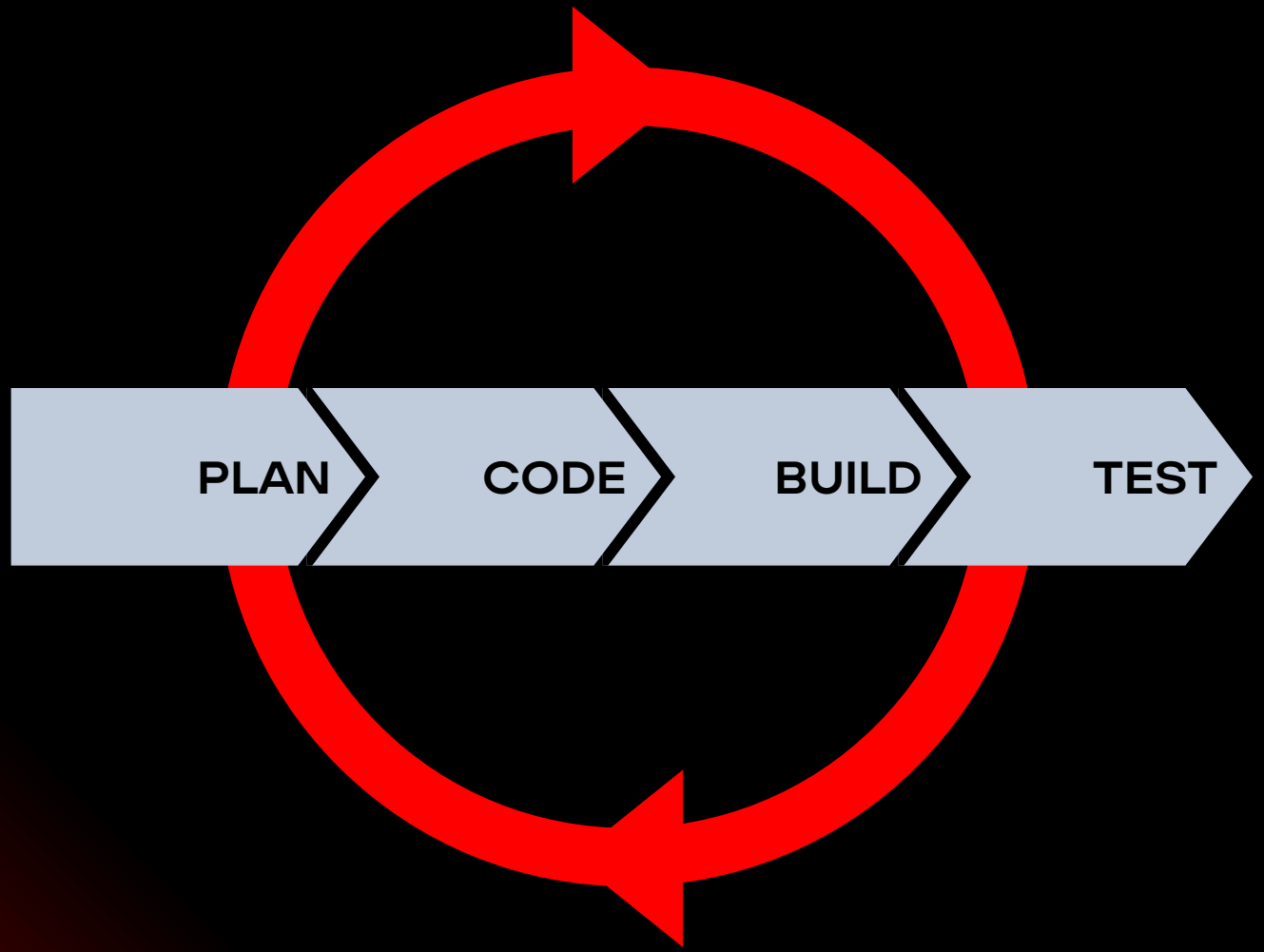
01

Конвейер CI/CD

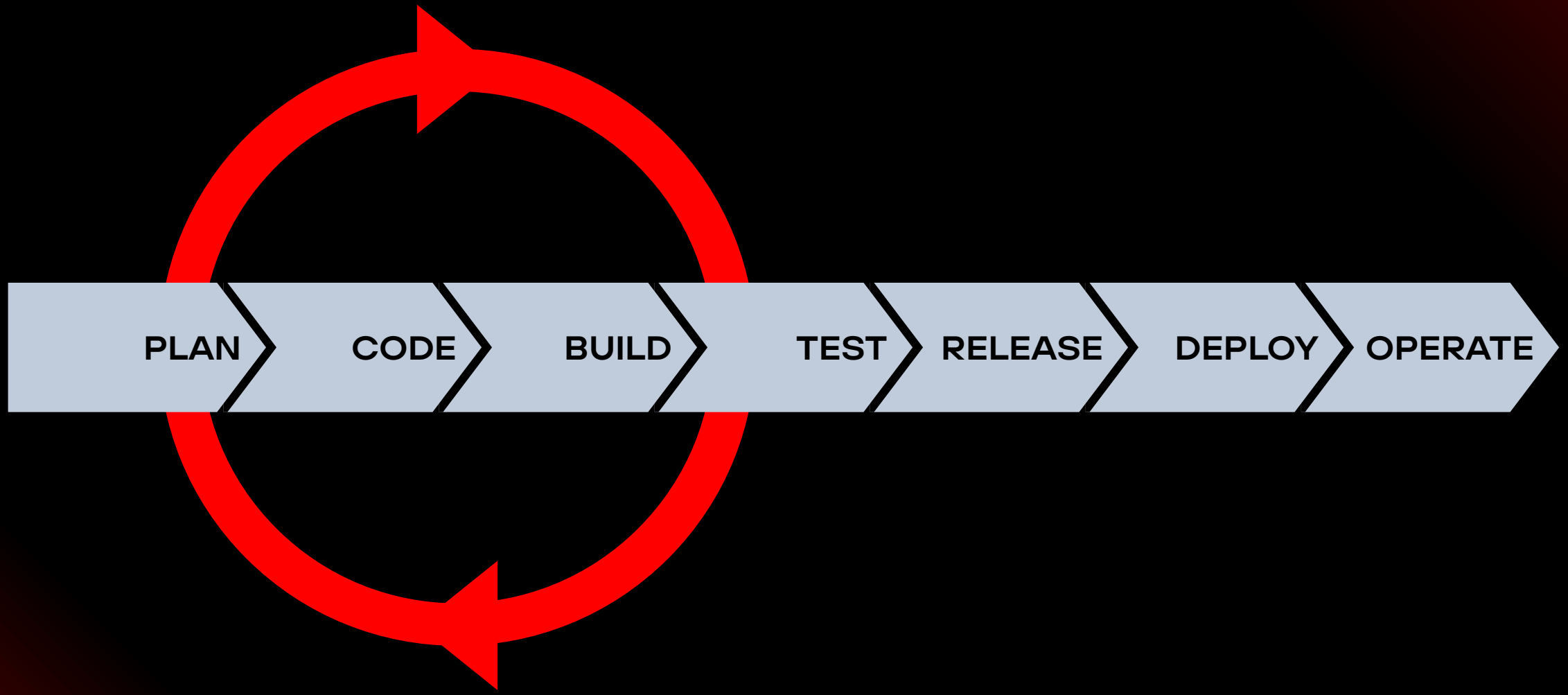
Конвейер CI/CD



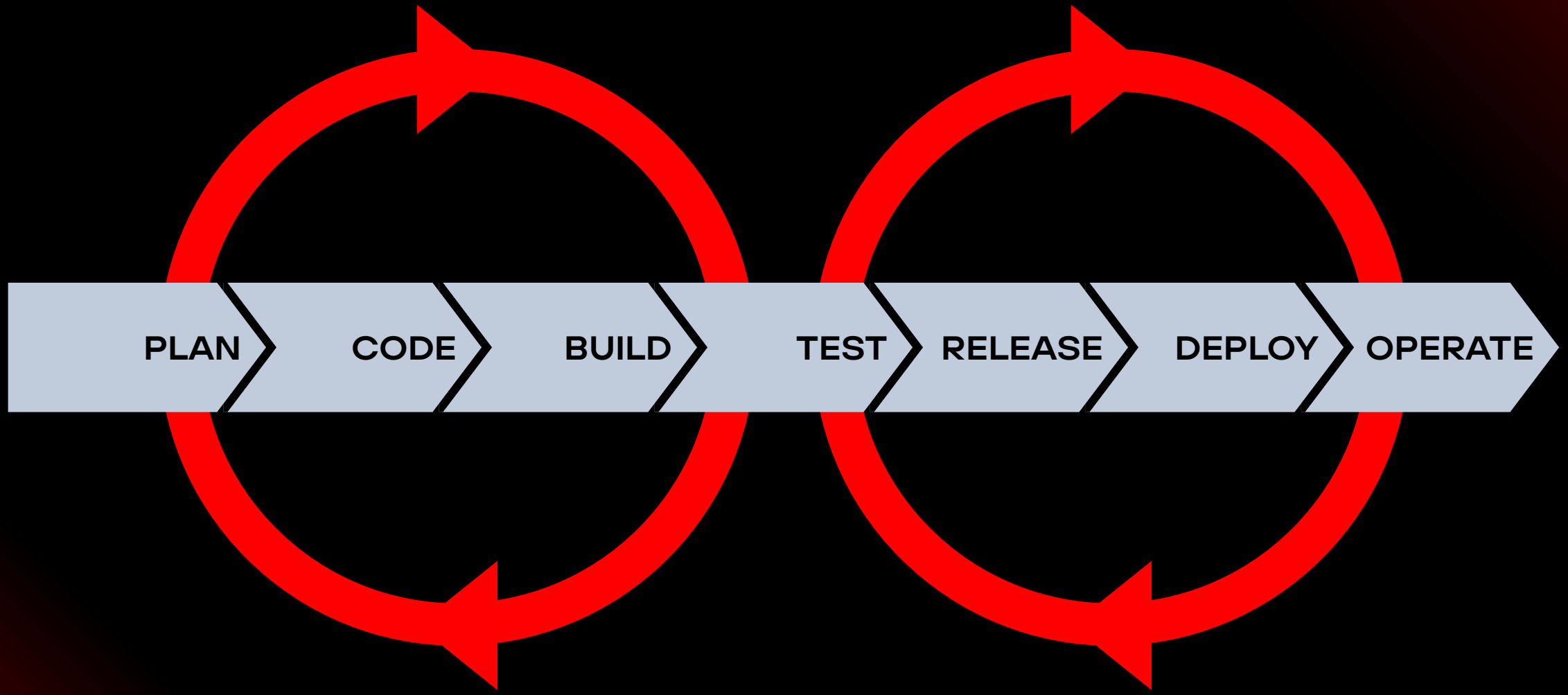
Конвейер CI/CD



Конвейер CI/CD



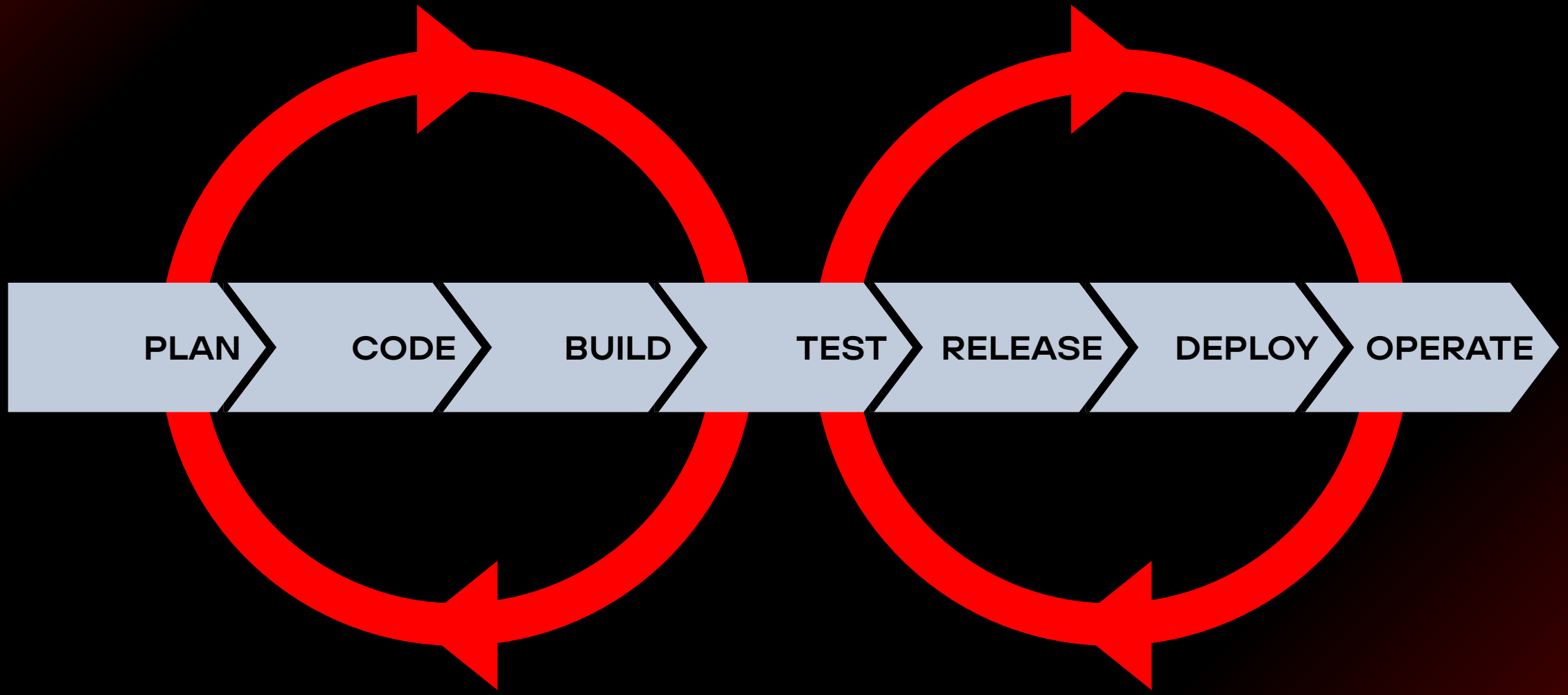
Конвейер CI/CD



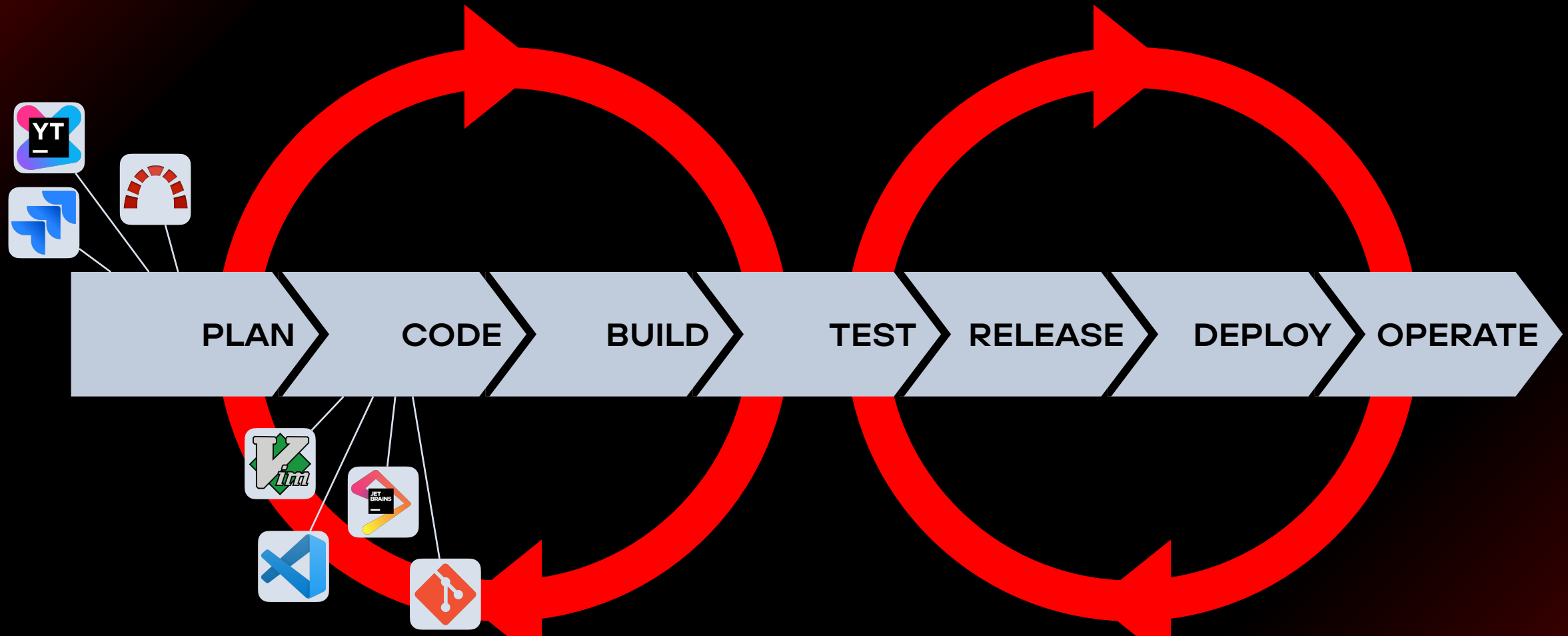
02

Инфраструктура конвейера CI/CD

