DevSecOps & Container Security & CI/CD

Безопасность разработки

Михаил Бессараб, IBM Security Services

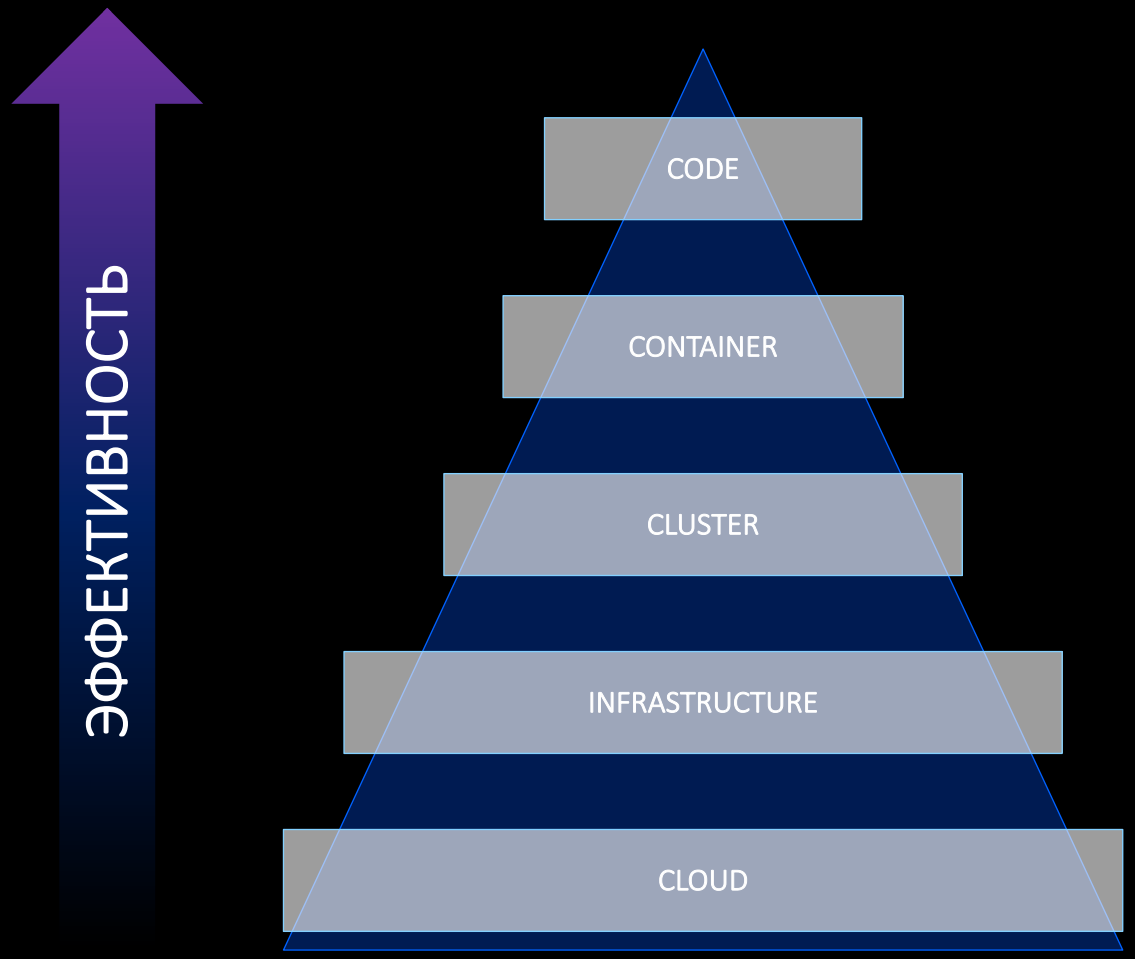
mbessarab@ru.ibm.com

IBM **Security**

DevSecOps framework IBM (Что хотелось бы знать)

Эталонная архитектура IBM Security DevSecOps

Defense in depth (Что нужно знать)



Мониторинг каких активностей может производиться?

