

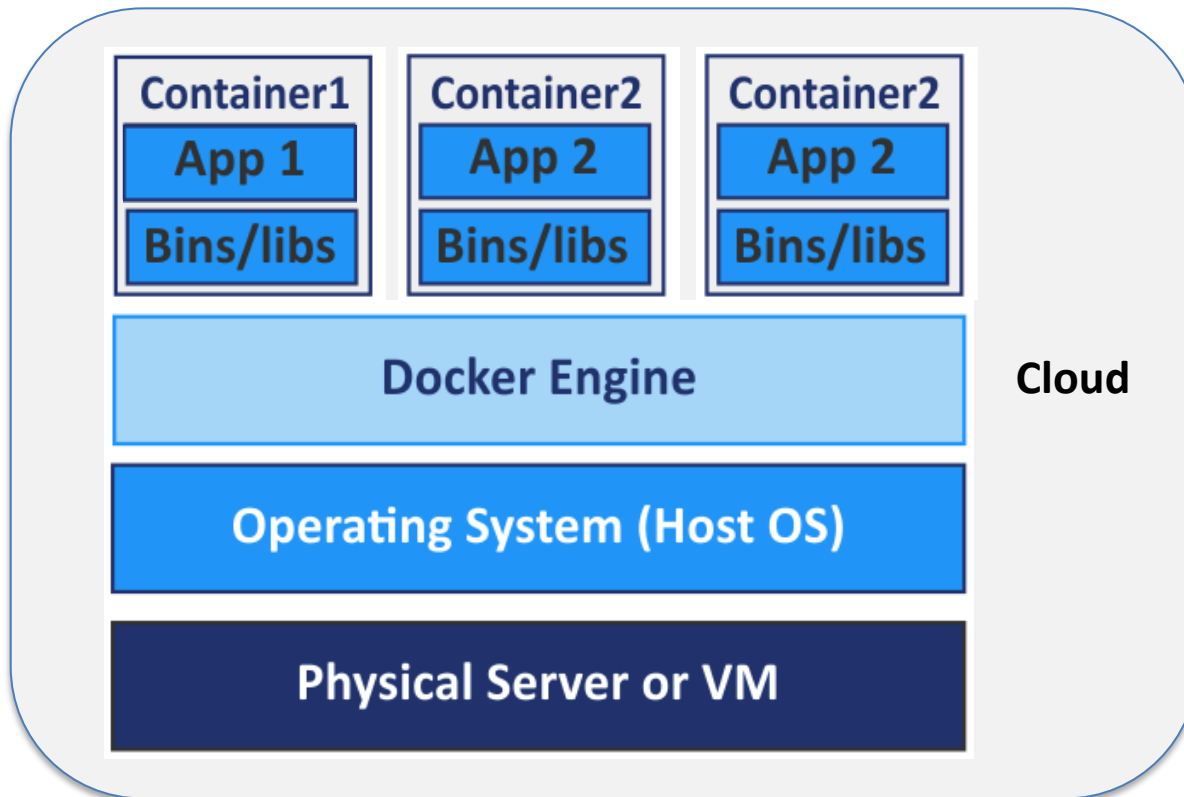


Встраивание безопасности в ИТ процессы и разработку (DevSecOps)

