QSC20

QUALYS SECURITY CONFERENCE 2020

The Need to Shift Left and What It Means to Security

Alex Mandernack
Security Solution Architect
Product Management
Qualys, Inc

Traditional World

Each app team builds their own image

(CentOS v1, v2, v3)

PenTest report to Dev (t0+1Mo)

- Dev team dealing with out of date findings
- Not machine readable
- Repeated work across apps 1, 2, 3 (OS level vulns)
- Not doing it often enough due to cost, efficient reasons

Deploy application

(1, 2, 3)

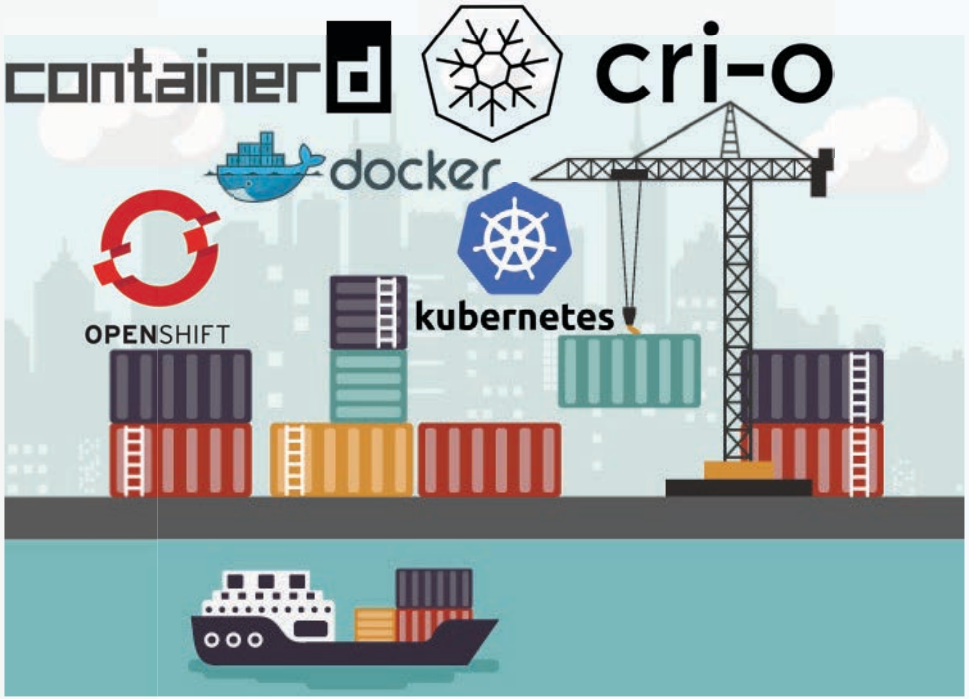
Scan in production (VM, WAS, PC etc.)

- Findings for app 1, 2, 3
- Separate patching workflows for running production workloads (v1, v2, v3

Inefficiencies, slows things down, no standardization across teams, repetition in security workflows

Qualys.

The Driver: Scale, Elasticity & DevOps Pipeline



Qualys.

Can Security Teams do Better?

Shifting Security to the Left

- Developers and security teams must think about security, sooner
- Get security tools into the process earlier
- Automate! Leverage API's, CI plugins
- Golden images
- Scan in the CI pipeline
  - Vulnerability gates in the pipeline
  - Vulnerability information at the fingertips of Dev

