Security oriented OpenShift within regulated environments

Dawid Szymański - IT Architect, BZWBK
Tomasz Cholewa - Lead Cloud Architect (RHCA), Mindbox
Jarosław Stakun - Lead Solutions Architect, Red Hat

9th May 2018
Why?
Road to OpenShift
Before Containers

World of Containers

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel

X86 VM
Before Containers

World of Containers

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel

X86 VM

IBM LPAR
Before Containers

World of Containers

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel

X86 VM

IBM LPAR

Technology obsolescence
Before Containers

- X86 VM

World of Containers

- IBM LPAR

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel

- Technology obsolescence

- A lot of manual work
Before Containers

X86 VM

Almost no control over development components

World of Containers

IBM LPAR

Almost no control over development components

OpenShift Infra Design

Technology obsolescence

A lot of manual work

OpenShift Pipeline

OpenShift App Devel

OpenShift Pipeline

OpenShift App Devel
Almost no control over development components

A lot of different versions of platforms

A lot of manual work

Before Containers

World of Containers

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel

X86 VM

IBM LPAR

Technology obsolescence
A lot of different versions of platforms

Almost no control over development components

X86 VM

IBM LPAR

Technology obsolescence

A lot of manual work

Compliance and security are pain in the ...
X86 VM

Almost no control over development components

IBM LPAR

A lot of different versions of platforms

Changes are required in many places

Technology obsolescence

A lot of manual work

Compliance and security are pain in the ...

Before Containers

World of Containers

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel

World of Containers

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel
Docker Swarm Architecture PoC
Before Containers  World of Containers  OpenShift Infra Design  OpenShift Pipeline  OpenShift App Devel

Docker Swarm Architecture PoC

FE 2.0 Project
Before Containers

World of Containers

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel

Docker Swarm Architecture PoC

FE 2.0 Project

Docker Swarm Infra PoC
Before Containers

World of Containers

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel

Docker Swarm Architecture PoC

FE 2.0 Project

Docker Swarm Infra PoC

BZWBK24 Docker in Production
We all go together!
Before Containers → World of Containers → OpenShift Infra Design → OpenShift Pipeline → OpenShift App Devel

- Docker Swarm Architecture PoC
- FE 2.0 Project
- Docker Swarm Infra PoC
- BZWBK24 Docker in Production

We all go together! Docker Swarm issues
Before Containers

World of Containers

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel

Docker Swarm Architecture PoC

FE 2.0 Project

Docker Swarm Infra PoC

We all go together!

Docker Swarm issues

RFI

RFP

BZWBK24 Docker in Production

We all go together!
Docker Swarm Architecture PoC

FE 2.0 Project

Docker Swarm Infra PoC

We all go together!

Docker Swarm issues

RFI RFP

OpenShift!

Before Containers

World of Containers

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel

BZWBK24 Docker in Production
Bank central

1️⃣ Use internal registry and
2️⃣ external if needed!

Secure by design!
1️⃣ Service Serving Certificate Secrets!

OpenShift Infra Design

OpenShift Pipeline

OpenShift App Devel

Before Containers

World of Containers

4 Clusters
2 Prod / 2 Test

3 Clusters
2 Prod / 1 Test

Use internal registry and external if needed!
Adjusting deployments to new cloud native reality
Before Containers  World of Containers  OpenShift Infra Design  OpenShift Pipeline  OpenShift App Devel
Continuous Deployment pipeline

- Only defined list of people allowed to approve

- Checkout
- Deploy zt002
- Running smoke tests
- Deploy zt004
- Deploy prod
Speeding up deployment with CD pipelines
Release pipeline

Multiple microservices

All that is required to run an app
# Release pipeline

<table>
<thead>
<tr>
<th></th>
<th>Checkout</th>
<th>Check release project</th>
<th>Delete project</th>
<th>Create project</th>
<th>Deploy application</th>
<th>Running smoke tests</th>
<th>Publish release</th>
<th>Email notification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>11s</td>
<td>4s</td>
<td>5s</td>
<td>8s</td>
<td>17s</td>
<td>1min 6s</td>
<td>50s</td>
<td>1s</td>
</tr>
<tr>
<td><strong>fe20-release-0.4.3</strong></td>
<td></td>
<td>2s</td>
<td>2s</td>
<td>4s</td>
<td>8s</td>
<td>1min 10s</td>
<td>46s</td>
<td>1s</td>
</tr>
<tr>
<td>Apr 04</td>
<td></td>
<td>2s</td>
<td>2s</td>
<td>4s</td>
<td>8s</td>
<td>1min 10s</td>
<td>46s</td>
<td>1s</td>
</tr>
<tr>
<td>14:26</td>
<td></td>
<td>2s (paused for 15s)</td>
<td>2s</td>
<td>4s</td>
<td>8s</td>
<td>1min 10s</td>
<td>46s</td>
<td>1s</td>
</tr>
<tr>
<td></td>
<td>14s</td>
<td>4s (paused for 1min 6s)</td>
<td>6s</td>
<td>9s</td>
<td>19s</td>
<td>55s</td>
<td>51s</td>
<td>1s</td>
</tr>
<tr>
<td><strong>fe20-release-0.4.2</strong></td>
<td></td>
<td>15s (paused for 3s)</td>
<td>6s</td>
<td>9s</td>
<td>20s</td>
<td>1min 4s</td>
<td>51s</td>
<td>1s</td>
</tr>
<tr>
<td>Mar 22</td>
<td></td>
<td>2 commits</td>
<td>6s</td>
<td>9s</td>
<td>20s</td>
<td>1min 4s</td>
<td>51s</td>
<td>1s</td>
</tr>
<tr>
<td>14:04</td>
<td></td>
<td></td>
<td>6s</td>
<td>9s</td>
<td>20s</td>
<td>1min 4s</td>
<td>51s</td>
<td>1s</td>
</tr>
<tr>
<td><strong>fe20-release-0.4.1</strong></td>
<td></td>
<td>12s (paused for 2s)</td>
<td>6s</td>
<td>9s</td>
<td>20s</td>
<td>51s</td>
<td>47s</td>
<td>1s</td>
</tr>
<tr>
<td>Mar 22</td>
<td></td>
<td>1 commits</td>
<td>6s</td>
<td>9s</td>
<td>20s</td>
<td>51s</td>
<td>47s</td>
<td>1s</td>
</tr>
<tr>
<td>12:40</td>
<td></td>
<td></td>
<td>6s</td>
<td>9s</td>
<td>20s</td>
<td>51s</td>
<td>47s</td>
<td>1s</td>
</tr>
<tr>
<td><strong>fe20-release-0.4.1</strong></td>
<td></td>
<td>11s (paused for 4min 23s)</td>
<td>7s</td>
<td>8s</td>
<td>20s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mar 22</td>
<td></td>
<td>1 commits</td>
<td>7s</td>
<td>8s</td>
<td>20s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:25</td>
<td></td>
<td></td>
<td>7s</td>
<td>8s</td>
<td>20s</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Creating secure and compliant container images
Use github.com to fork/clone images sources
Use github.com to fork/clone images sources