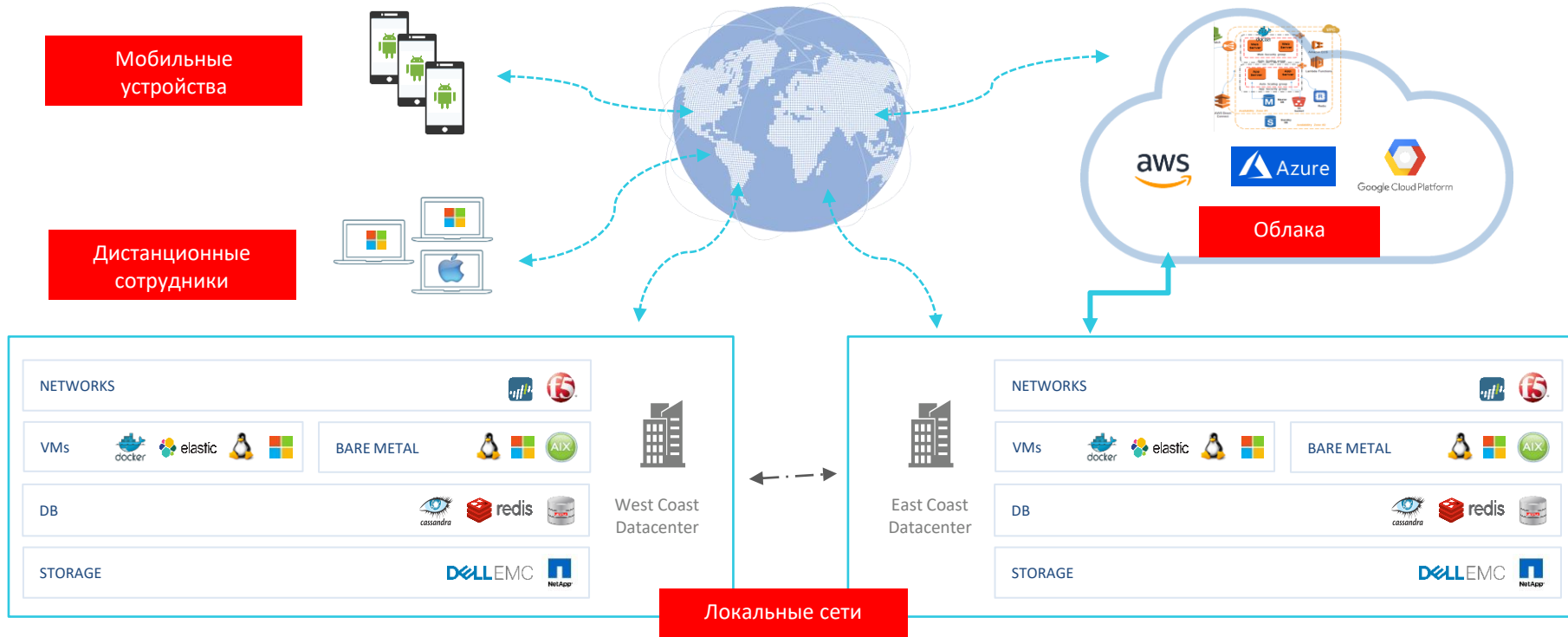
Павел Сотников | CISSP

Управляющий Директор по Восточной Европе, Кавказу и Центральной Азии

Современная ИТ инфраструктура