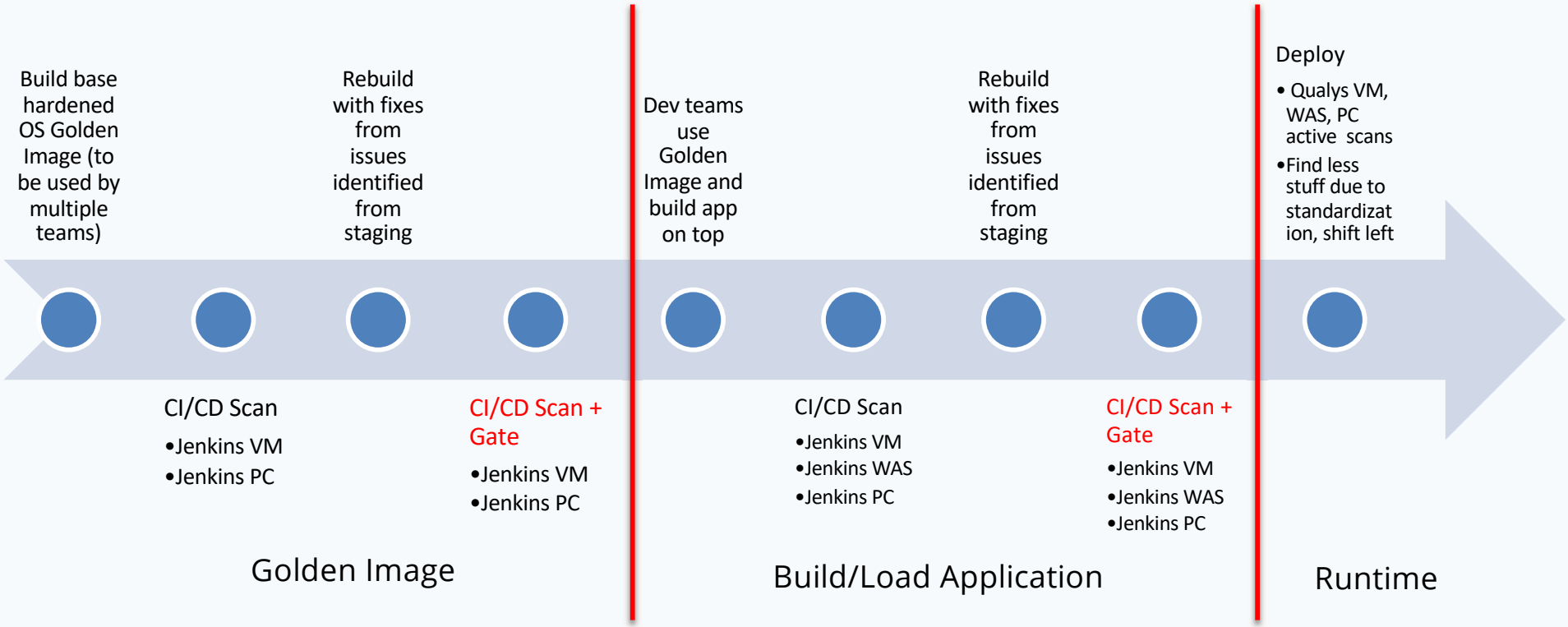
Qualys.

The New Role of the Security Team

- Must not be a roadblock
- Provide security tooling that is self-service for DevOps, Dev
  - CI Plugins
  - APIs
  - Scripting
- Verify and audit the process
  - Dashboards/live data
  - Trending

Qualys.

Shift Left with Qualys!



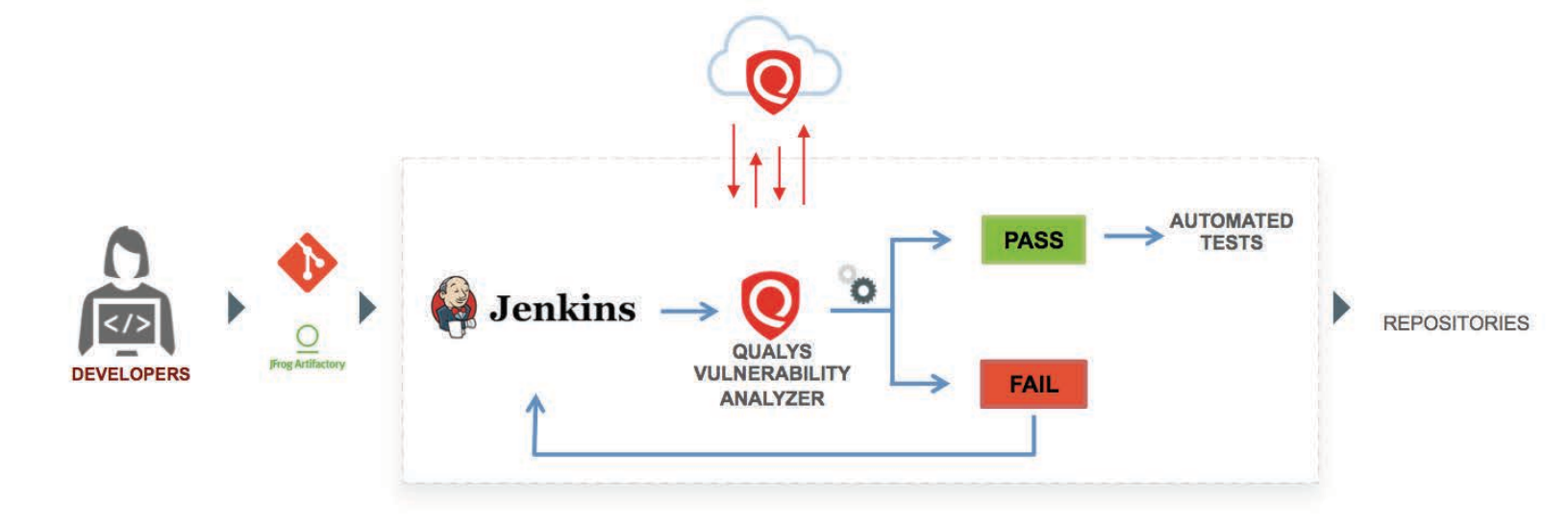
Qualys.