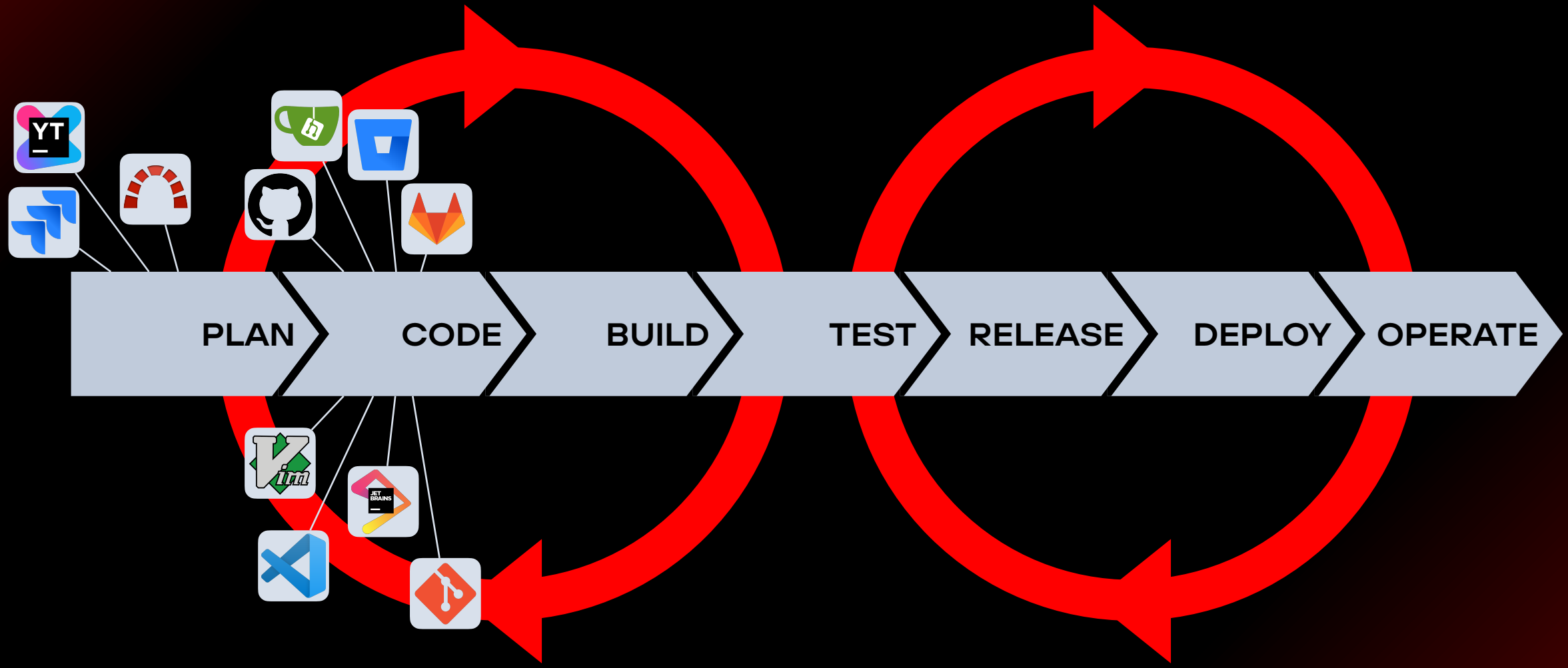
Инфраструктура конвейера CI/CD



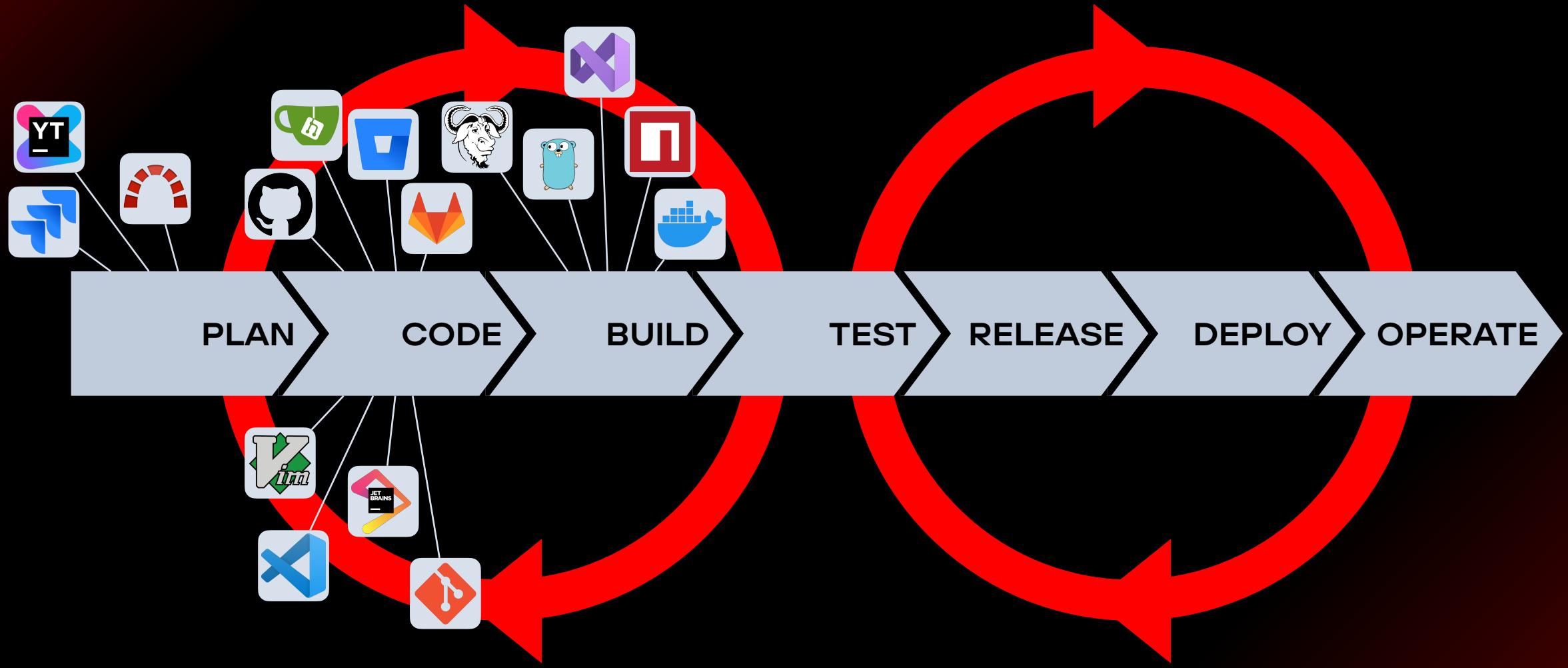
Инфраструктура конвейера CI/CD



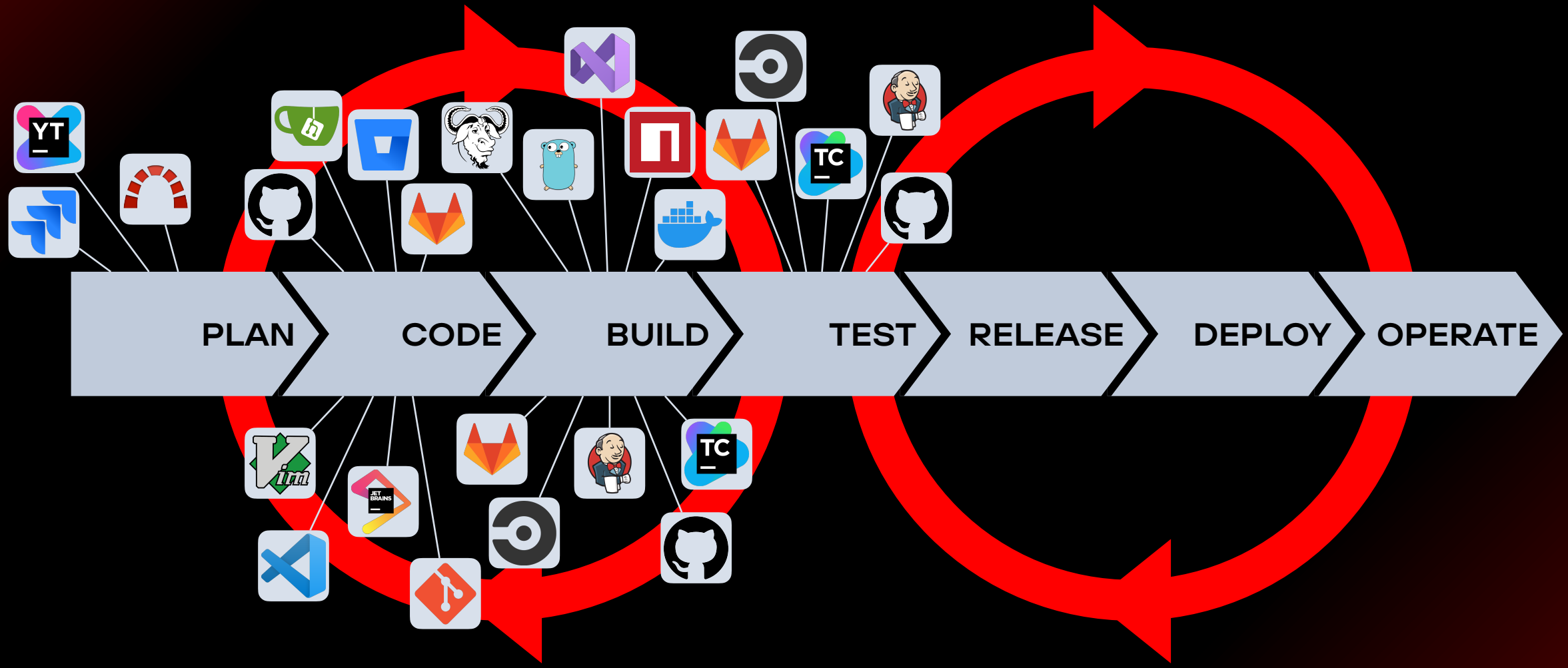
Инфраструктура конвейера CI/CD



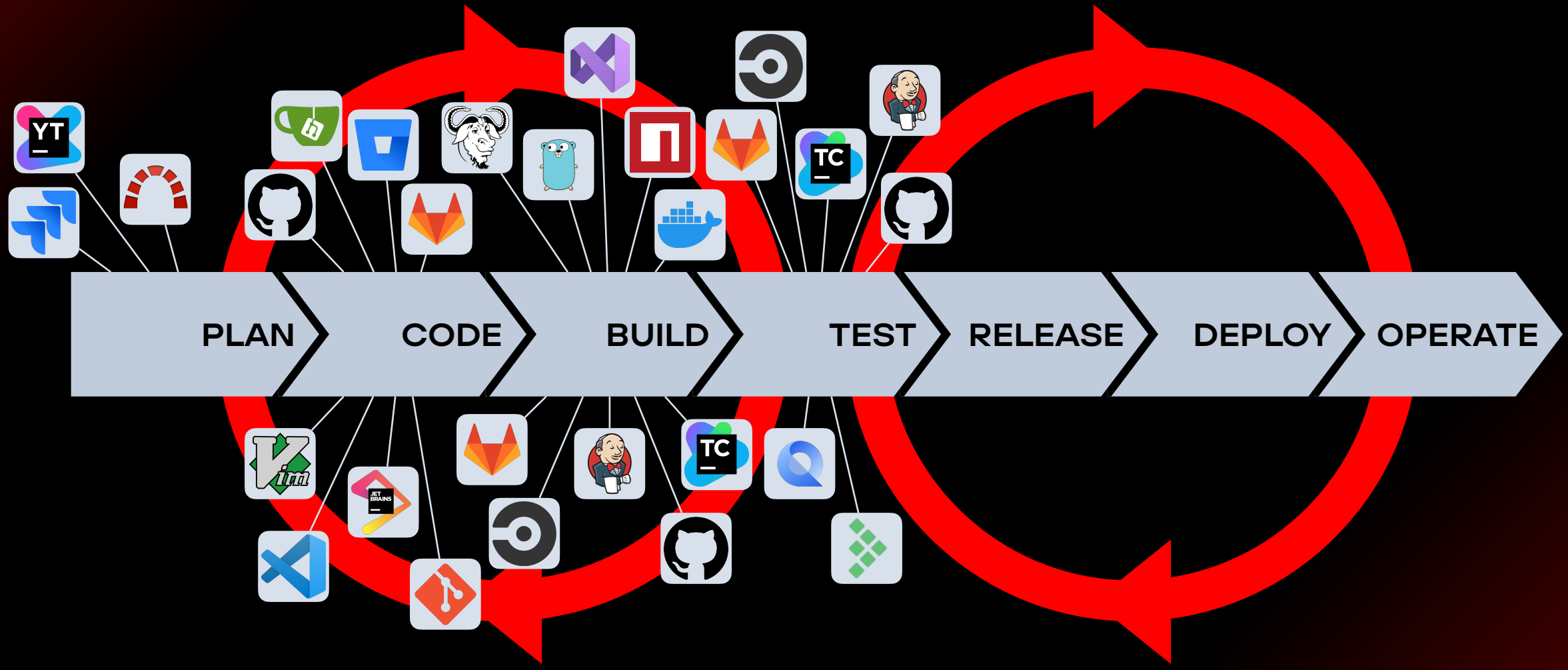
Инфраструктура конвейера CI/CD



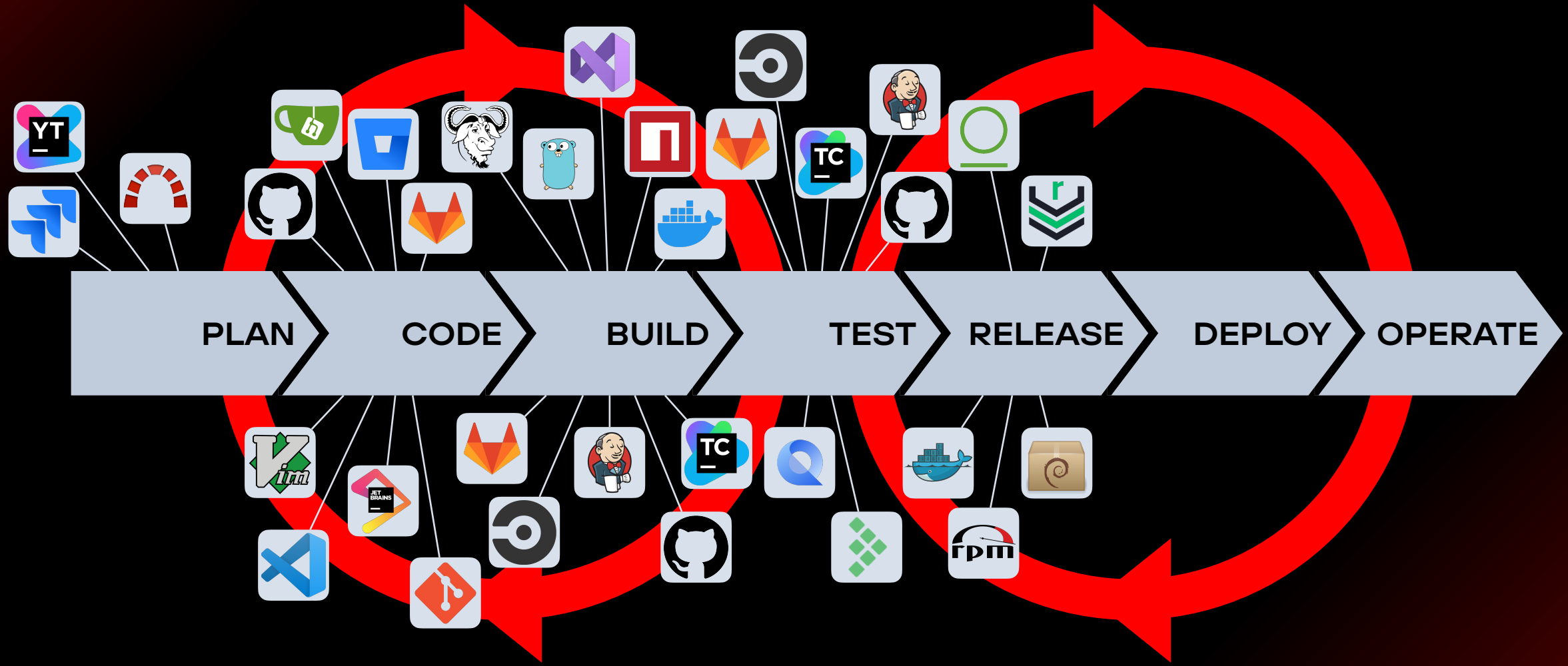
