DevSecOps

Ashish K Thakur

IBM

Agenda

- DevOps
- DevSecOps
- Architecture
- Continuous Integration
- Continuous Delivery
- Continuous Deployment
- Tooling

What is DevOps?

- People, process and tools
- CAMS
  - Culture
  - Automation
  - Metrics
  - Sharing

Culture

- Collaboration across roles, break silos
- Focus on business instead of departmental objectives
- Trust
- Learn, via playbacks, experimentations, usage analytics (KPIs)
- Balance quality and velocity

Squads, tribes, guilds

- Squads - group of people working together to deliver a feature or a product
    - Diversity
    - Autonomy
    - Colocation
    - Productivity
    - Transparency
    - Blameless root-cause analysis
    - Peer recognition
    - Fun
- Tribes - Set of squads
- Guilds - Example - UI guild, everything UI

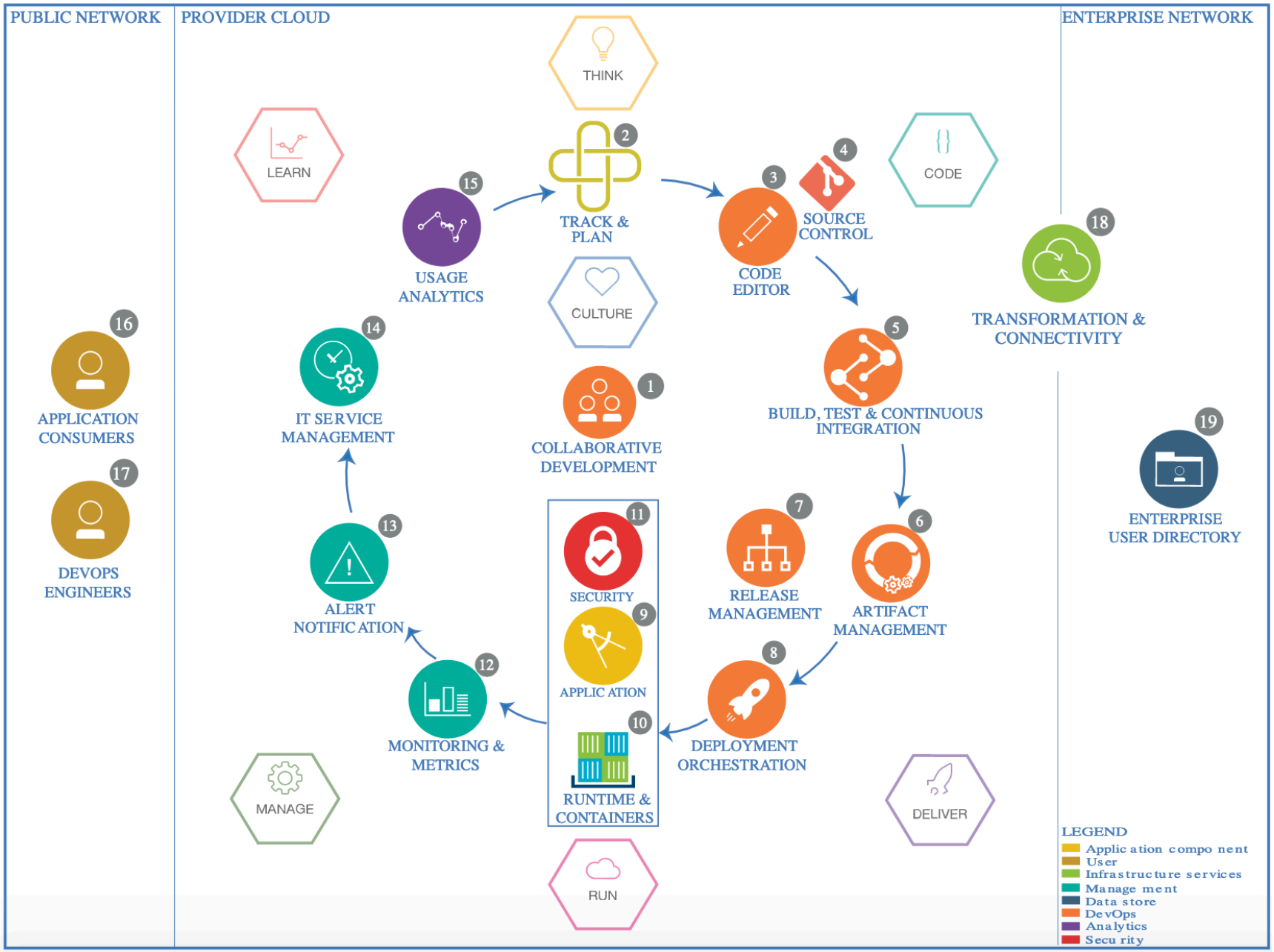
What is DevSecOps?