- SAST/DAST
- Настройки приложения

- Сканирование уязвимостей
- Конфигурация контейнера
- Подпись образов

- Доступ к API
- Роли (RBAC)
- Политики (Admission control)

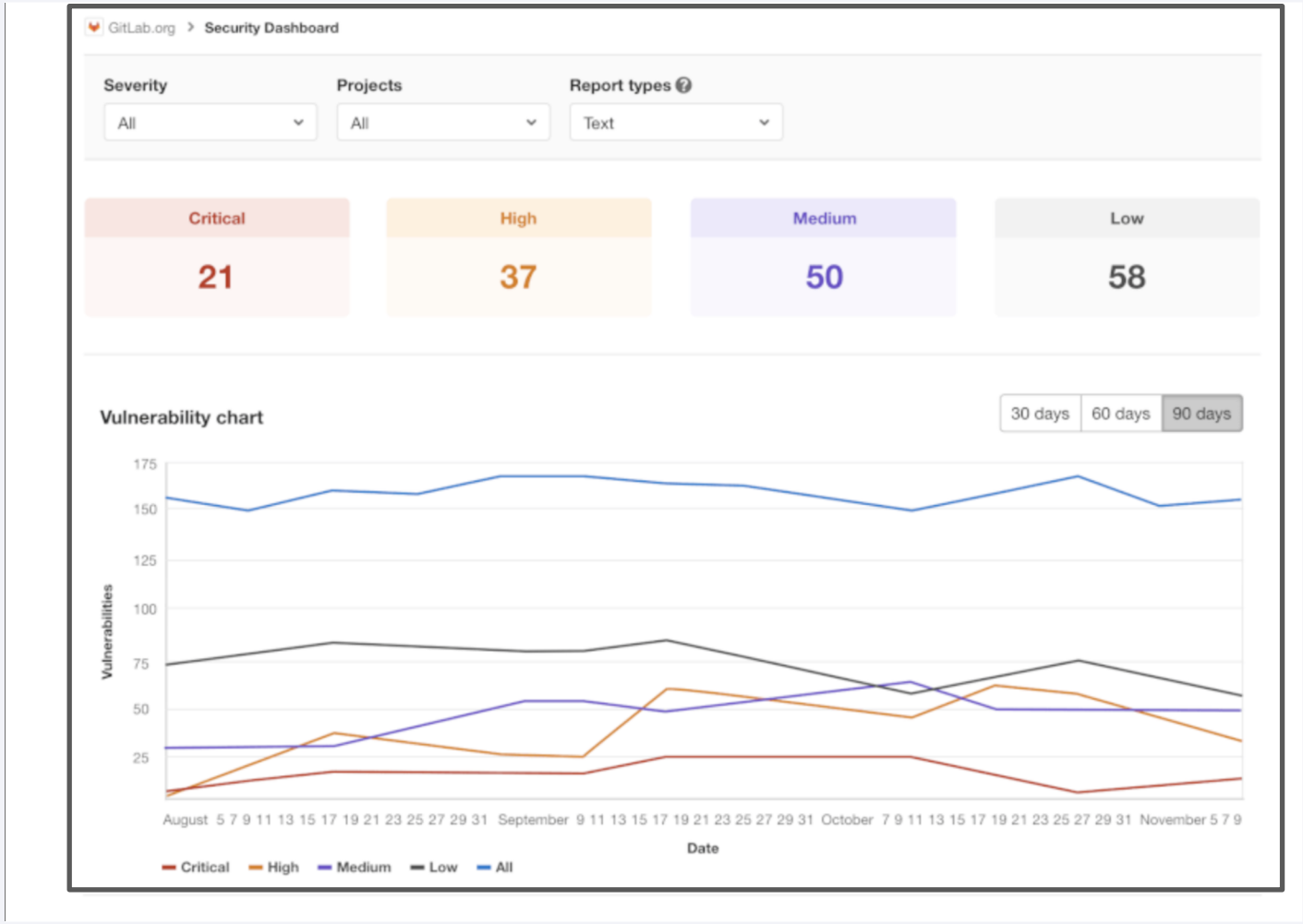
- Сетевая безопасность
- Взаимодействие узлов кластера