Инфраструктура конвейера CI/CD



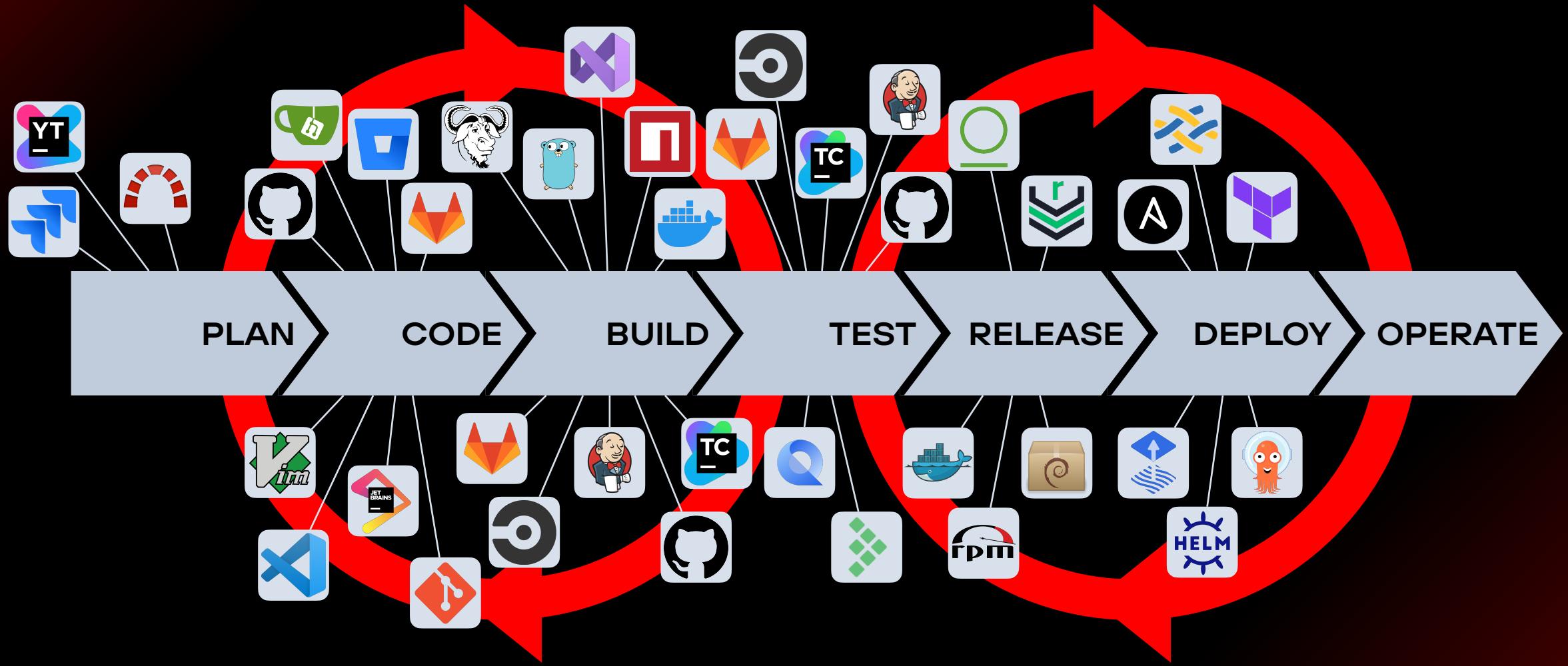
Инфраструктура конвейера CI/CD



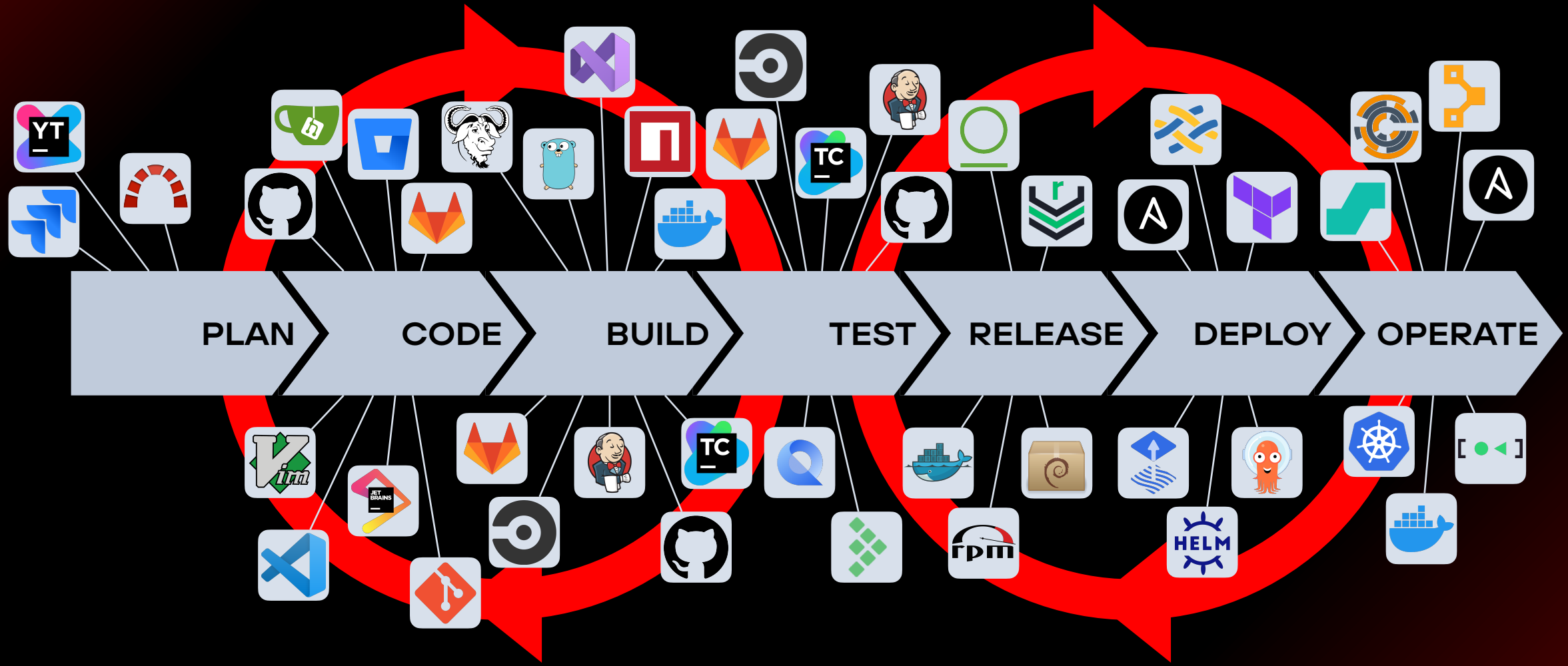
Инфраструктура конвейера CI/CD



Инфраструктура конвейера CI/CD



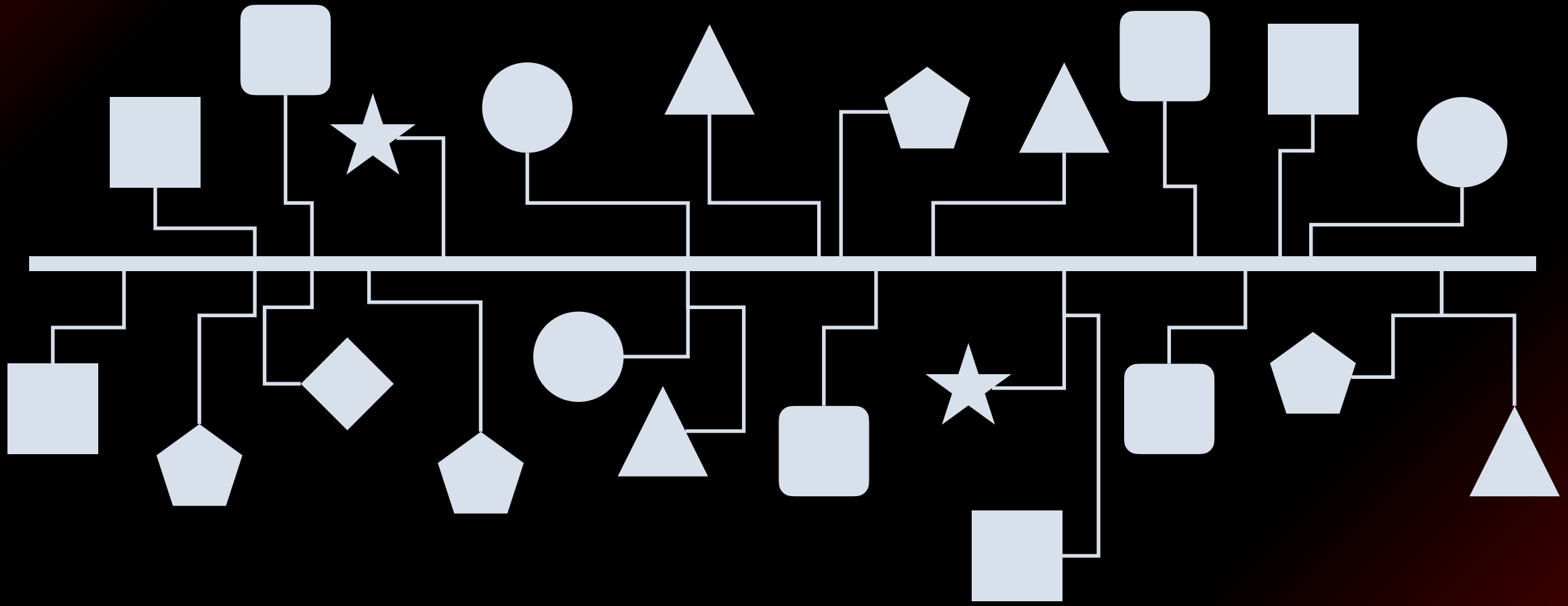
Инфраструктура конвейера CI/CD