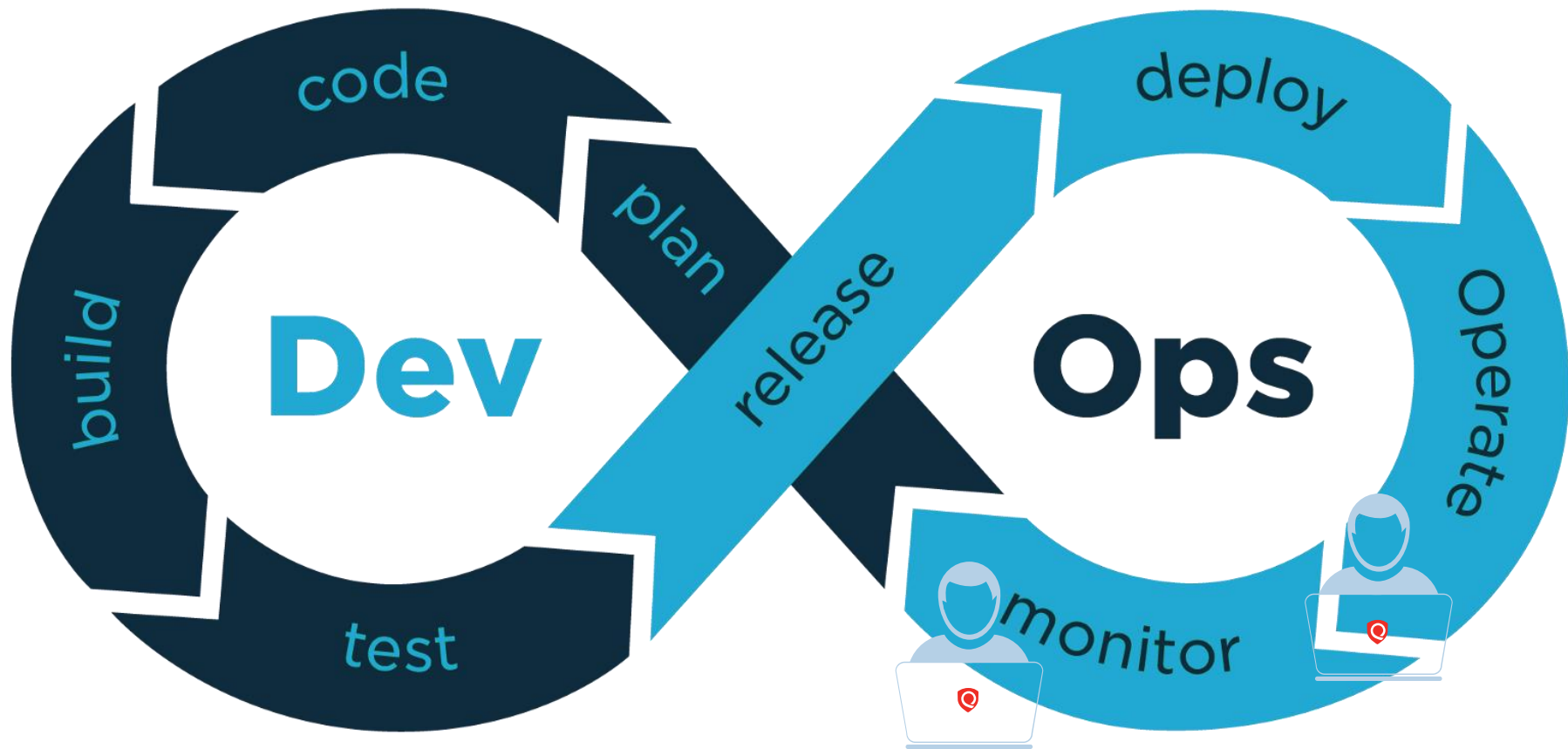
Но всё гораздо сложнее



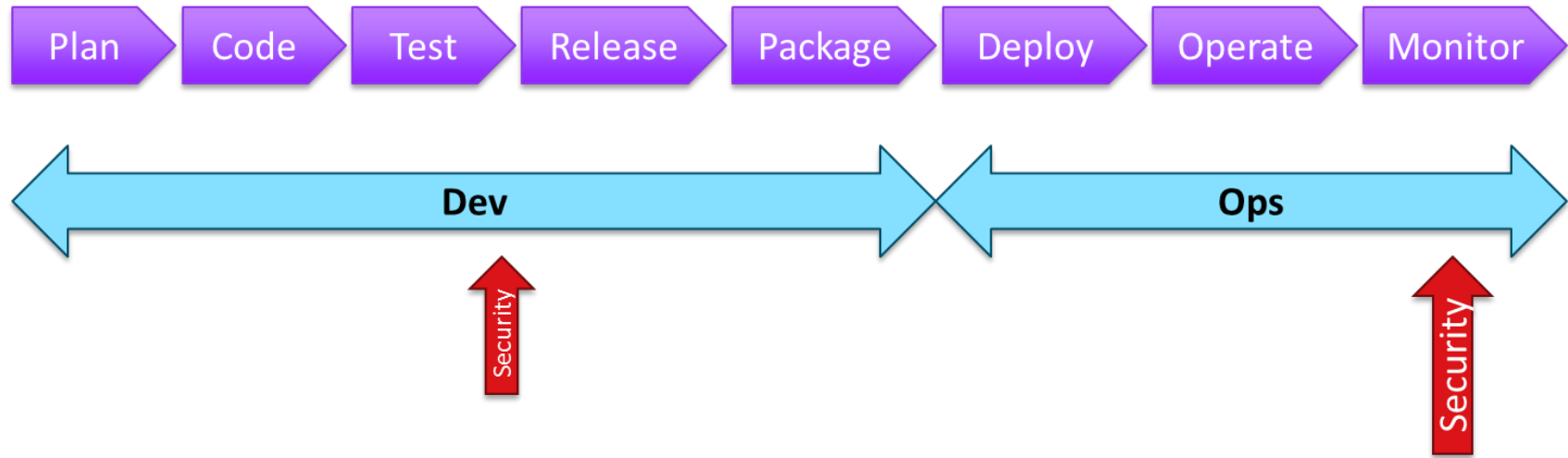
Такую инфраструктуру не защитить посредством
традиционных инструментов/подходов