- Brings Developers, Security and Operations folks together - Break silos
- Shift-left - testing and security are shifted to the left through automated unit, functional, integration, and security testing
- Think about security at all phases of the software lifecycle
    - Plan
    - Develop
    - Build
    - Test
    - Release
    - Deploy
    - Operate
    - Monitor

Why?

- Improve
  - Mean time to production
  - Deployment speed
  - Production failure rate
  - Mean-time to recovery

DevOps Reference Architecture

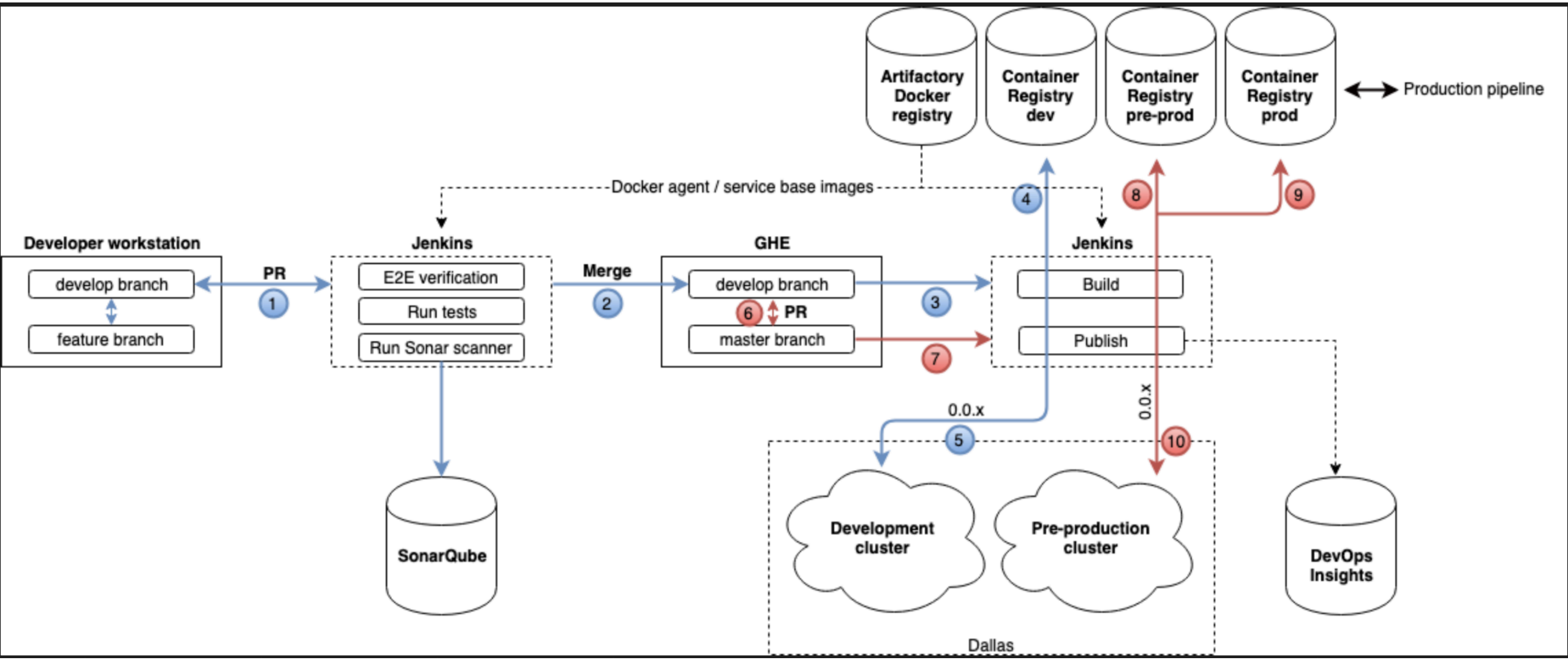


How?