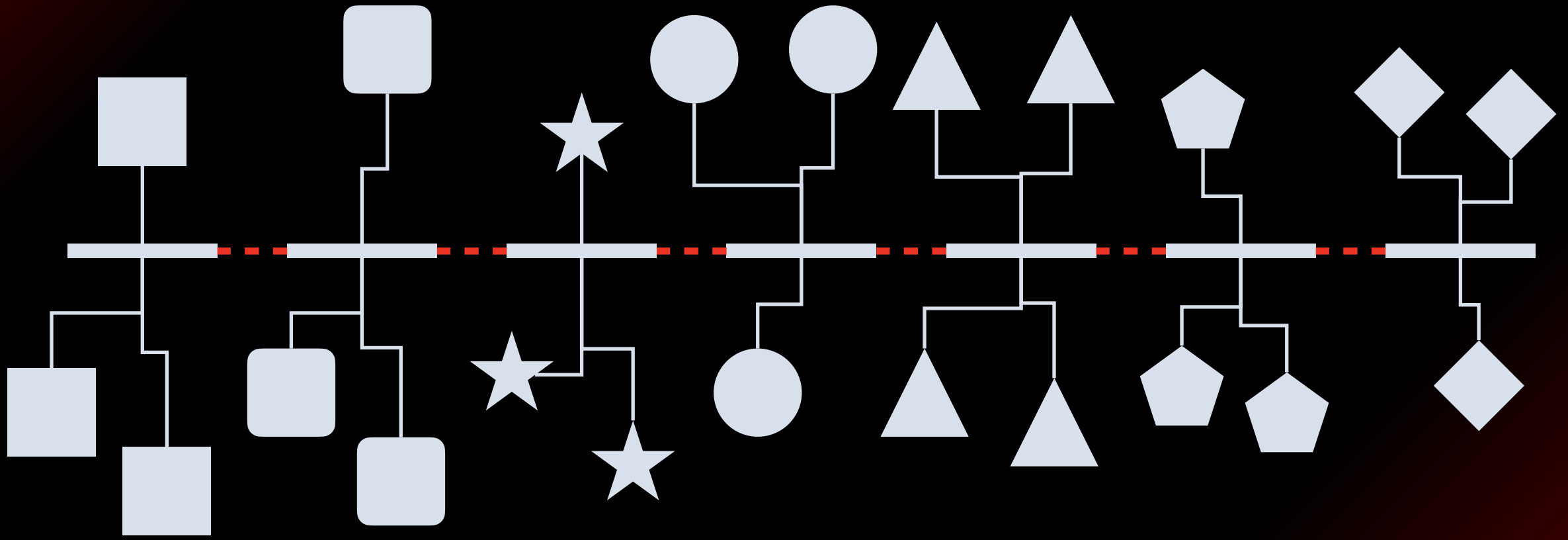
03

Функциональный и безопасный CI/CD

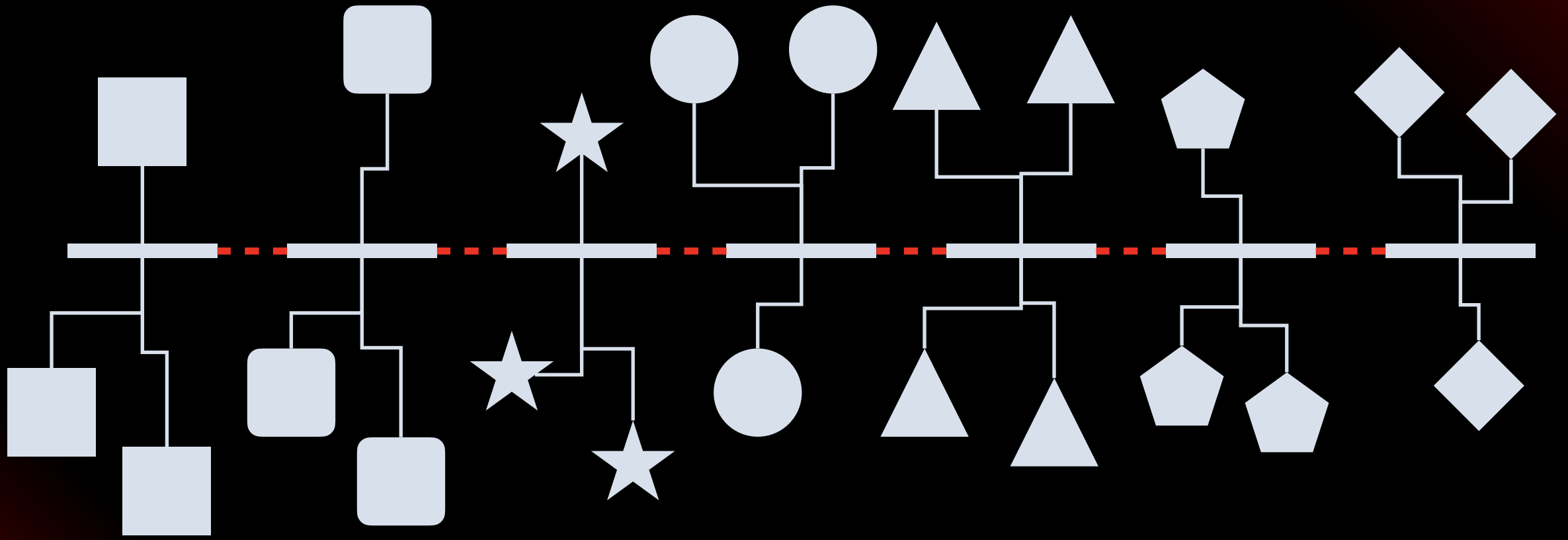
Сетевая сегментация



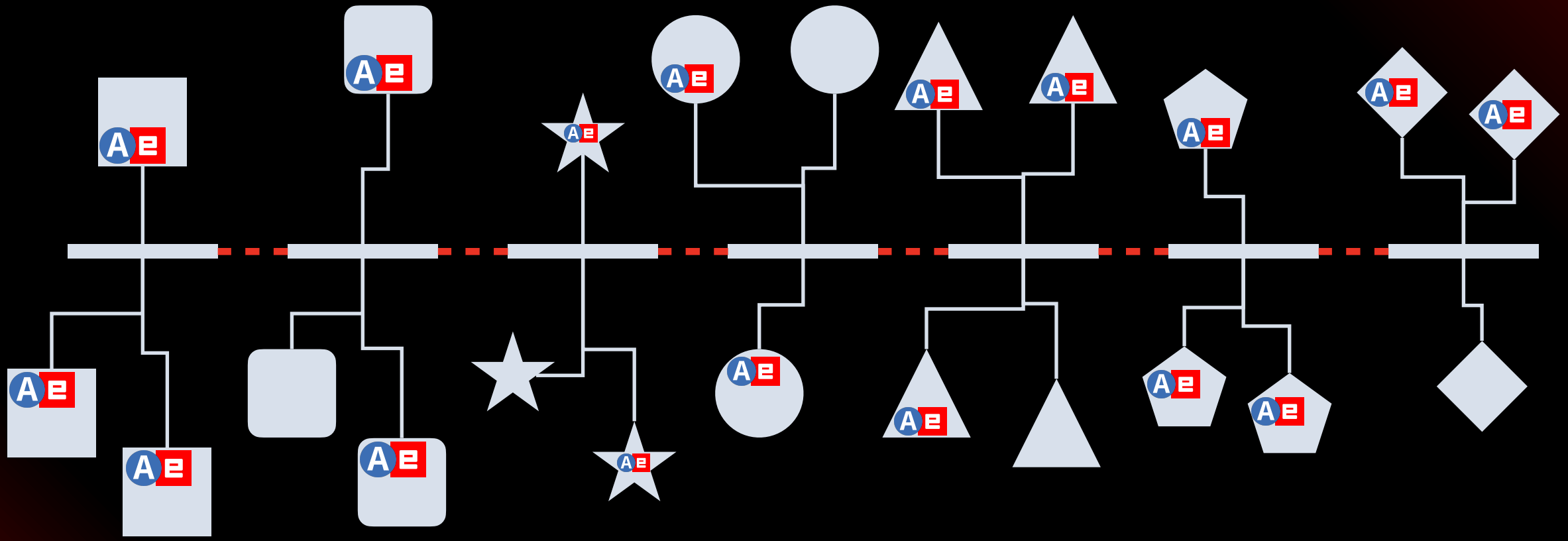
Сетевая сегментация



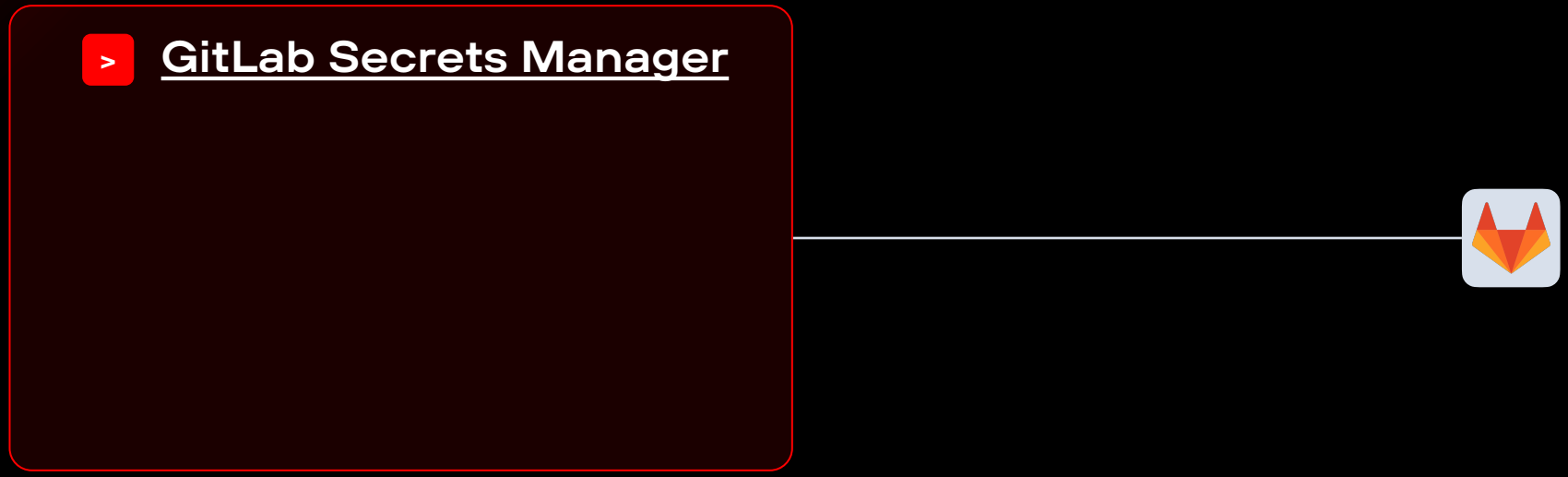
Мониторинг событий безопасности



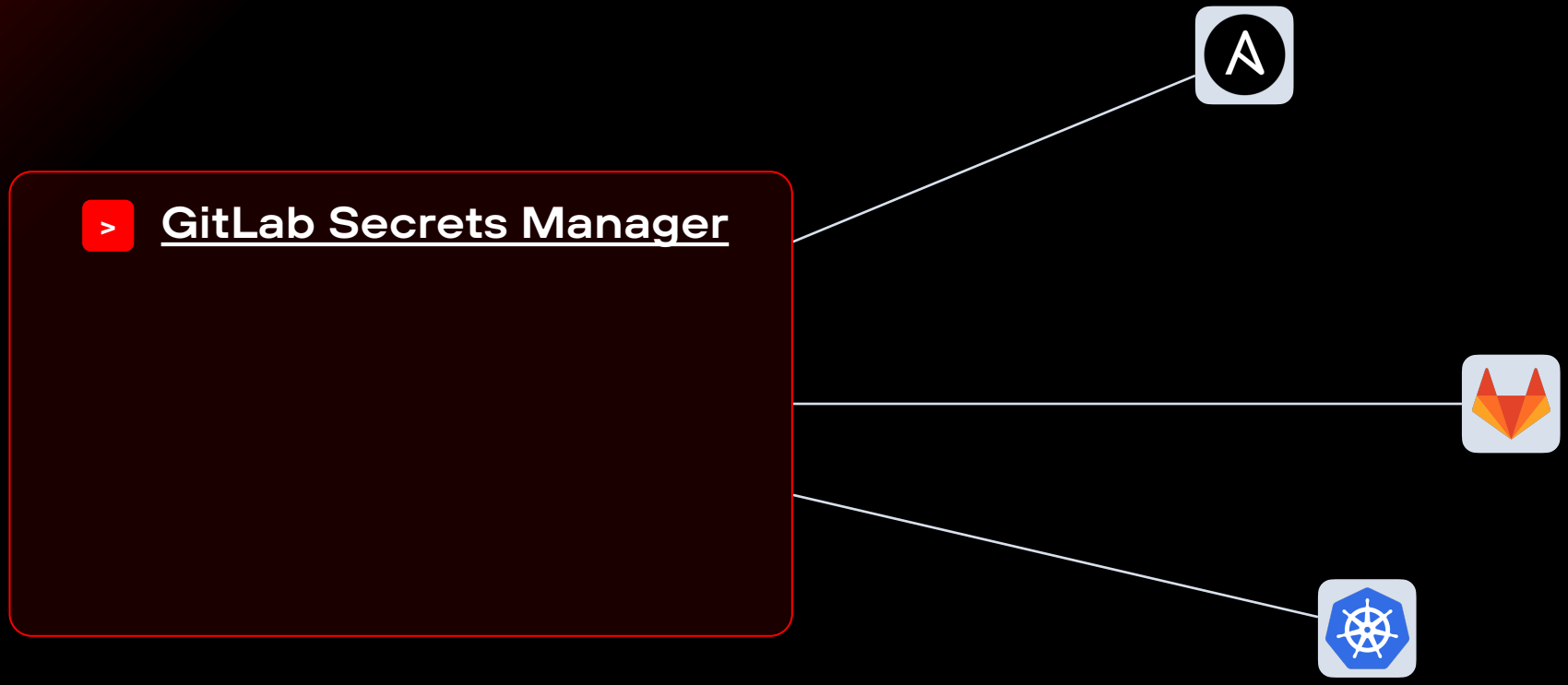
