What to do with those security scans…Facing challenges shifting left

Eric Zirkelbach - Franchise Tax Board – State of California

DEVOPS WORLD by CloudBees

Enterprise Data Revenue Project – FTB

- EDR (Phase 1)
- EDR was the first phase of the Tax Systems Modernization effort. The project focused on creating process improvements resulting in efficiencies, new service options, and increased revenue. The project spanned 5 years, 2011 to 2016, and generated approximately $3.7 billion in additional revenue over the life of the project and an additional $1 billion annually.

https://www.ftb.ca.gov/about-ftb/data-reports-plans/enterprise-data-revenue-project.html

Enterprise Data Revenue Project (con’t)

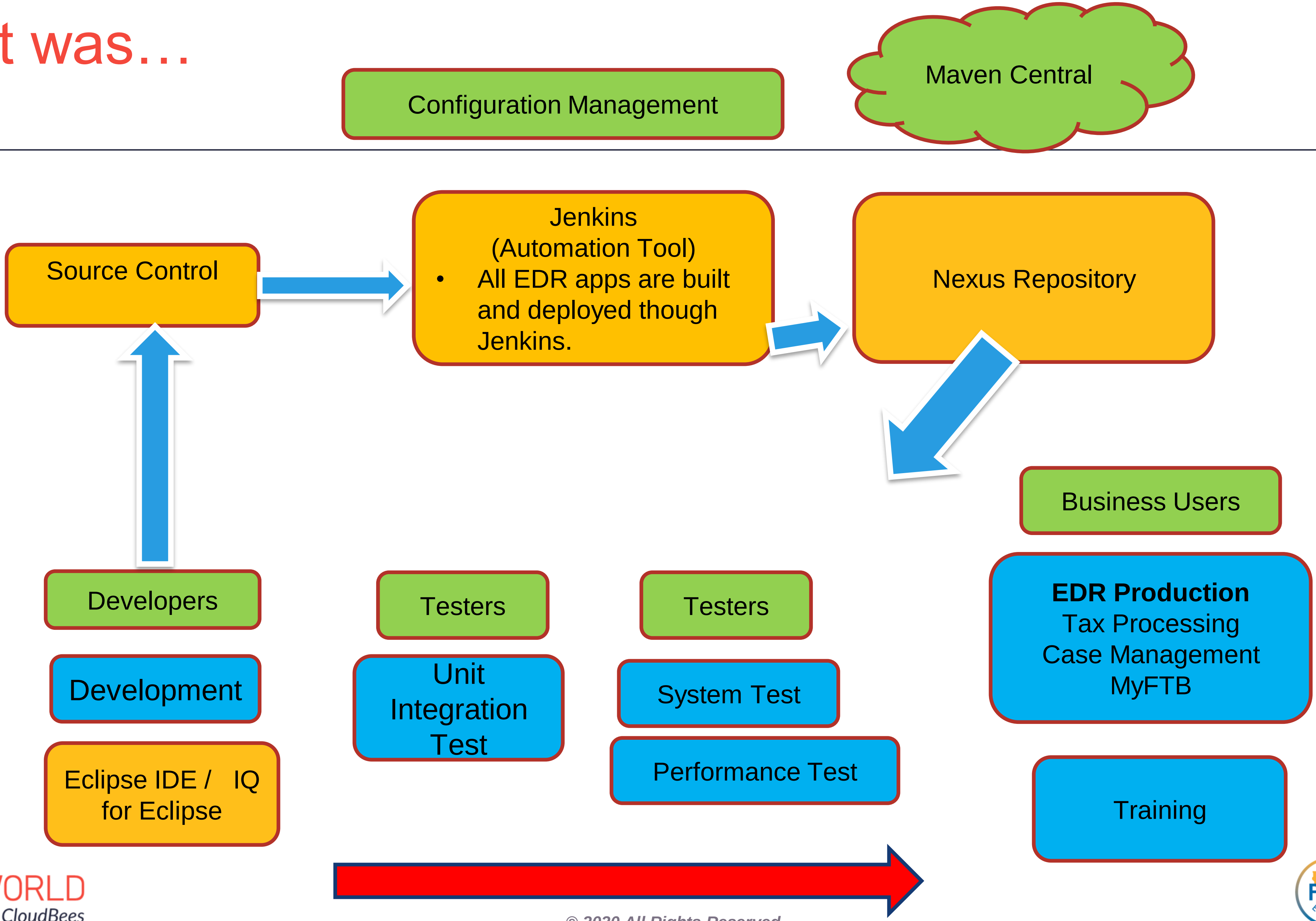
1. New return processing system - Automated processes with real-time validation, data capture, and fraud detection for personal income tax and business entity returns.
2. Improved analytics - Centralized warehouse making data accessible to legacy systems, users and enterprise data modeling mart.
3. New self-service options for taxpayers and representatives - Secure access to online tax information and services, such as viewing returns, payments, withholding, chat, send message and much more.