- Agile
- Microservices
- Continuous integration - Continuously integrate small, manageable changes with the system
- Continuous delivery

Continuous Integration - Practice

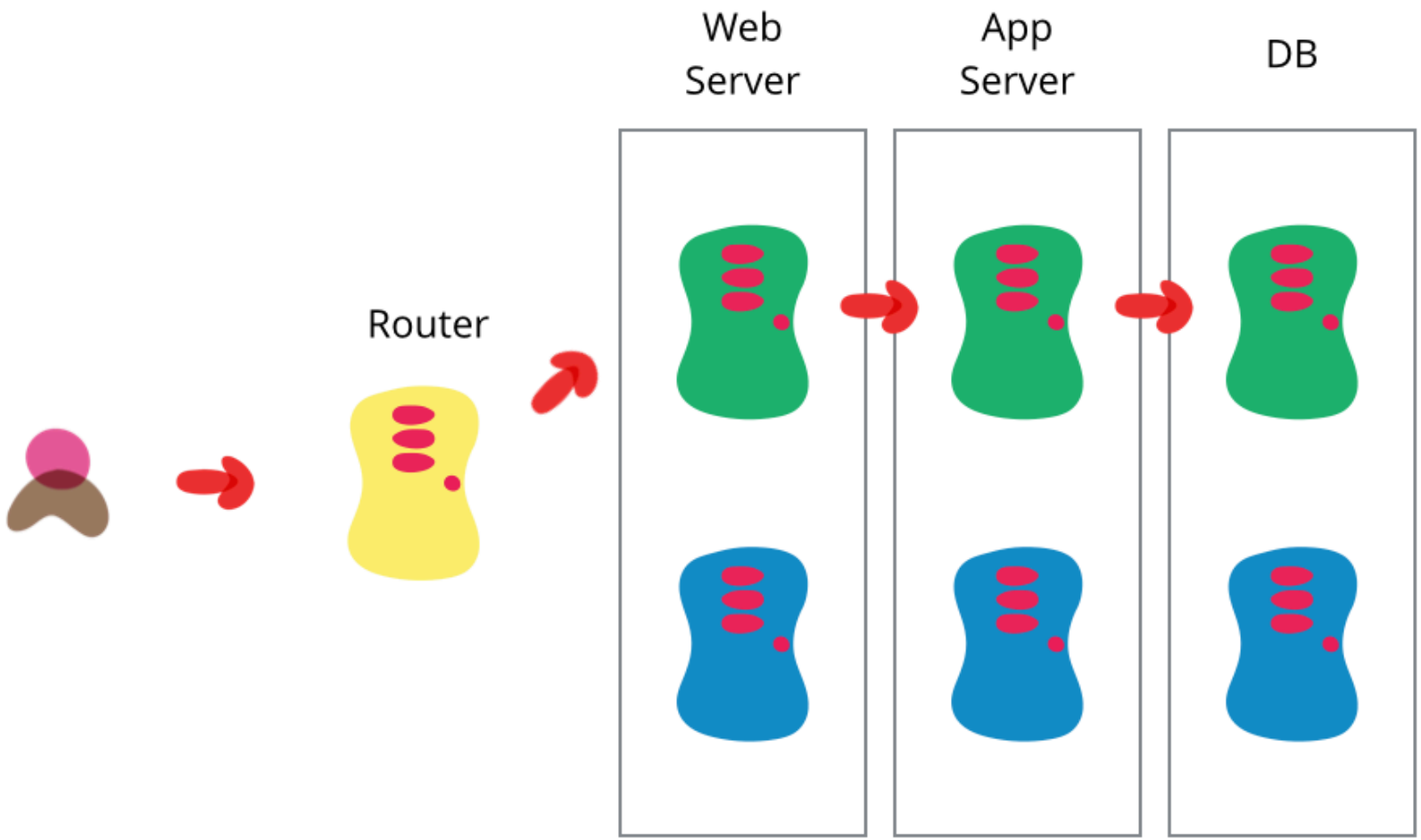
- Choose an SCM (Source code management) tool, ex -GIT
- Automate the build
- Make Your Build Self-Testing
- Everyone Commits To the Mainline Every Day
- Every Commit Should Build the Mainline on an Integration Machine
- Fix Broken Builds Immediately
- Keep the Build Fast
- Test in a Clone of the Production Environment
- Everyone can see what's happening
- Automate Deployment


Artifactory Docker registry
Container Registry dev
Container Registry pre-prod
Container Registry prod
Production pipeline
Docker agent / service base images
Developer workstation
develop branch
feature branch
PR
1
Jenkins
E2E verification
Run tests
Run Sonar scanner
Merge
2
GHE
develop branch
6
PR
master branch
3
7
Jenkins
Build
Publish
4
8
9
0.0.x
5
0.0.x
10
SonarQube
Development cluster
Pre-production cluster
Dallas
DevOps Insights