Мониторинг событий безопасности



Управление секретами

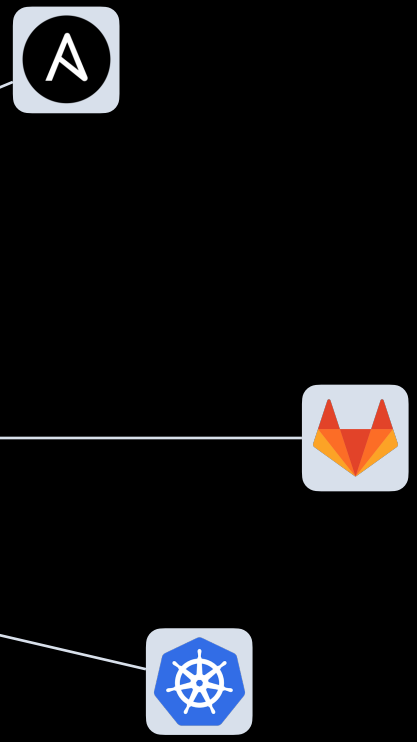


Управление секретами



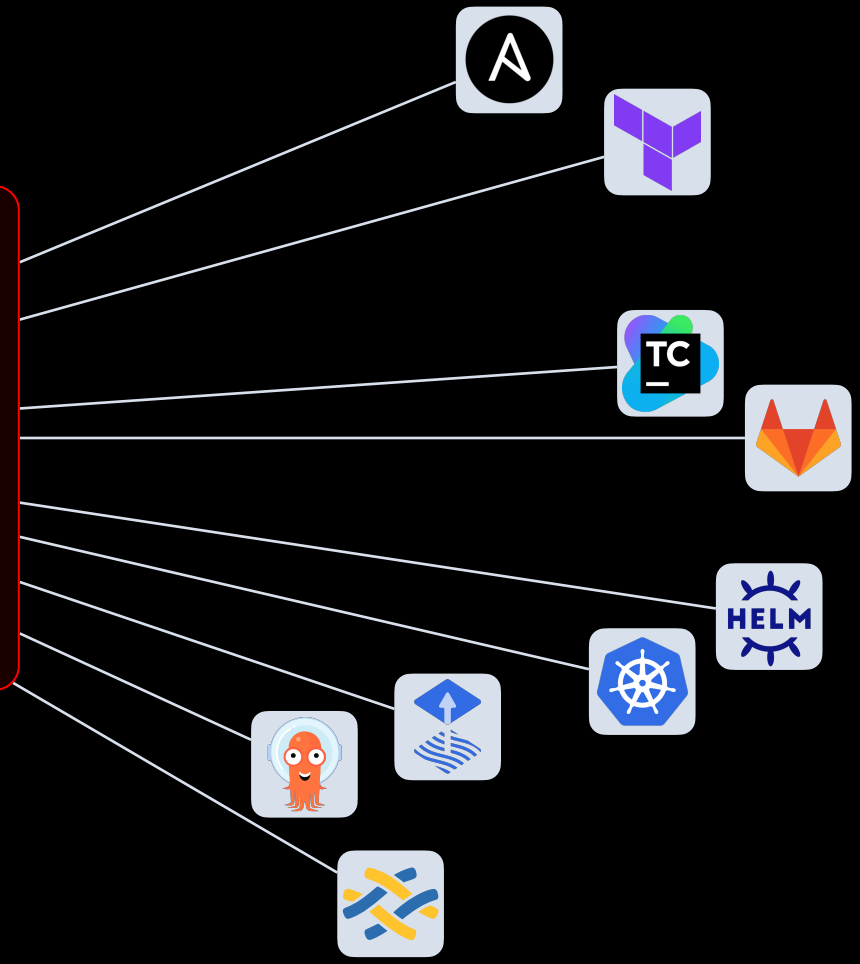
Управление секретами

- GitLab Secrets Manager
- Ansible Vault



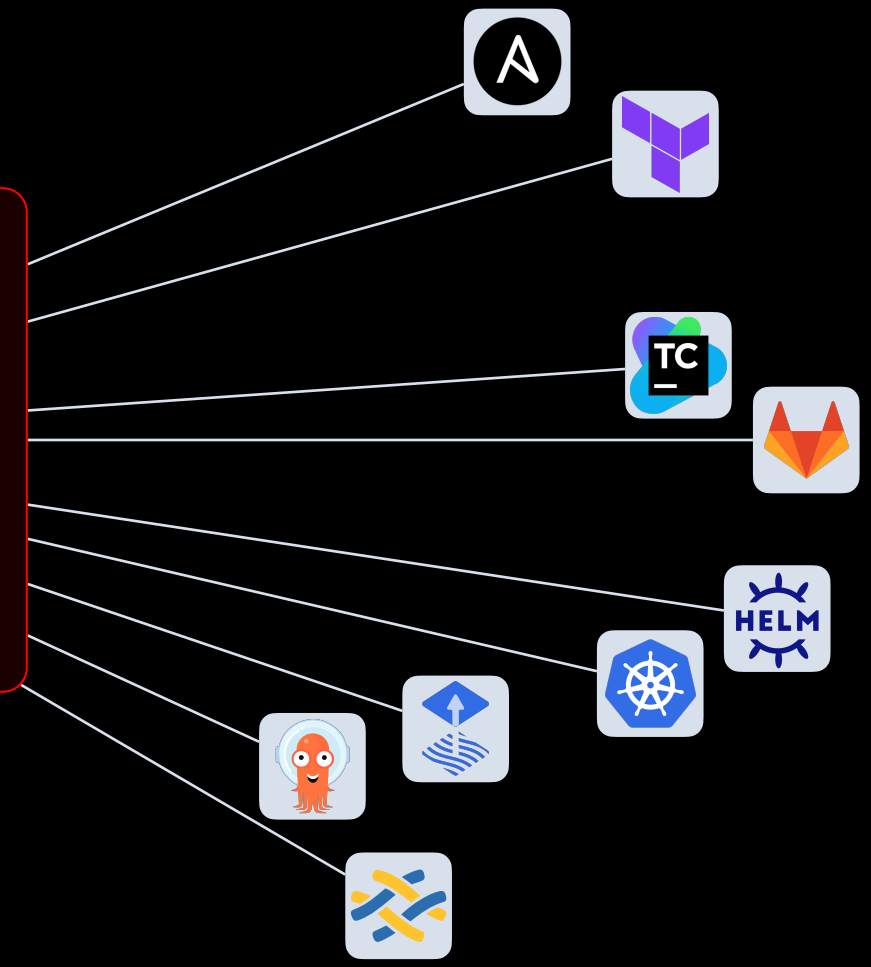
Управление секретами

- GitLab Secrets Manager
- Ansible Vault