Qualys Jenkins Plugin

Available on the Jenkins Marketplace

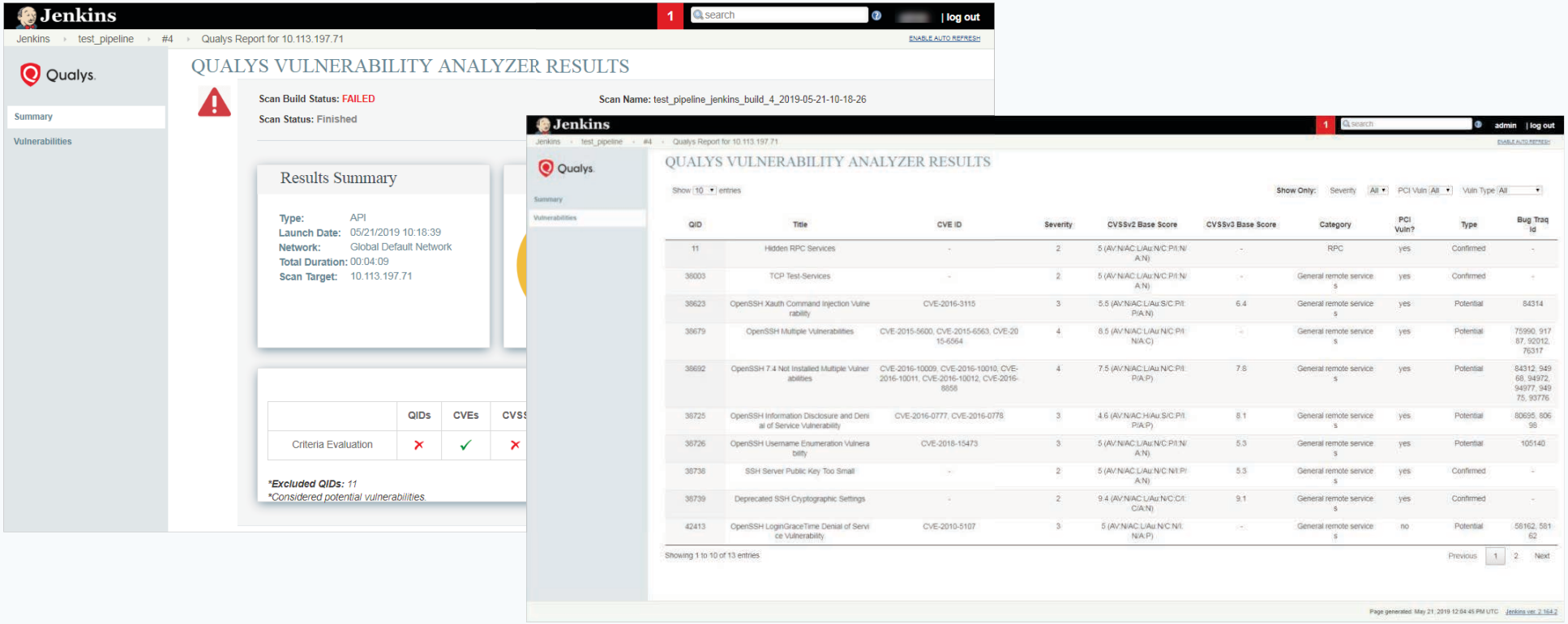
- Vulnerability Management
- Container Security
- Web Application Scanning
- API Security

Secure the CI Pipeline



Qualys.

Jenkins Vulnerability Management Plugin



Qualys.

Jenkins WAS Plugin

Jenkins

Jenkins › WASPluginFreestyle_2 › #23 › Qualys WAS Scan Status

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: SUCCES

Auth Status: Not Used

Number of Requests: 1688

Links Crawled: 12

Total Duration: 18 min 45

Criteria Evaluation

Jenkins

Jenkins › WASPluginFreestyle_2 › #23 › Qualys WAS Scan Status

Qualys.