Почему старые процессы не работают?

- Клиент-серверная архитектура
- Большинство традиционных инструментов требуют вовлечения сотрудника безопасности
- Инструменты заточены на работу только с Production системами
- Большое количество точечных решений, нет взаимосвязи продуктов по безопасности
- Безопасники не вовлечены в ИТ процессы/разработку (DevOps)



Куда встроить безопасность?



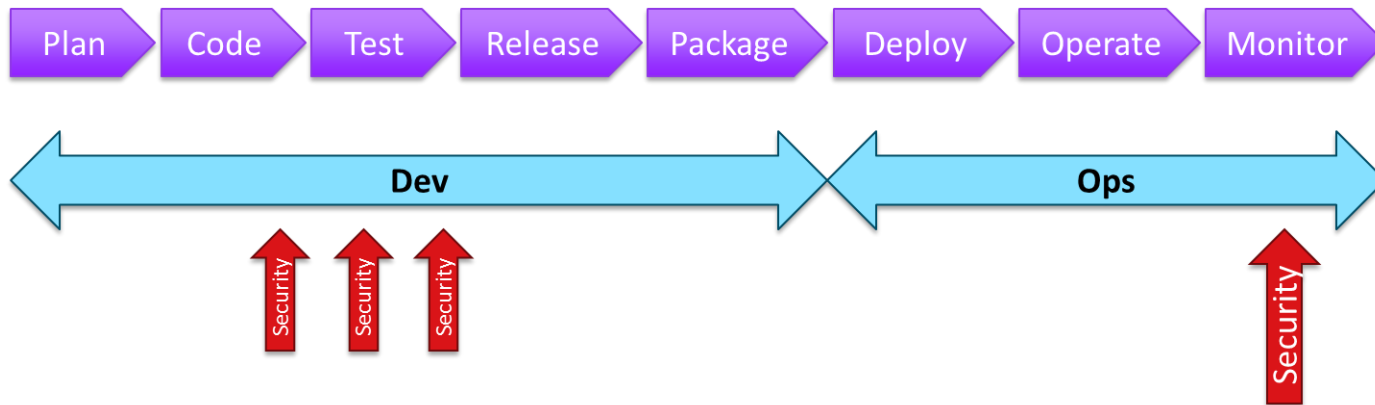
Термин: Сдвиг Влево

«**Улучшение качества** и снижение сбоев за счёт проведения тестирования на более ранних фазах SDLC»