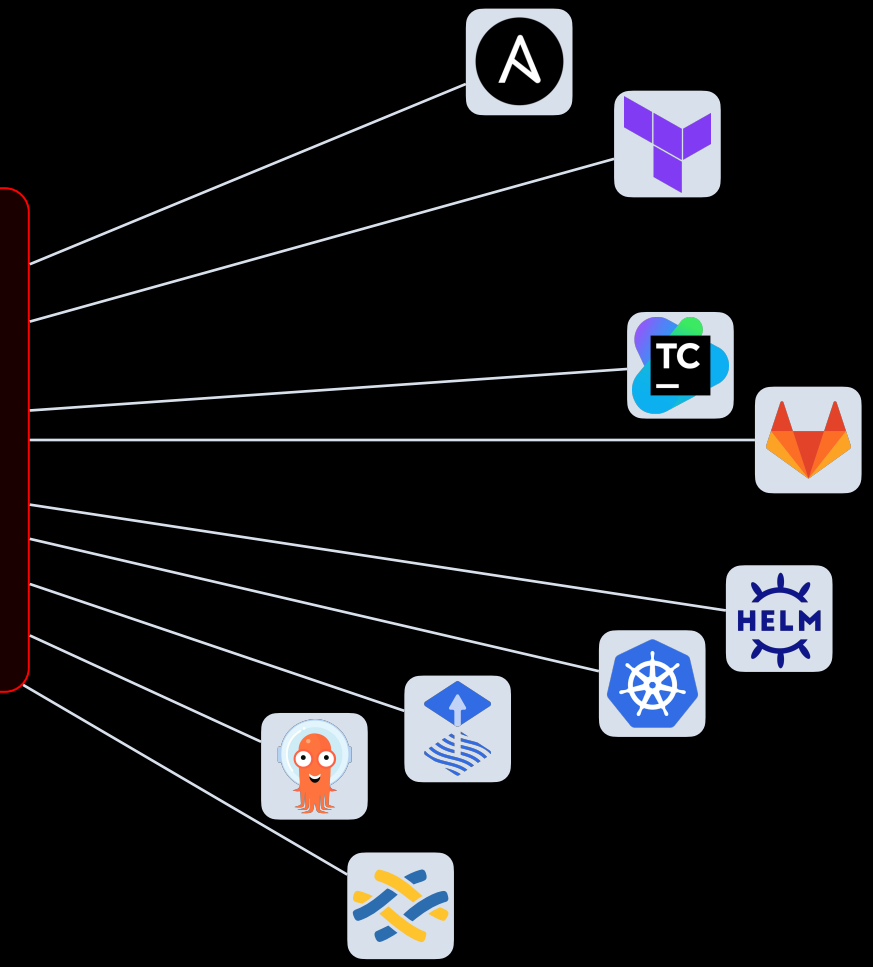
Управление секретами

- GitLab Secrets Manager
- Ansible Vault
- HashiCorp Vault

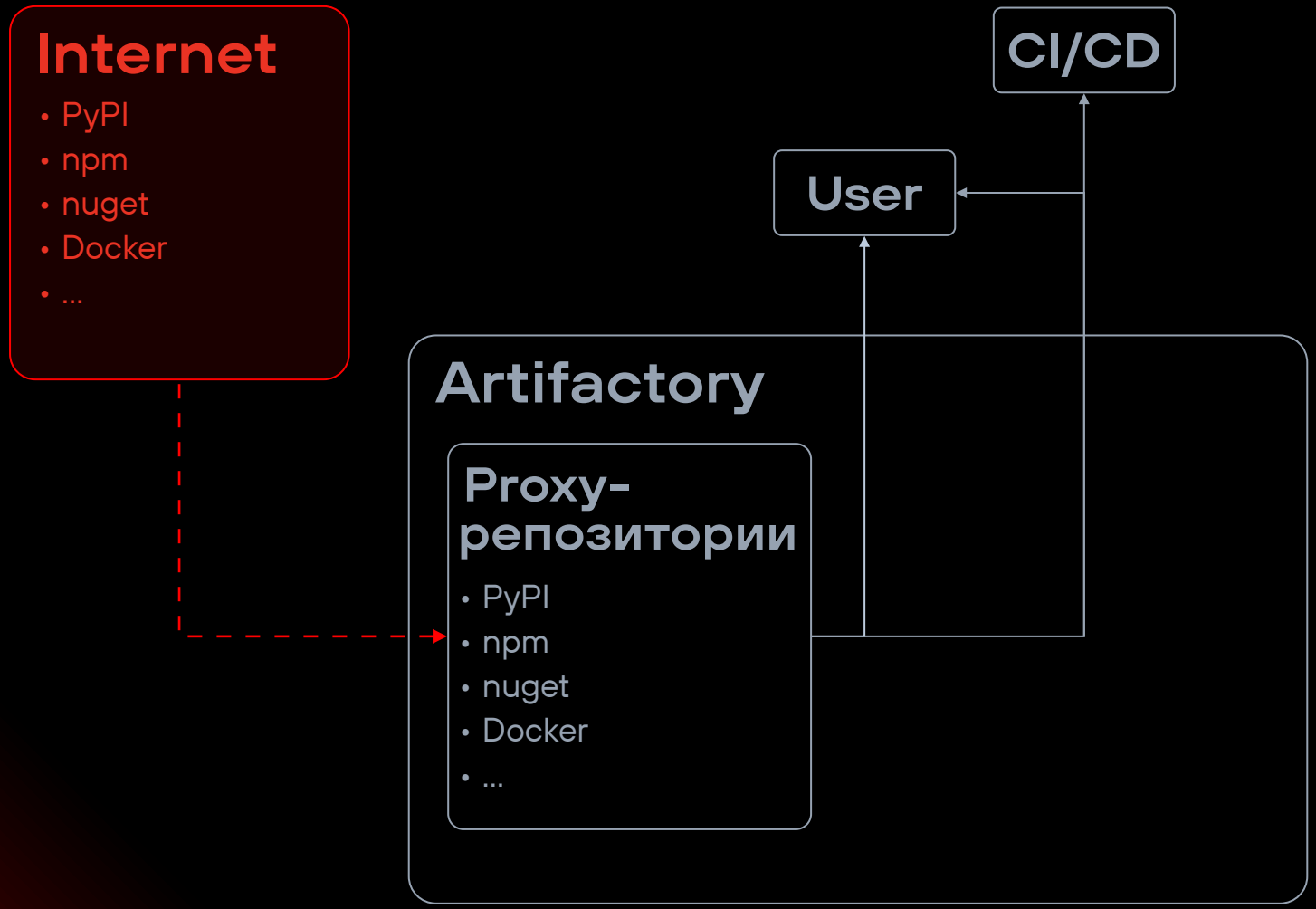


Управление секретами

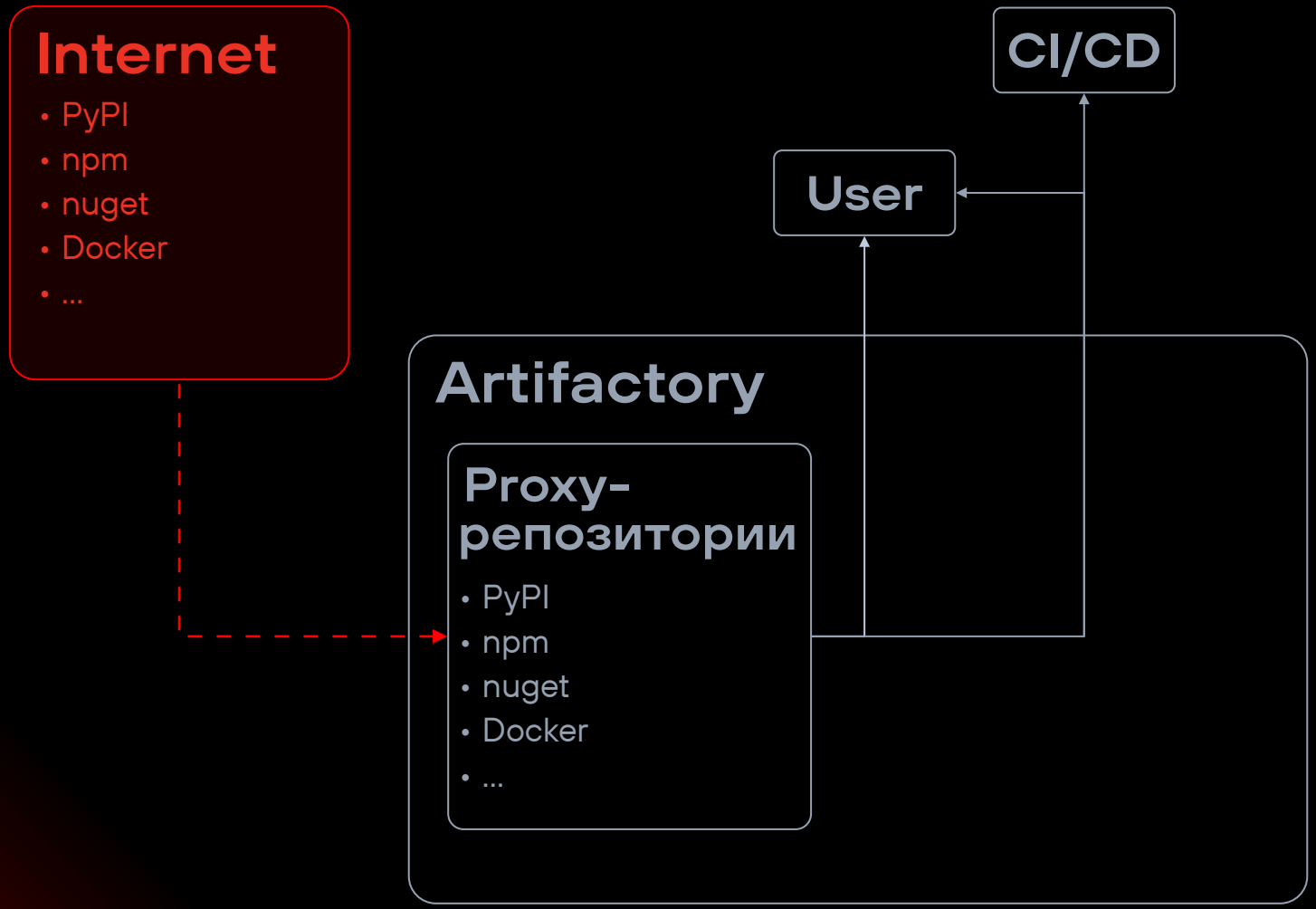
- GitLab Secrets Manager
- Ansible Vault
- HashiCorp Vault
- NetBox Secrets
- *{ password manager }*