Summary

Vulnerabilities

QUALYS VULNERABILITIES RESULTS

Show 10 entries

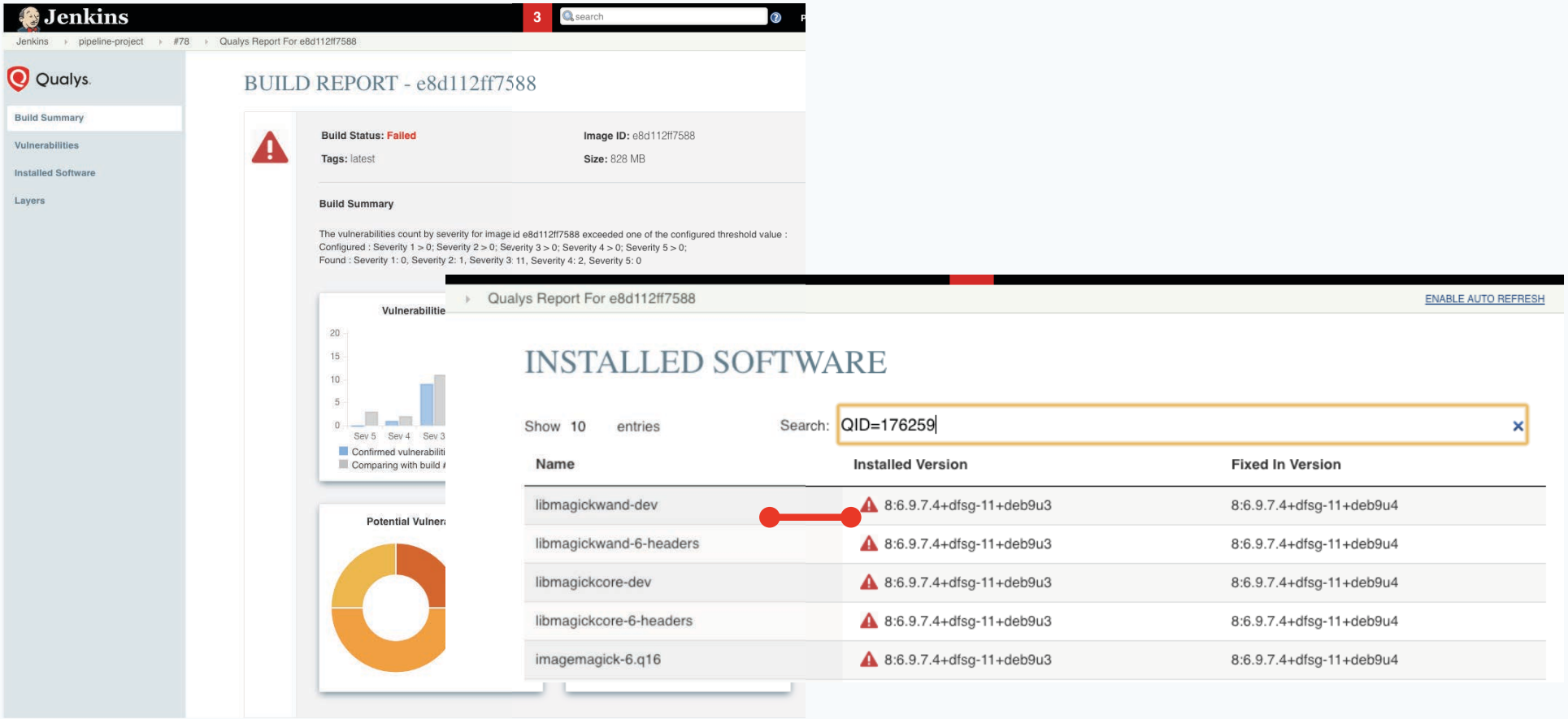
QID	Title	URL	Available Unauthenticated?
150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	http://google-gruyere.appspot.com/922324844025/feed.gtl?uid=%22%3E%3Cqss%20a%3DX166455440Y1Z%3E	Yes
150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	http://google-gruyere.appspot.com/922324844025/login?uid=%3CEMBED%20SRC%3D%2F%2Flocalhost%2Fq.swf%20AllowScriptAccess%3Dalways%3E%3C%2FEMBED%3E&pw=password	Yes
150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	http://google-gruyere.appspot.com/922324844025/snippets.gtl?uid=%20onEvent%3DX166495528Y1Z%20	Yes
150053	Login Form Is Not Submitted Via HTTPS	http://google-gruyere.appspot.com/922324844025/saveprofile	Yes
150053	Login Form Is Not Submitted Via HTTPS	http://google-gruyere.appspot.com/922324844025/login	Yes
150081	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/feed.gtl?uid=cheddar	Yes
150081	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/feed.gtl	Yes
150081	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/#	Yes
150081	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/	Yes
150081	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/newaccount.gtl	Yes

Showing 1 to 10 of 43 entries

Previous 1 2 3 4 5 Next

Qualys.

Jenkins Container Security Plugin



Qualys.

Demo

Qualys GitHub

Automation scripts

Reporting scripts

Open Source community

https://github.com/Qualys

Qualys.

Thank you

Alex Mandernack
amandernack@qualys.com