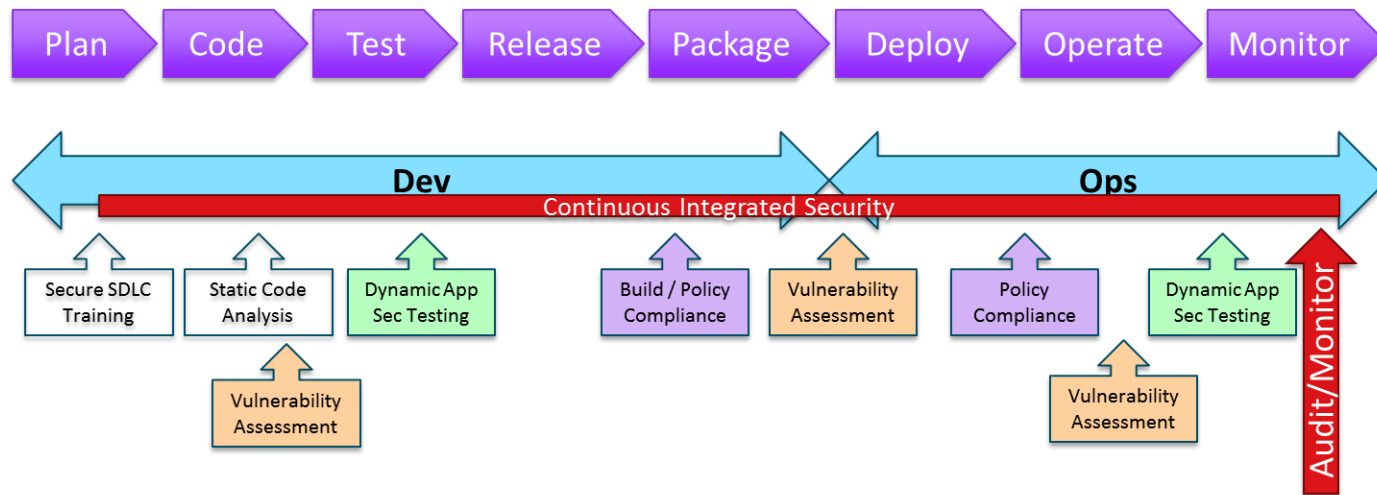
Сдвиг Влево очень хорошо соотносится с методологией **Agile**

- Делать больше на ранних этапах, когда это дешевле и эффективнее
- Непрерывная разработка и тестирование
- Петли обратной связи для увеличения качества

Как применить подход Сдвиг Влево к безопасности?