Enterprise Data Revenue Project (con't)

- 4. Business improvements - Correspondence imaged and routed electronically allowing for efficient case assignment and processing of work.

- 5. Improved legacy systems - Improved notices for taxpayers and enhanced enforcement tools for collection staff.

How it was…



Configuration Management

Maven Central

Source Control

Jenkins
(Automation Tool)

- All EDR apps are built and deployed though Jenkins.

Nexus Repository

Business Users

Developers

Development

Eclipse IDE / IQ for Eclipse

Testers

Unit Integration Test

Testers

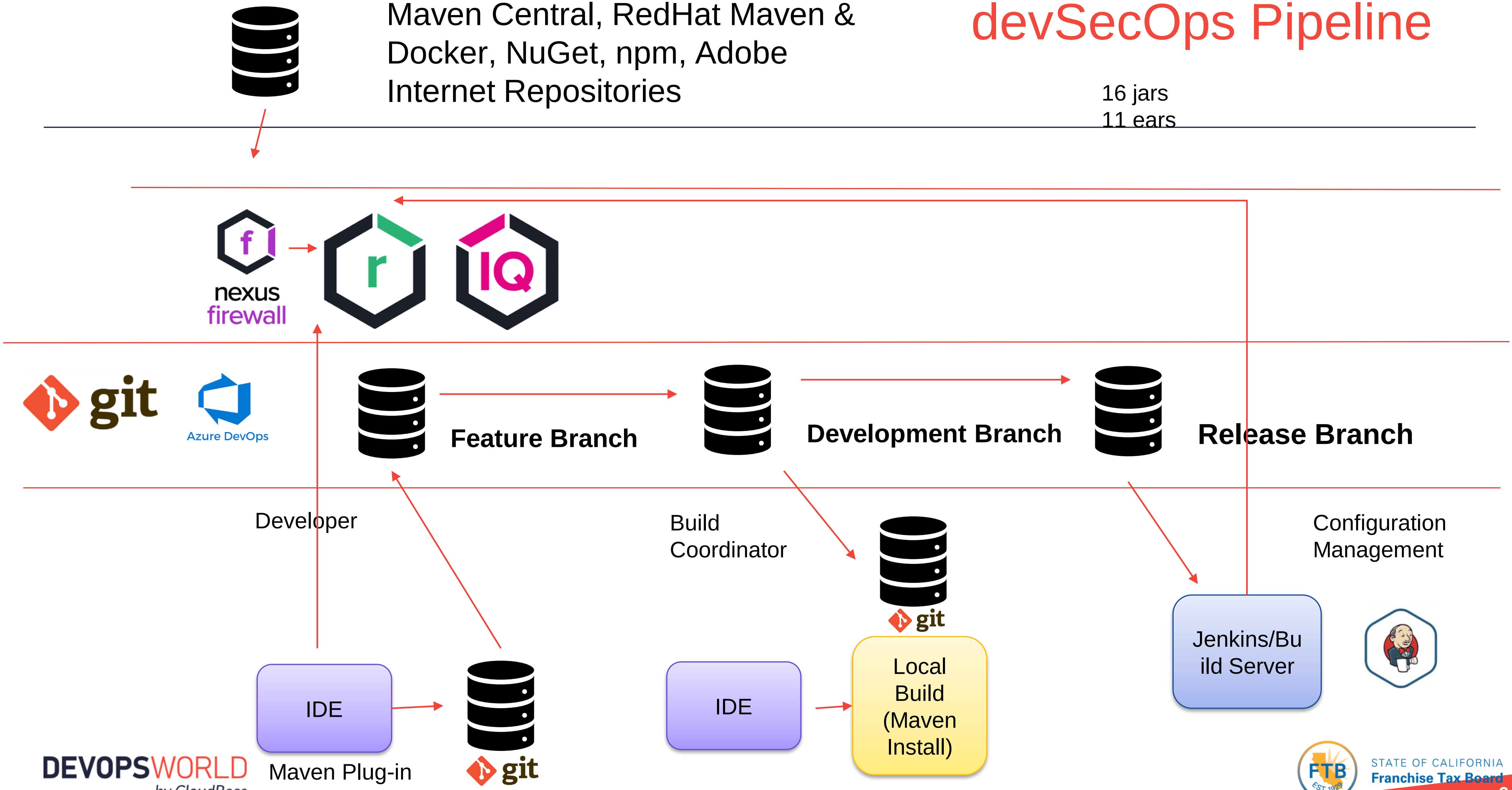
System Test

Performance Test

EDR Production
Tax Processing
Case Management
MyFTB

Training

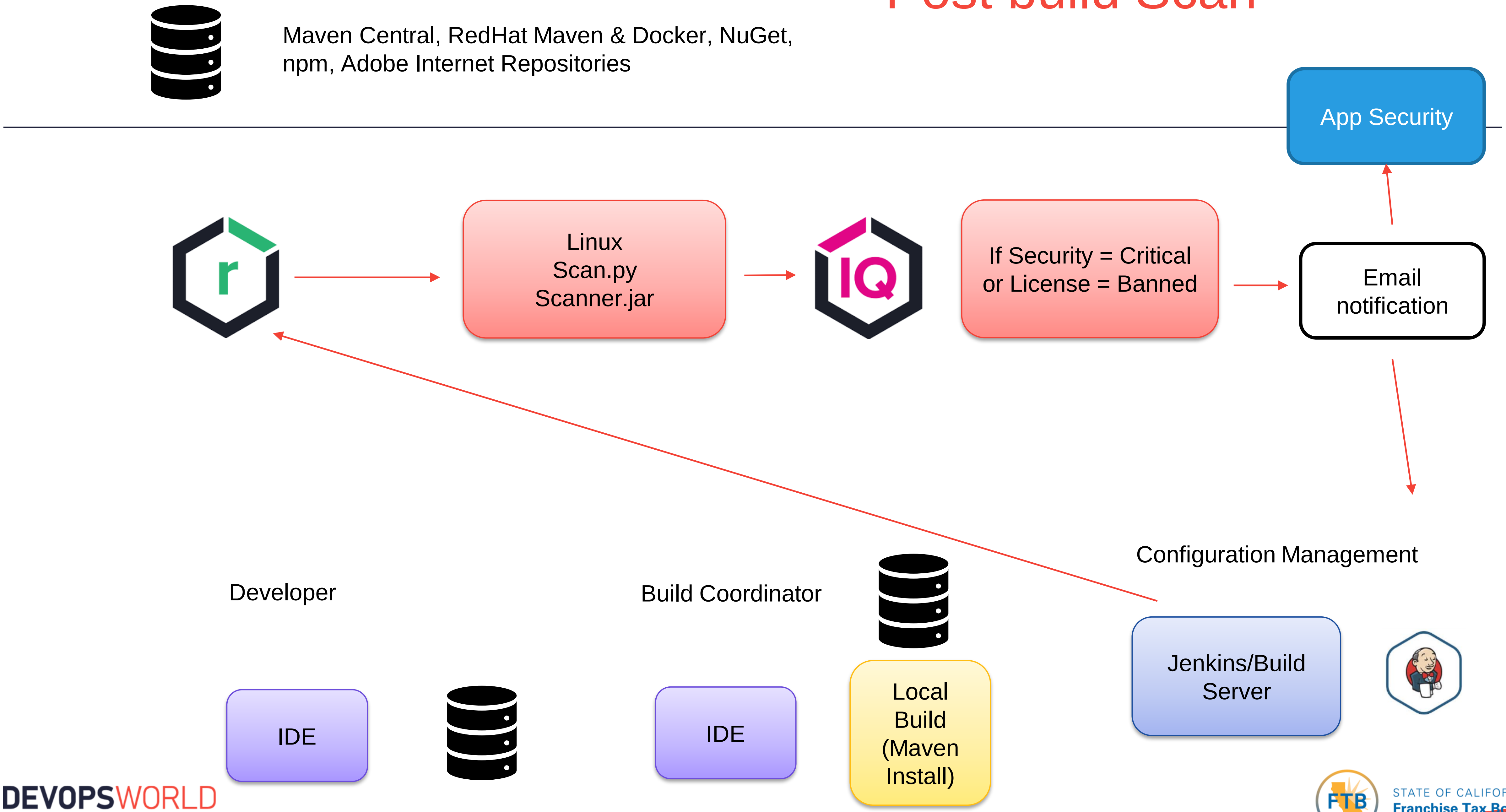
devSecOps Pipeline



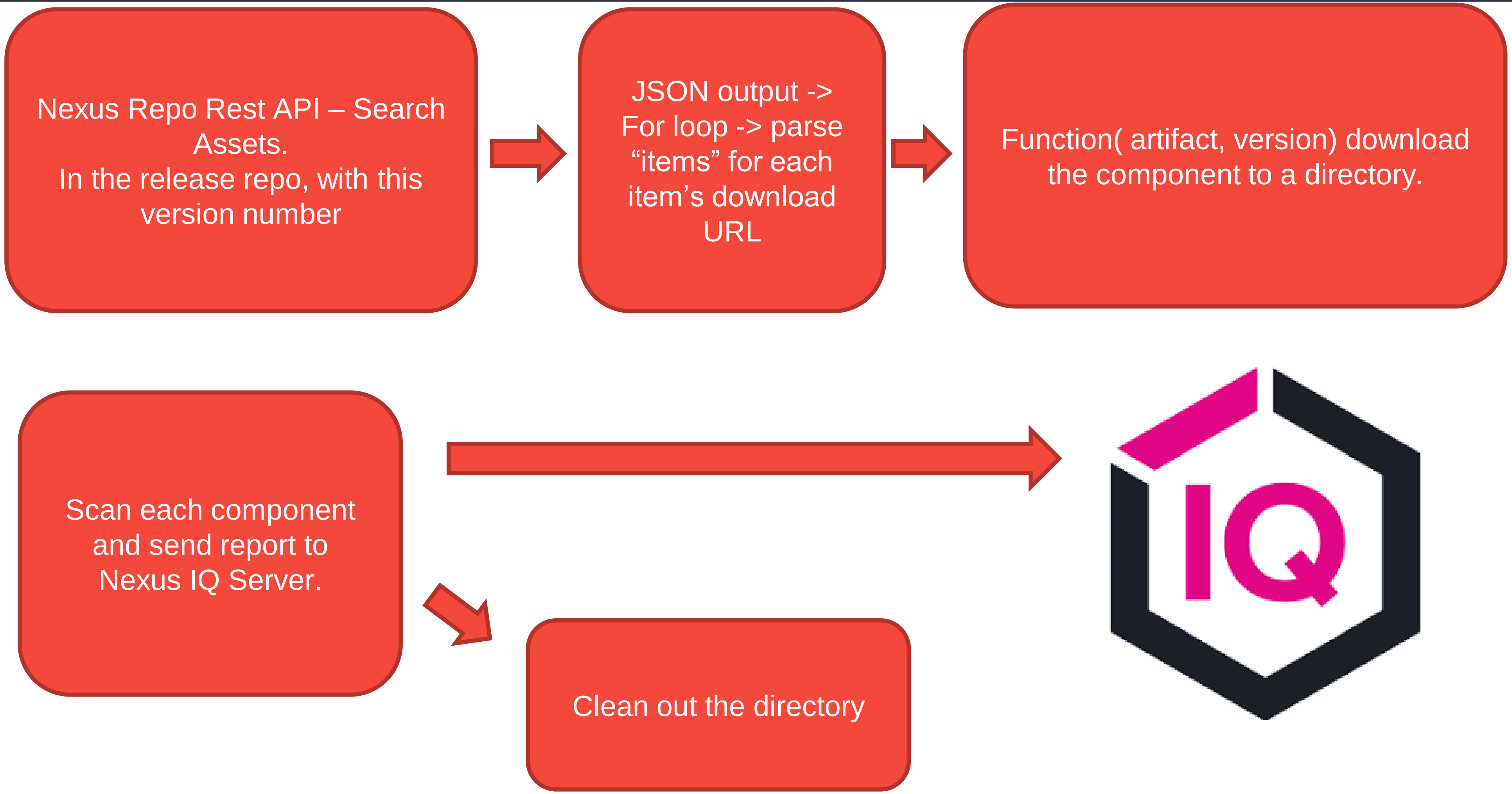
DEVOPSWORLD by CloudBees

STATE OF CALIFORNIA Franchise Tax Board

Post build Scan