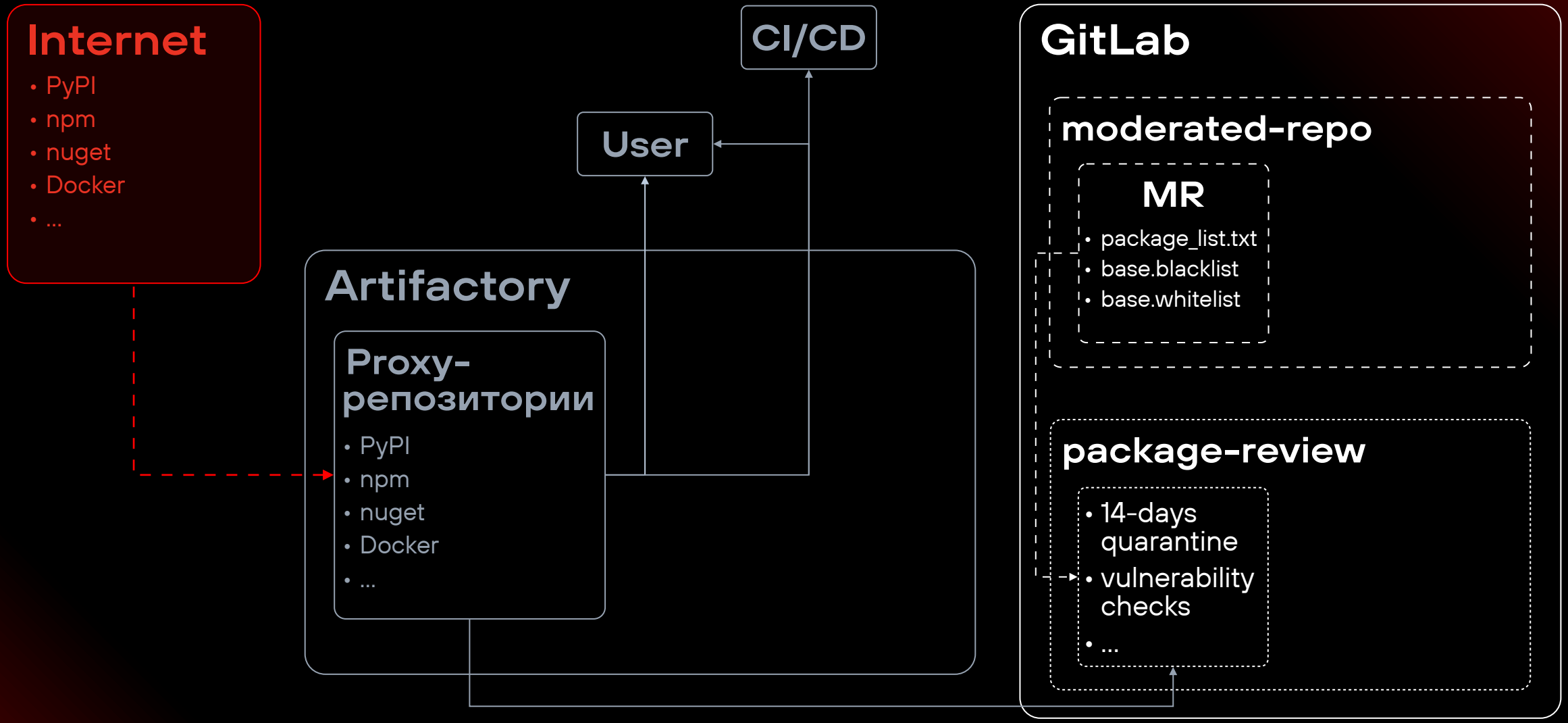
Контроль зависимостей



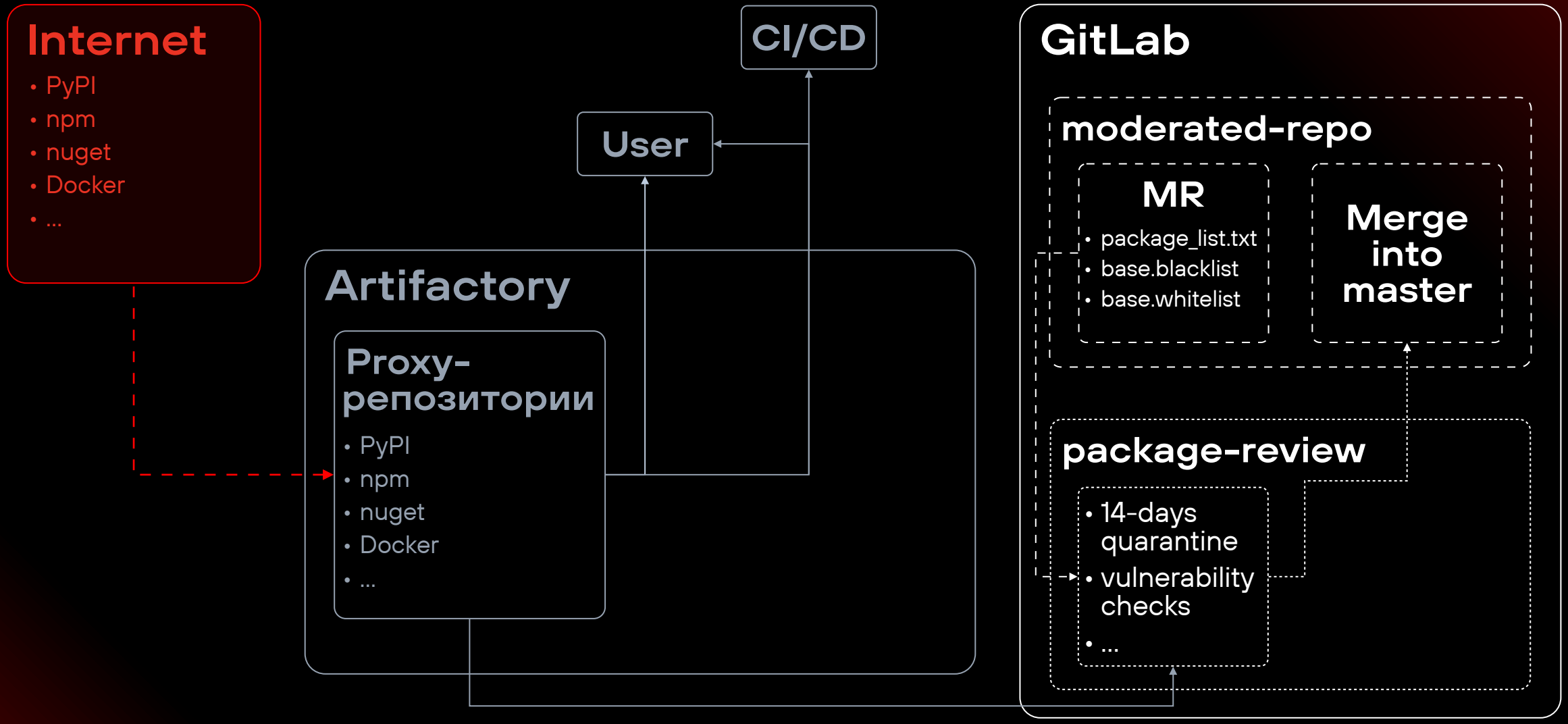
Контроль зависимостей



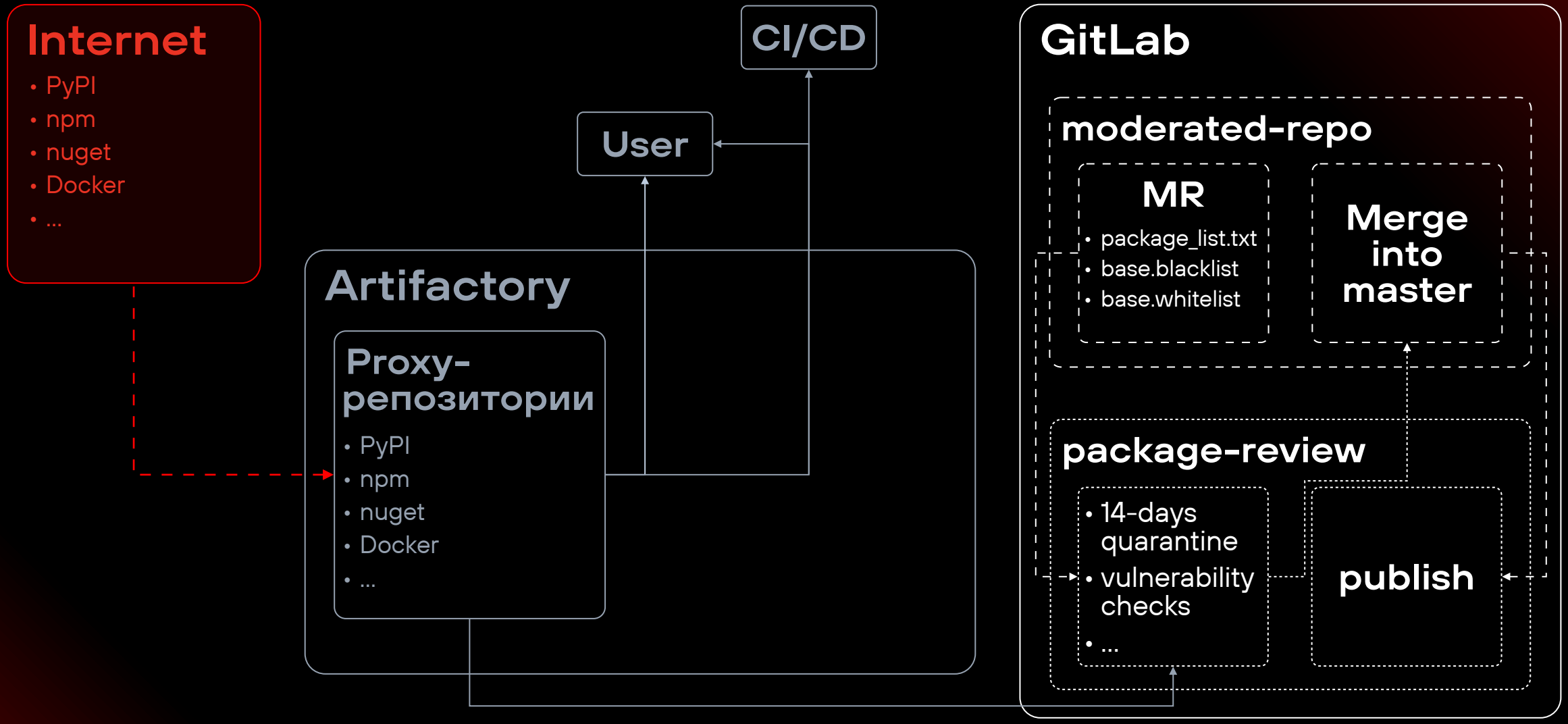
Контроль зависимостей



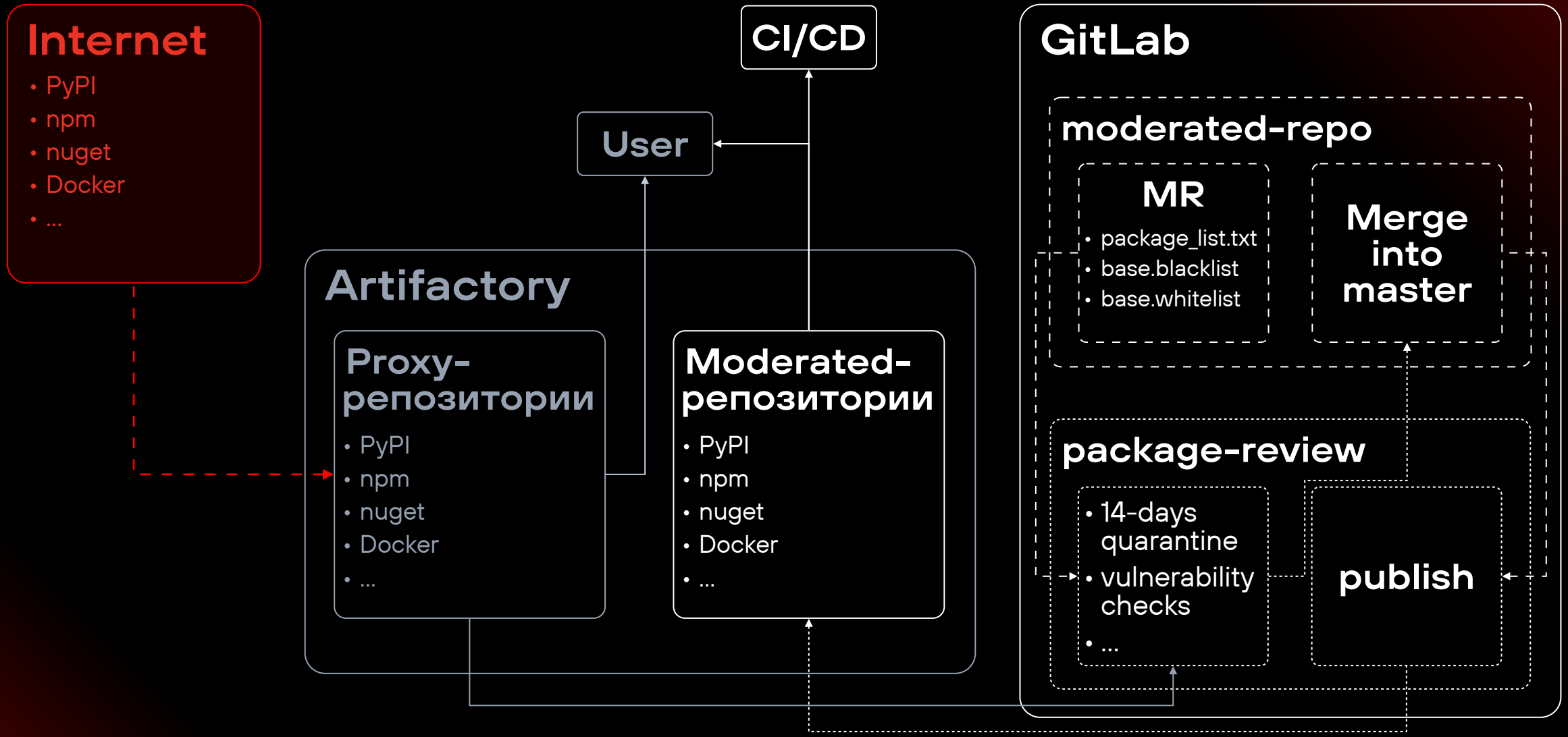
Контроль зависимостей



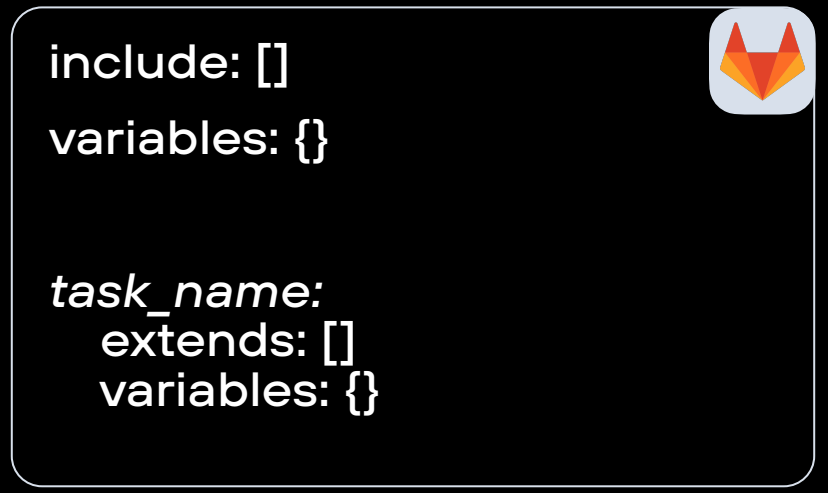
Контроль зависимостей



Контроль зависимостей



Шаблонизация CI/CD



Шаблонизация CI/CD

include: []

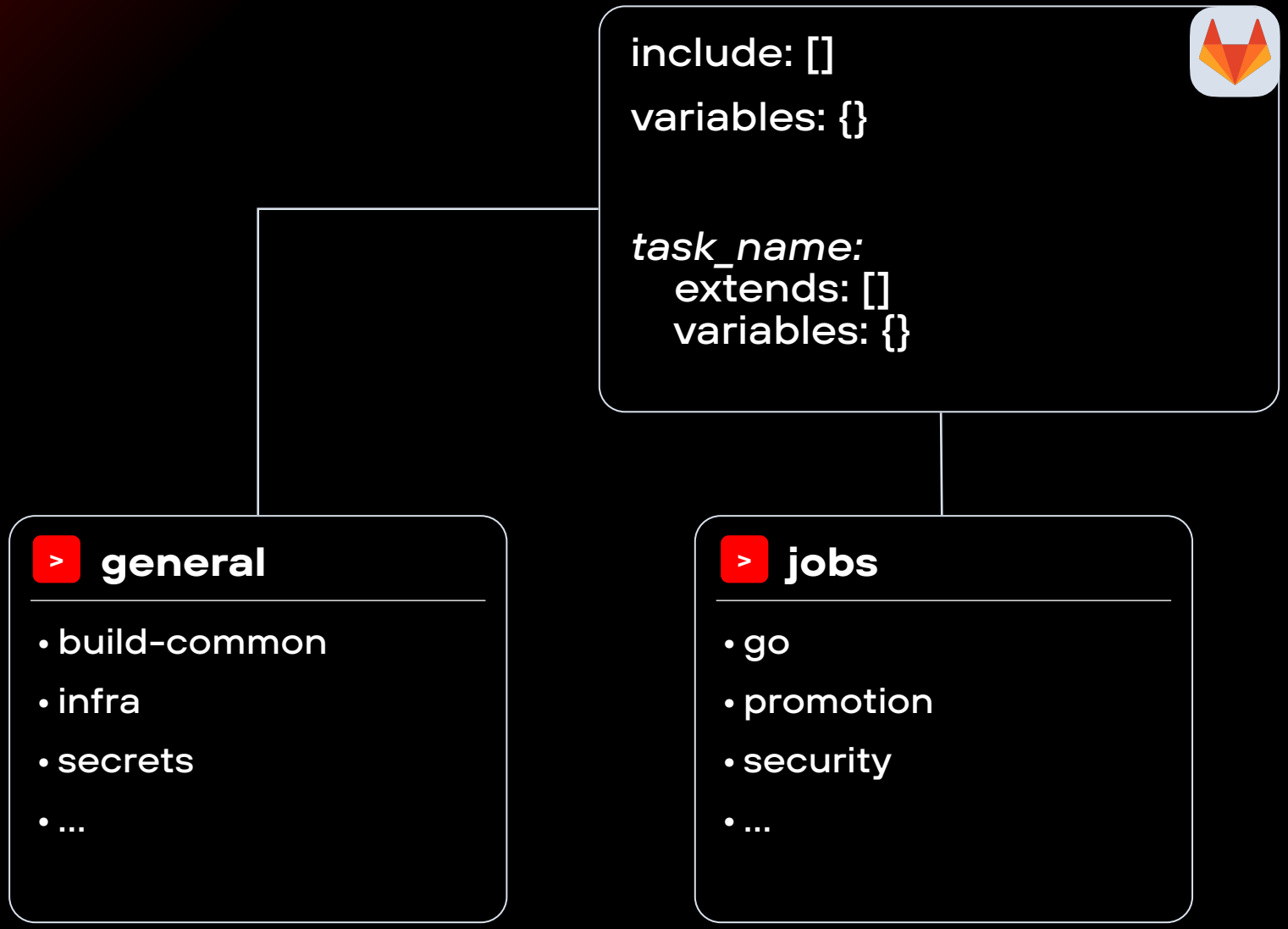
variables: {}

task_name:
  extends: []
  variables: {}

general

- build-common
- infra
- secrets
- ...