Непрерывная Безопасность



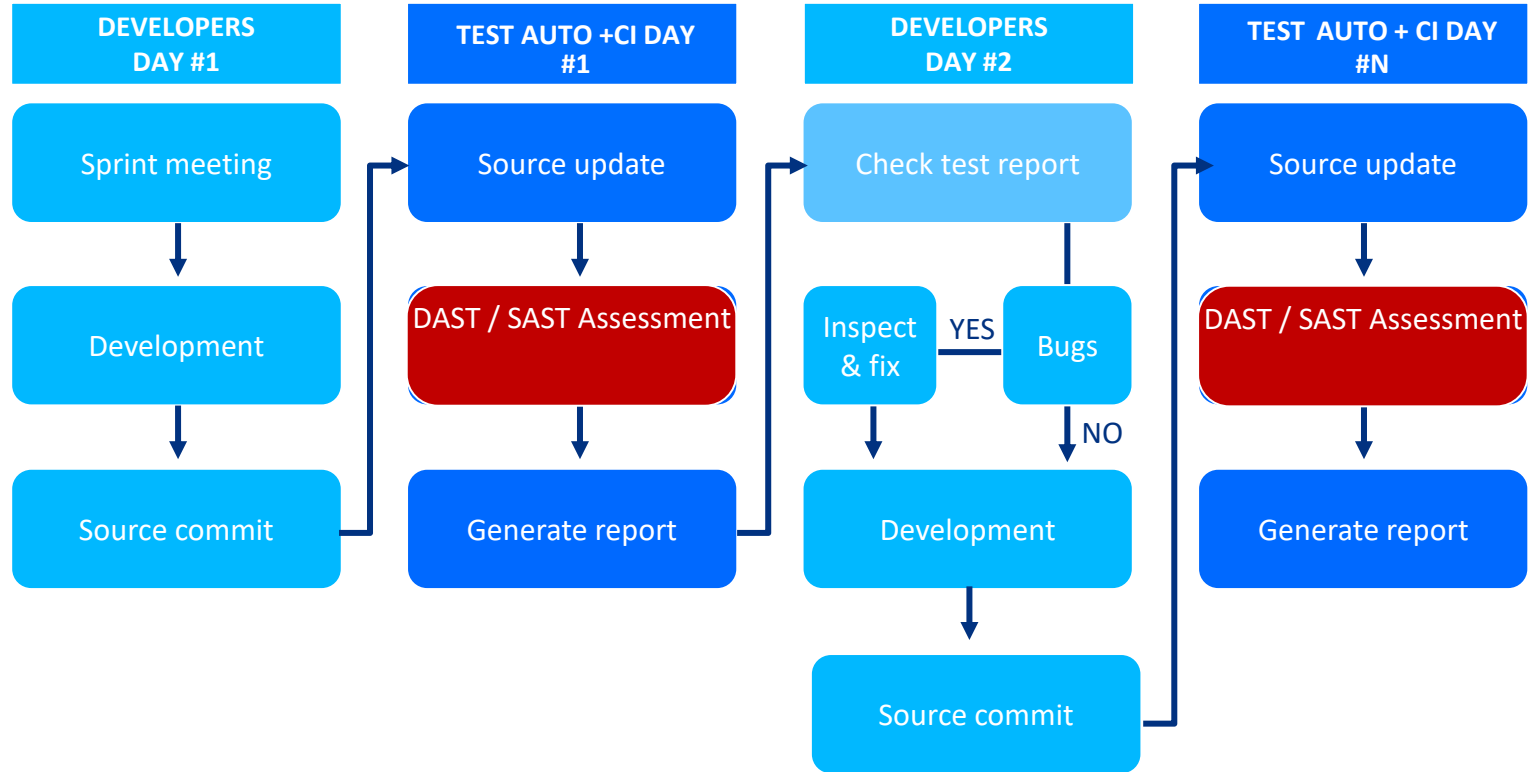
Plan/Code/Test

- Обучение сотрудников основам безопасной разработки
- Привлечение архитекторов безопасности к проектам
- Внедрение инструментов безопасности в конвейер разработчиков
 - SAST сканирование
 - DAST сканирование
- Software composition analysis



Code/Test

SPRINT 1



Configure Scan Pass/Fail Criteria

Set the conditions to fail the build job. The build will fail when ANY of conditions are met.

Failure Conditions

By Vulnerability Severity

By Q

F

Timeout
Qualys V

Freq

Hov

Time

Hov

**Jenkins**

5 GP | log out

Jenkins > WASPluginFreestyle_2 > #23 > Qualys WAS Scan Status [ENABLE AUTO REFRESH](#)

 **Qualys.**

Summary

Vulnerabilities

Scan ID: 23011099

Scan Status: **FINISHED**

Scan Reference: was/1550144860224.32559210

Scan Name: WASPluginFreestyle_2_jenkins_build_23_2019-02-14-17-14

Scan Report: [Click here to view Scan Report on Qualys Portal](#)

Target URL: <http://google-gruyere.appspot.com/922324844025/>

Results Summary

Results Status: SUCCESSFUL

Auth Status: Not Used

Number of Requests: 1688

Links Crawled: 12

Total Duration: 18 min 45 s

Results Stats

Vulnerabilities: 43

Information Gathered: 11

Sensitive Contents: 0

Vulnerabilities (43)



Sev 5 (15)
Sev 4 (2)
Sev 3 (8)
Sev 2 (2)
Sev 1 (16)

Pass/Fail Criteria Results Summary

	QIDs	Severity 5	Severity 4	Severity 3	Severity 2	Severity 1
Criteria Evaluation	✗	✗	✗	✗	✗	✗