Continuous delivery

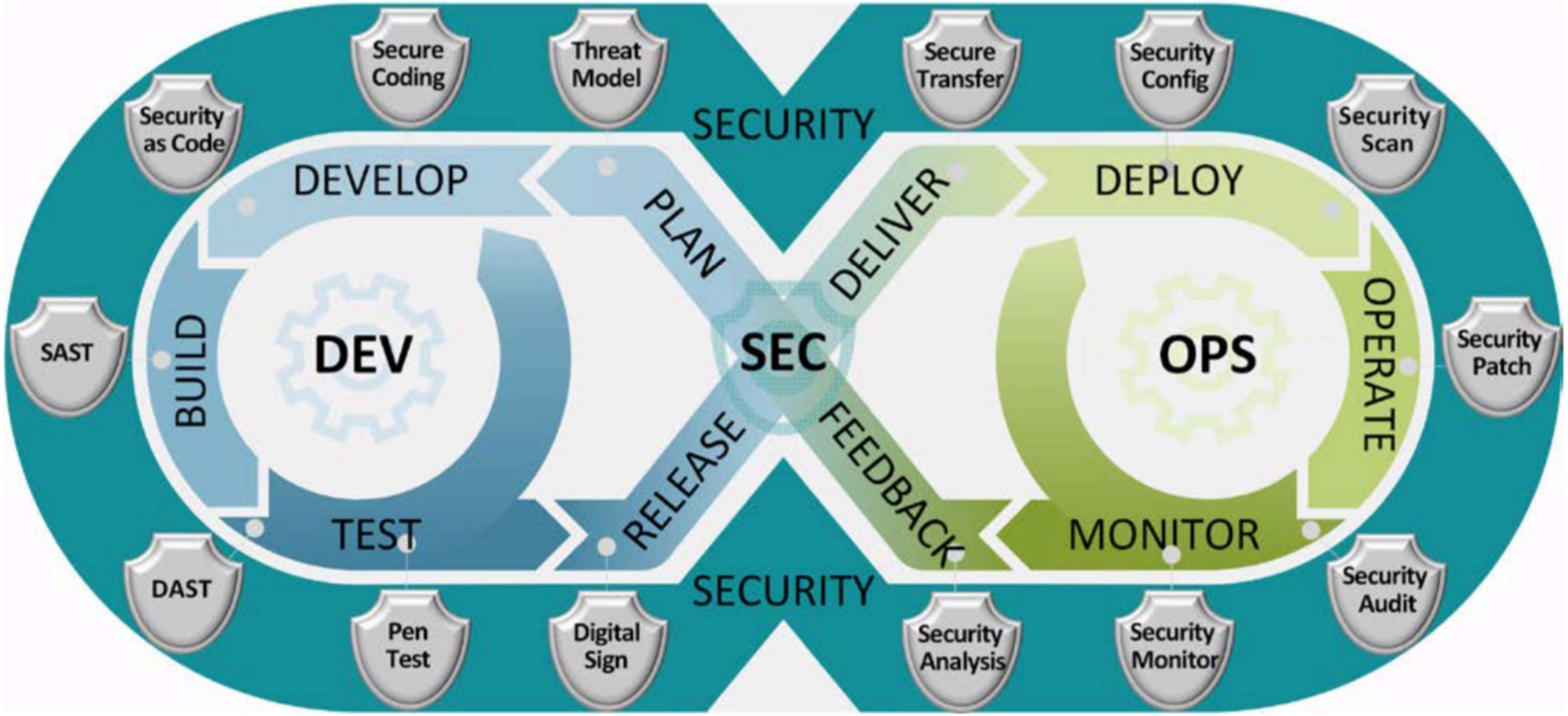
- Every change must be releasable: enables Auditing, traceability, documentation
- Code branches must be short-lived: Integrate frequently
- Deliver through an automated pipeline
- Automate almost everything: Infrastructure included
- Aim for zero downtime: K8s, Blue-Green deployments (in more details)

Blue Green Deployment



DevOps can be practiced only on Cloud?