Шаблонизация CI/CD

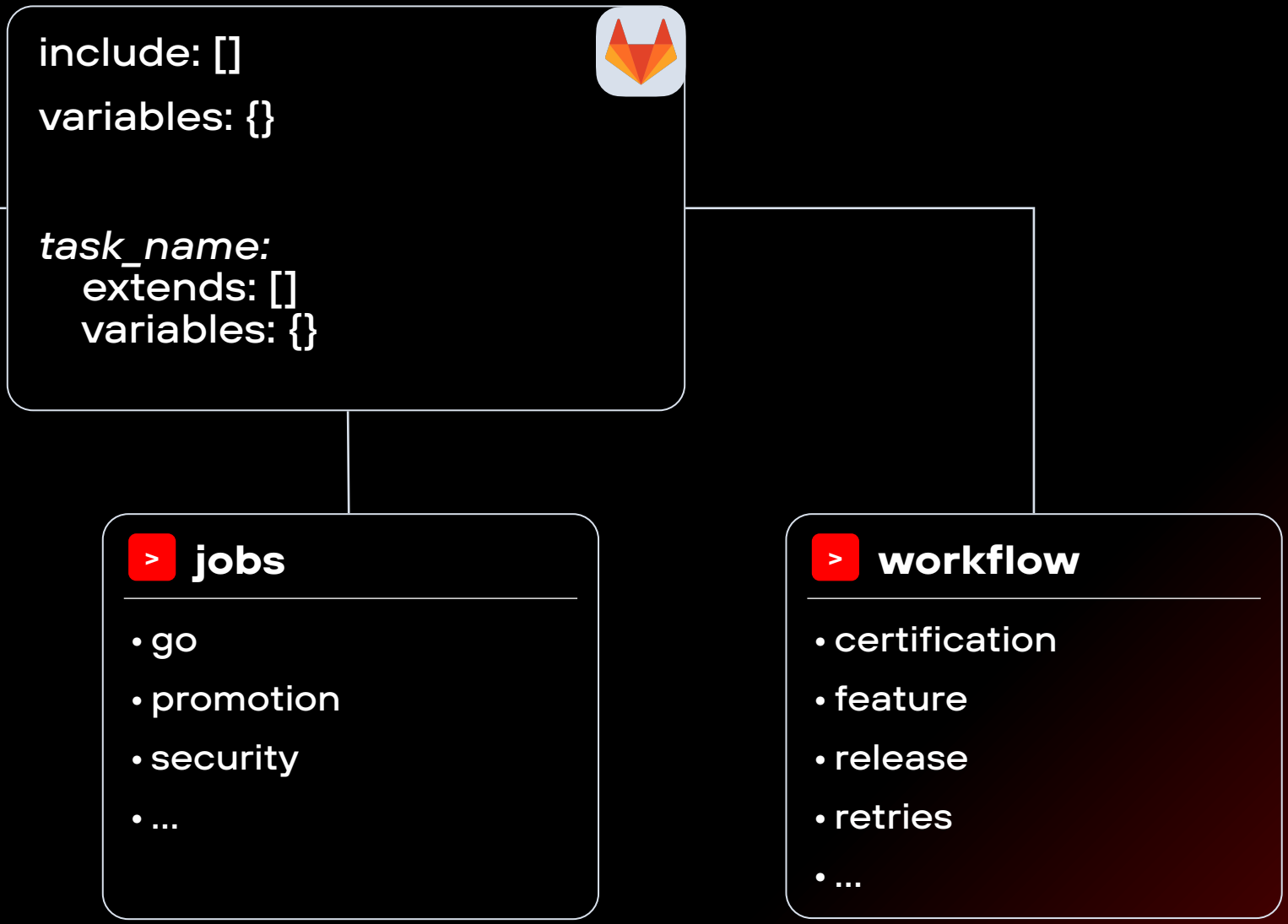


Шаблонизация CI/CD

include: []

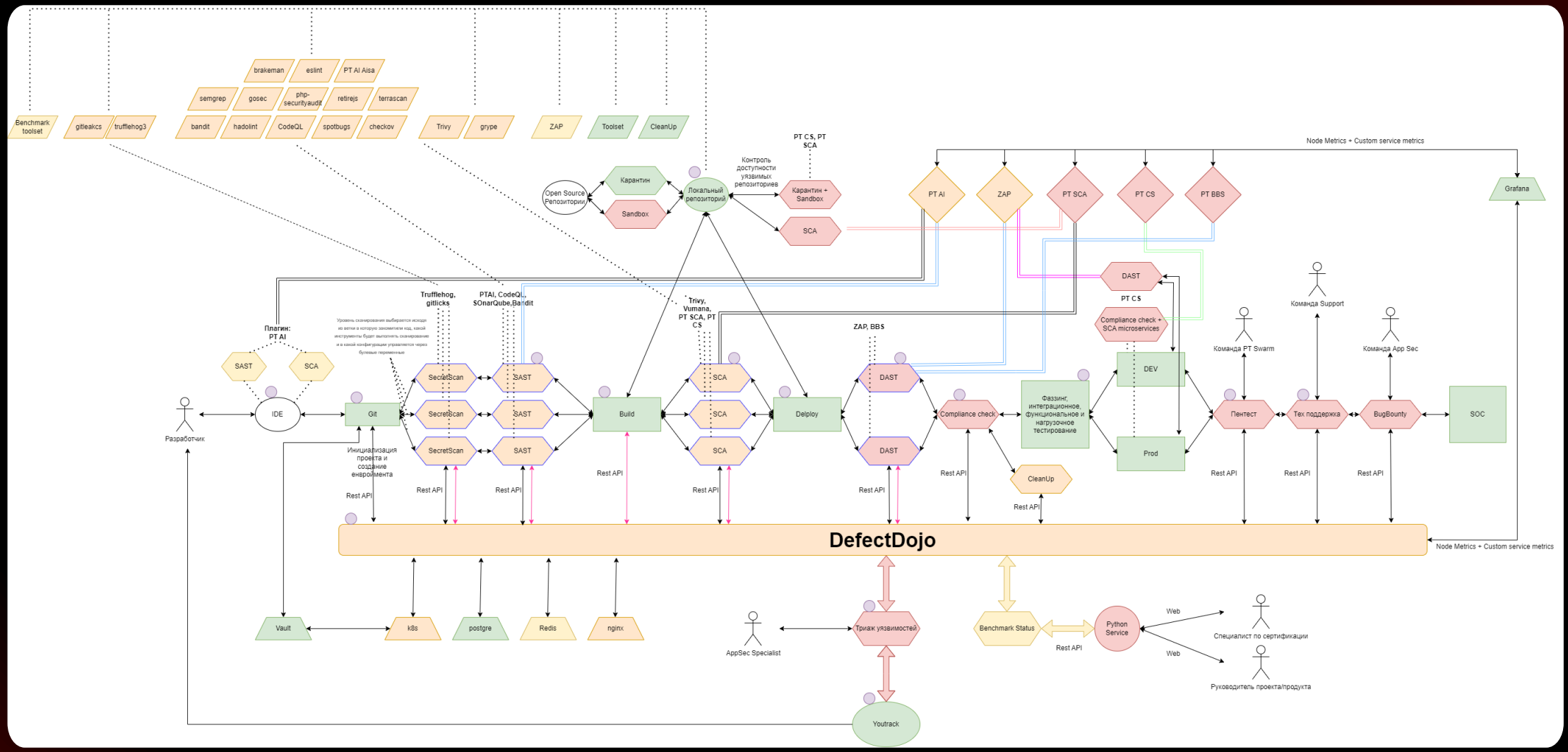
variables: {}

task_name:
  extends: []
  variables: {}



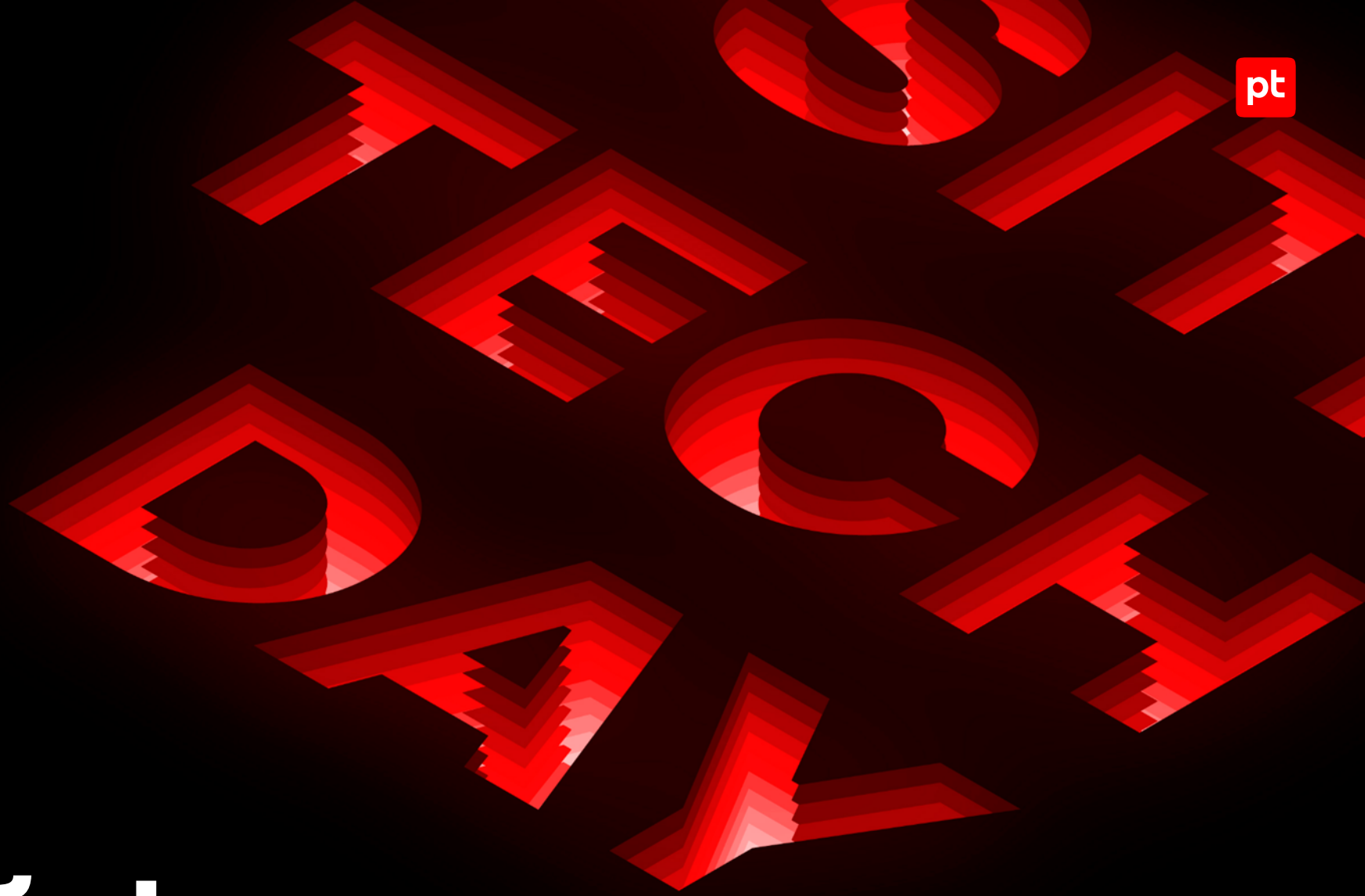
DevSecOps

DevSecOps


Benchmark toolset
gitleakcs
trufflehog3
brakeman
eslint
PT AI Aisa
semgrep
gosec
php-securityaudit
retirejs
terrascan
bandit
hadolint
CodeQL
spotbugs
checkov
Trivy
grype
ZAP
Toolset
CleanUp
Open Source Репозитории
Карантин
Sandbox
Локальный репозиторий
Контроль доступности уязвимых репозиториев
PT CS, PT SCA
Карантин + Sandbox
SCA
Node Metrics + Custom service metrics
PT AI
ZAP
PT SCA
PT CS
PT BBS
Grafana
DAST
PT CS
Compliance check + SCA microservices
Команда Support
Команда PT Swarm
Команда App Sec
DEV
Prod
Плагин: PT AI
SAST
SCA
Trufflehog, gitlicks
PTAI, CodeQL, SOnarQube,Bandit
Trivy, Vumana, PT SCA, PT CS
ZAP, BBS
SecretScan
SecretScan
SecretScan
SAST
SAST
SAST
SCA
SCA
SCA
DAST
DAST
IDE
Git
Build
Delploy
Compliance check
Фаззинг, интеграционное, функциональное и нагрузочное тестирование
CleanUp
Пентест
Тех поддержка
BugBounty
SOC
Разработчик
Инициализация проекта и создание енвройментa
Rest API
DefectDojo
Node Metrics + Custom service metrics
Vault
k8s
postgre
Redis
nginx
AppSec Specialist
Триаж уязвимостей
Youtrack
Benchmark Status
Python Service
Web
Web
Специалист по сертификации
Руководитель проекта/продукта

За безопасность надо платить, а за ее отсутствие – расплачиваться!

Уинстон Черчилль



Спасибо!