✗ Violates criteria ✓ Satisfies criteria - Not Configured

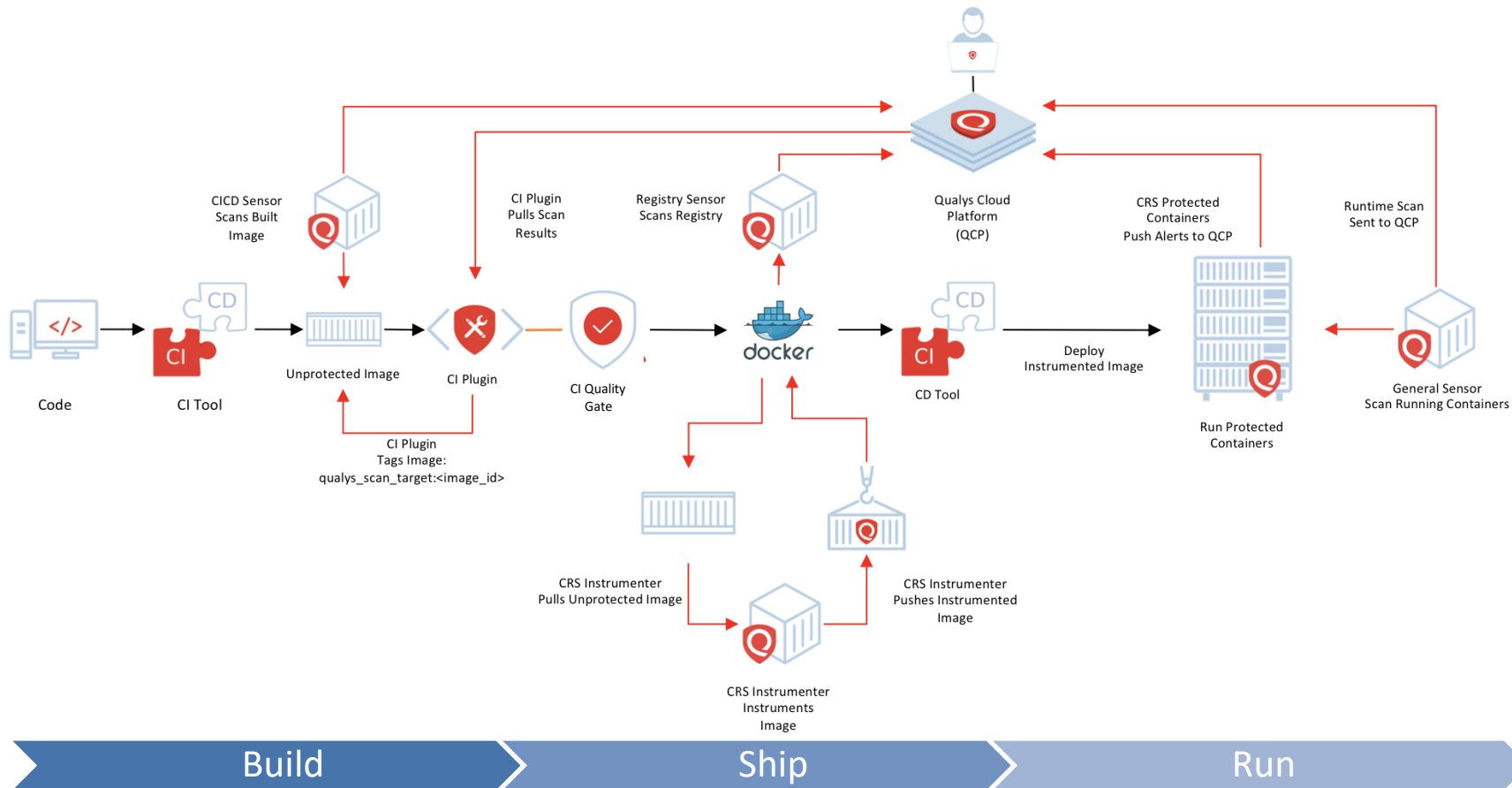
Page generated: Feb 20, 2019 3:01:51 PM IST Jenkins ver. 2.121.3