DevOps Myths



[DoD - DevSecOps reference, Software Lifecycle]

DevSecOps - Tooling @plan/design

- Threat Modeling
    - Architecture diagrams
    - OWASP Threat Dragon

Tooling @develop

- Discipline !! Decoding JWT on websites, formatting JSONs on those sites
  - Know JWT format and decode locally using base64, alias pretty='python -m json.tool'
- Pair Programming - tmux
- IDE plugins - Sonarlint
- Linters
- IaC (Infrastructure as Code) - Terraform, Ansible
  - Codify IBM Cloud Security Groups, DNS, WAF, Clusters etc
- SaC (Security as Code)
  - Kubernetes policies - PodSecurityPolicy, NetworkPolicy
  - Calico policies - GlobalNetworkPolicy
- Code Review
  - Coding guidelines - https://github.com/golang/go/wiki/CodeReviewComments

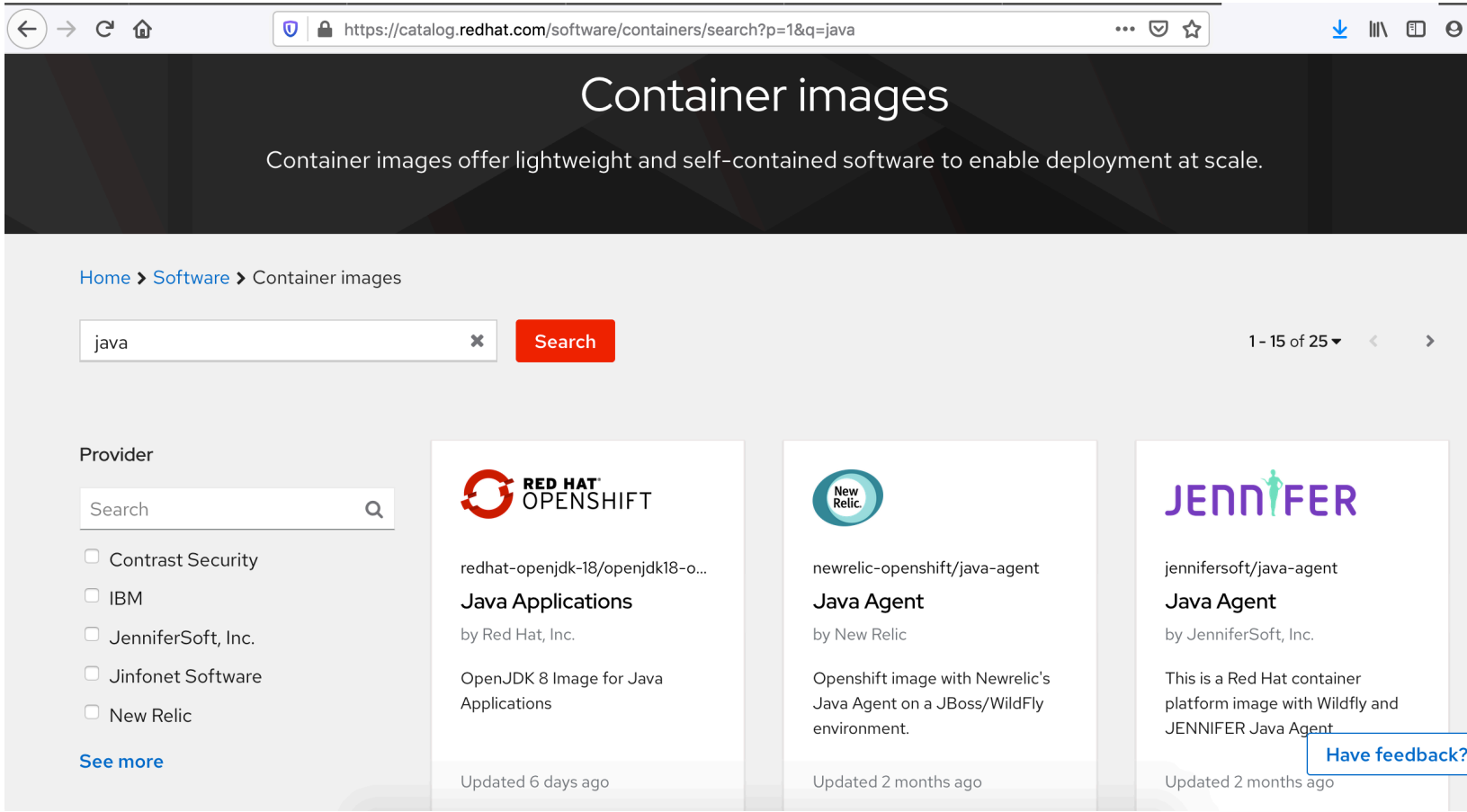
Tooling @build

- NPM Audit, Python Bandit etc
- SAST
  - SonarQube
    - Code Reliability
    - Application Security
    - Technical Debt

Tooling @test

- DAST
  - OWASP ZAP

Tooling @release



- Container images
  - Hardened
  - Versioned
  - Scanned for vulnerabilities
  - With the release of the Red Hat Universal Base Image (UBI), you can now take advantage of the greater reliability, security, and performance of official Red Hat container images where OCI-compliant Linux containers run - whether you're a customer or not.