Maven Central, RedHat Maven & Docker, NuGet, npm, Adobe Internet Repositories
App Security
Linux Scan.py Scanner.jar
IQ
If Security = Critical or License = Banned
Email notification
Configuration Management
Developer
Build Coordinator
IDE
IDE
Local Build (Maven Install)
Jenkins/Build Server

Nexus-iq-cli.jar – How we use it…



Nexus Repo Rest API – Search Assets.
In the release repo, with this version number

JSON output -> For loop -> parse “items” for each item’s download URL

Function(artifact, version) download the component to a directory.

Scan each component and send report to Nexus IQ Server.

Clean out the directory

Nexus IQ Server – Great reports, now what?

Discussed with Dev leads and asked for their input.
Started weekly meetings with AppSecurity.
Established AppSecurity as the Policy Administrator.
AppSecurity determines priority on vulnerable jars.
AppSecurity creates a defect under a Change Order for each occurrence.
EDR management creates a variance if it can be shown that the code used in the jar does not contain the vulnerability. This gives dev time to add the task to the workload.
At this stage, we are on a case by case basis.

Shifting left

- AppSecurity defect is worked as a Task in TFS.
- Development installs and makes code changes for updated or replaced jar.
- CM team builds, scans and deploys artifact(s), goes thru normal test cycle.

Going forward -→

- Strategy is to clean up the components. In progress
- Purge the Maven hosted or cached components
- Lockdown the firewall.
- Leads and architects have or will have the Sonatype IQ for Eclipse plugin.

Nexus Repository - Pro

- FTB Enterprise Architecture has made our Nexus repo the official Enterprise wide repository for our in house components.
- Along with Java artifacts, we have .net and Docker images that are being built and hosted.
- Some of the features we have appreciated are:
  - API – Developers love this stuff, we do too.
  - Roles – Since we use Active Directory, we can created a role based on a Security group in AD and assign them rights.
  - Users – this keeps improving, Allows to easily search and find a user and grant rights on an ad hoc basis.
  - Tasks – This is improving as well, many administrative functions like keeping the database compressed is automated, set and forget.
  - Upgrading – Only 2 files need to be edited or copied over.
  - Service – Fastest response times, excellent support engineers!

Cloudbees Jenkins

- Cloudbees Operations Center
- Jenkins Master - agents
- Jenkins Development - agent
- Runs nearly all our build and deploy jobs
- Runs scheduled jobs at specific times
- We use the pipeline feature for automation, written in groovy.
- Great support for a very stable and consistent product.

Thank you

FTB – State of California

Eric Zirkelbach

DEVOPS WORLD by CloudBees