Need all images to be RHEL based
Use github.com to fork/clone images sources

Need all images to be RHEL based

Sources not binaries! No docker hub!
Use github.com to fork/clone images sources

Need all images to be RHEL based

Sources not binaries! No docker hub!

Own proxies and repos
Before Containers

Use github.com to fork/clone images sources

World of Containers

Need all images to be RHEL based

OpenShift Infra Design

Sources not binaries! No docker hub!

OpenShift Pipeline

Own proxies and repos

Create own base images for s2i and other products

OpenShift App Devel
Use github.com to fork/clone images sources

Create own base images for s2i and other products

Need all images to be RHEL based

Sources not binaries! No docker hub!

Own proxies and repos

Internal non-public Certificate Authority
Use github.com to fork/clone images sources

Create own base images for s2i and other products

Need all images to be RHEL based

Internal non-public Certificate Authority

Sources not binaries! No docker hub!

Own proxies and repos

All exposed services protected by TLS
Use github.com to fork/clone images sources

Create own base images for s2i and other products

Need github.com to fork/clone images sources

Need all images to be RHEL based

Sources not binaries! No docker hub!

Own proxies and repos

Internal non-public Certificate Authority

All exposed services protected by TLS

Need to provide boilerplates for developers
Use github.com to fork/clone images sources

Create own base images for s2i and other products

Need all images to be RHEL based

Sources not binaries! No docker hub!

Own proxies and repos

Internal non-public Certificate Authority

Need to provide boilerplates for developers

All exposed services protected by TLS

When you need adjustment you change it in one place
FROM registry.access.redhat.com/rhel7:latest

RUN ln -sf /usr/share/zoneinfo/Europe/Warsaw /etc/localtime
RUN cd /etc/pki/ca-trust/source/anchors/ && \
    curl -Awget -O "http://pki.bzwbk.pl/pki/CA1.crt" && \
    update-ca-trust extract
[...]

Dealing with security and compliance requirements
Security controlled with code

Old

SSL
APP1
SSL
APP3
SSL
APP3

New

OpenShift Router (https)
APP1
APP1
APP1
Traffic isolation between applications
Traffic isolation

Project1

Project2
Outbound traffic

Traditional (static) firewall

Project1

Project2
Inbound traffic

Traditional (static) firewall

Project1

Project2
You can’t always get what you want

Impossible in OpenShift < 3.9
Overcoming OpenShift shortcomings
SECURITY ACROSS ALL LAYERS

- Self-Service
- Service Catalog (Language Runtimes, Middleware, Databases)
- Build Automation
- Deployment Automation
- OpenShift Application Lifecycle Management (CI/CD)
- Container Orchestration & Cluster Management (Kubernetes)
- Networking
- Storage
- Registry
- Logs & Metrics
- Security
- Infrastructure Automation & Management
- Enterprise Container Host
- Container Runtime & Packaging
- Atomic Host
- Red Hat Enterprise Linux

- CONTROL
  - Application Security
- DEFEND
  - Infrastructure
- EXTEND
AUTOMATED & INTEGRATED SECURITY

**CONTROL**
Application Security
- Container Content
- Container Registry
- CI/CD Pipeline
- Deployment Policies

**DEFEND**
Infrastructure
- Container Platform
- Container Host Multi-tenancy
- Network Isolation
- Storage
- Audit & Logging
- API Management

**EXTEND**
- Security Ecosystem

And this is what we call DevOps in a bank!
Contact us

Tomasz Cholewa, Mindbox
Lead Cloud Architect
tomasz.cholewa@mindboxgroup.com
https://mindboxgroup.com

Dawid Szymański, BZWBK
IT Architect
dawid.szymanski@bzwbk.pl
https://www.bzwbk.pl

Jarosław Stakun, Red Hat
Lead Solution Architect
jarek@redhat.com
http://www.openshift.com