- Доступ к учётным данным
- Доступ к ресурсам

Источник: https://kubernetes.io/docs/concepts/security/overview/

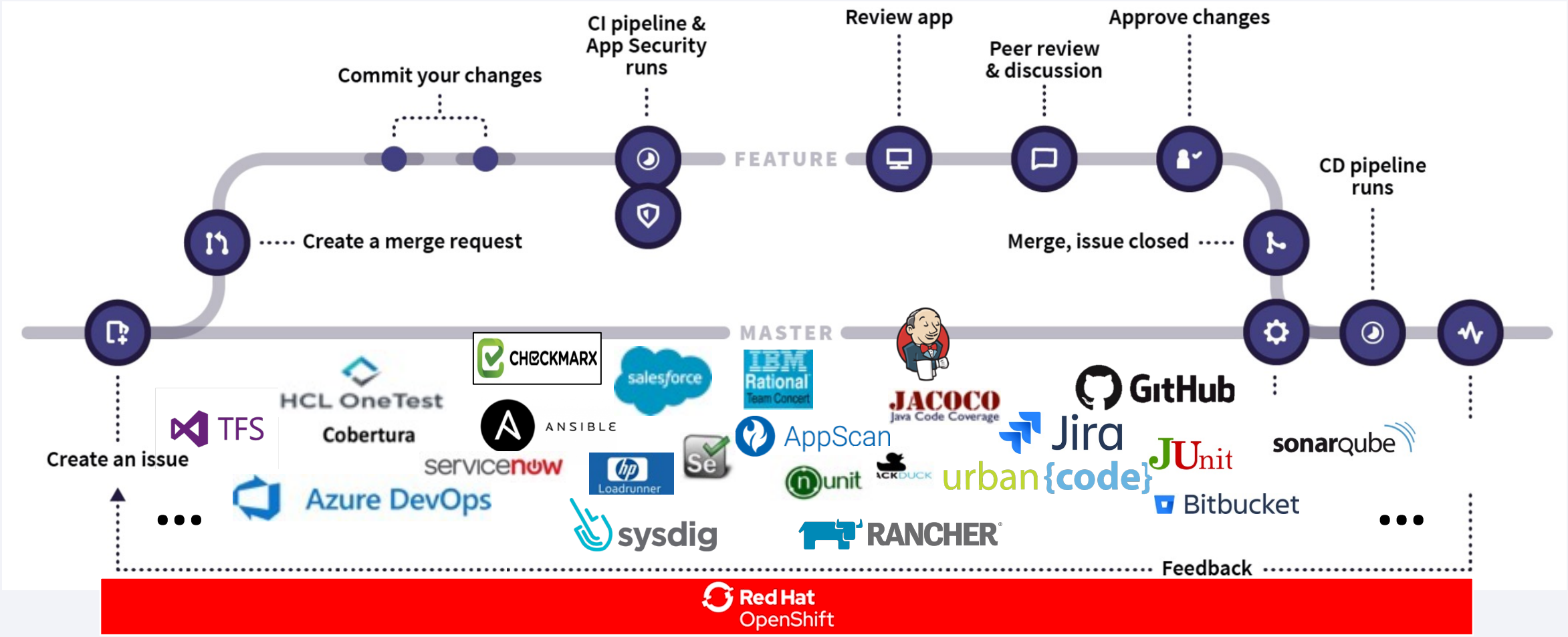
Что на самом деле мы хотим от DevSecOps

- **DevSecOps**
  - SAST
  - DAST
  - Container Scanning
  - Dependency Scanning
  - License Management
  - Secrets Detection
  - Fuzz Testing



Security Dashboards

Один инструмент для всего?



DevOps Security

GitLab

CYBERARK

IBM Security

IBM Cloud

CLOUD NATIVE
COMPUTING FOUNDATION

Container Security

Red Hat

sysdig

aqua

PRISMA
BY PALO ALTO NETWORKS

TREND MICRO

Реализация проектов по безопасности контейнеризации

Consulting and Systems Integration			Support Services
• Анализ технологий и процессов DevSecOps • Подготовка стратегии и дорожной карты по реализации защиты контейнерных технологий • Разработка требований по безопасности контейнерных сред	• Разработка архитектуры защиты контейнерных технологий • Проектирование встроенных и наложенных средств защиты • Разработка процессов ИБ в DevOps	• Внедрение средств защиты • Интеграция с SecOps (SOC, Vuln Mgmt, etc.) • Внедрение процессов DevSecOps	• Мониторинг • Сопровождение • Тюнинг • Управление политиками