Release/Package

- Контроль обновлений для образов контейнеров (images)
- Отслеживание использования open source компонентов
- Контроль использования правильных реестров
- Контроль конфигураций
- Встраивание инструментов безопасности непосредственно в контейнеры



Full coverage of Container Lifecycle



Operations – то, с чем сталкивается КАЖДАЯ компания

Deploy/Operate/Monitor

Платформенный подход

- минимизация систем безопасности
- консолидация функций безопасности агентов на устройствах

Использование стандартных образов ОС – преднастройка систем

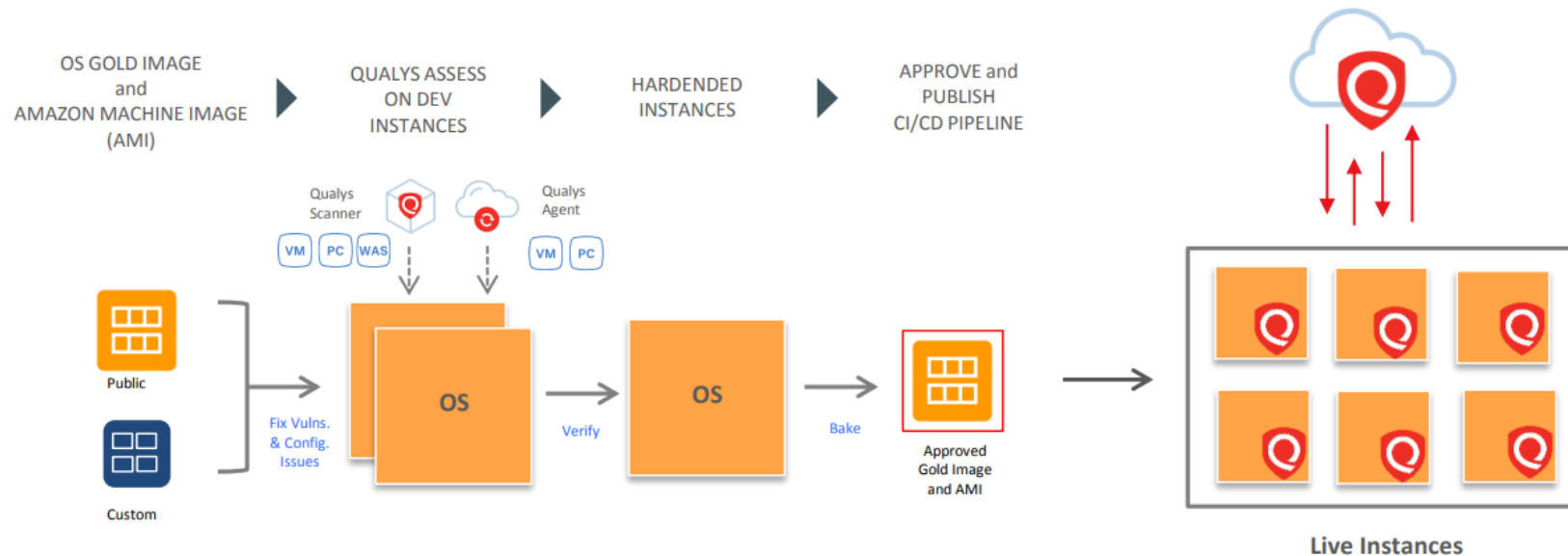
Автоматизация рутинных процессов сбора информации

Возможность сквозного поиска по собираемой информации

Интеграция между системами ИТ и ИБ (исключение человека из процесса)



Создание защищённых образов



План на ближайший год

- Изучить микросервисную архитектуру и процессы разработки
- Оценить текущие ИТ/ИБ решения по следующим параметрам
 - Платформа или нет (возможность консолидации систем посредством платформенного подхода)
 - Наличие API для интеграции с другими системами
 - Наличие плагинов для конвейеров разработчиков / возможность интеграции в эти конвейеры
 - Возможность работы в любой инфраструктуре (локальная сеть/облака/дистанционные сотрудники/мобильные устройства)



Спасибо!

psotnikov@qualys.com