Tooling @deploy

- Apply secrets to clusters from vault
- Deploy immutable versioned container images - consistent and predictable results

Tooling @monitor

- IBM Cloud Monitoring with Sysdig
- IBM Log Analysis with LogDNA
- IBM Cloud Security Advisor
  - Provides visuals
  - Provides notifications via webhooks

Security Advisor

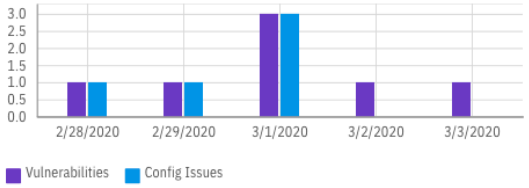
Built-in Insights

Last updated: 3/3/2020, 5:24:10 PM

Vulnerability in Images

Image with vulnerabilities	7
Image with configuration issues	5

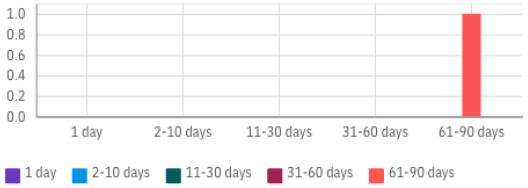
Images with vulnerabilities and config issues in the last...



Certificates

Certificates already expired	10
Certificates will expire tomorrow	0

Certificates that are about to expire in the next 90 days



Anomalies in Traffic

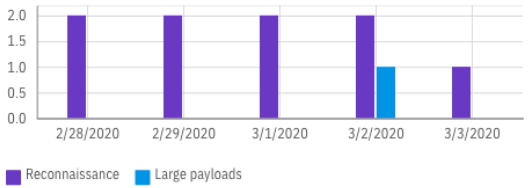
Higher than normal reconnaissance or data exchange activity	0
Outbound approach to a new server	0

No abnormal behavior detected in the last 5 days

Suspicious Inbound Traffic

Reconnaissance by suspicious clients	2
Abnormally large payloads sent by suspicious clients	1

Suspicious inbound traffic findings in the last 5 days



Suspicious Outbound Traffic

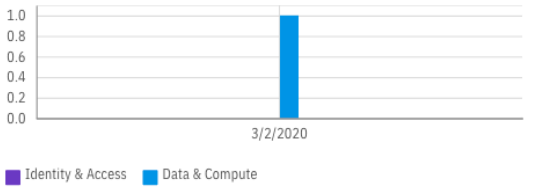
Outbound approaches to suspicious servers	0
Abnormally large payloads exchanged with suspicious servers	0

No compromised assets detected in the last 5 days

Access Analytics

Alerts on actions related to Identity and Access	0
Alerts on actions related to Data and Kubernetes	0

Activity related findings in the last 5 days



Security Advisor

Findings

IBM Vulnerability Advisor

Severity	Description	Resource
High	Image with vulnerabilities	us.icr.io [redacted] 20190826045955
High	Image with vulnerabilities	us.icr.io [redacted] 488f7e8c-20190424051919
High	Image with configuration issues	us.icr.io [redacted]
High	Image with vulnerabilities	us.icr.io [redacted]

Items per page: 10 1–4 of 4 items

Image with configuration issues

Finding number
mailicious-test-image-1.0

Severity
High

Source
IBM Vulnerability Advisor

Detection time
5/12/2020, 9:49:54 AM

Details
Image with configuration issues

Resource description

Account ID
[redacted]

Resource type
Image

Resource name
us.icr.io [redacted]

Resource ID
us.icr.io [redacted]

Resolution

Links

1. Go to Vulnerability Advisor to see what the issues are and possible corrective actions.

Tooling @operate

- Continuous vulnerability scans. Report result of scanned container images - github issue/slack alerts
- Smoke tests
- Chaos Monkey, Kube-Monkey
- Incidents RCA, Blameless postmortems

THANK YOU