Container Security

1. Build
2. Network
3. Host
4. Container Runtime
5. Orchestrator
6. Cloud
7. Data

sonarqube

Code Vulnerabilities

Secure registry & verified images

Istio

Service Mesh

HashiCorp Vault

Secure keys with access control

Prometheus

Monitoring

fluentd

Logging

App Definition and Development

Database

- TiKV – CNCF Graduated
- Vitess – CNCF Graduated
- CarbonData, Ignite, ArangoDB, BIGCHAINDB, cassandra, Cockroach Labs, Couchbase, CRATE.IO, CRUX, Dgraph, druid, FoundationDB, hazelcast, IBM DB2, iguazio, Infinispan, InterSystems, MariaDB, memSQL, SQL Server, mongoDB, MySQL, neo4j, noms, NUODB, ORACLE, OrientDB, PERCONA, pilosa, PostgreSQL, presto, Qubole, redis, RethinkDB, SCYLLA, SEATA, ShardingSphere, snowflake, software AG, STOLON, TAOS, TiDB, VERTICA, YugaByte

Streaming & Messaging

- cloudevents – CNCF Incubating
- NATS – CNCF Incubating
- Amazon Kinesis, HERON, nifi, Apache RocketMQ, Spark, Apache Storm, Azure Event Hubs, beam, deepstream, EMQ, Flink, Google Cloud Dataflow, hazelcast jet, kafka, KubeMQ, Lightbend, OpenMessaging, Pachyderm, Pravega, PULSAR, RabbitMQ, Siddhi, StreamSets, STRIMZI, talend

Application Definition & Image Build

- HELM – CNCF Graduated
- OPERATOR FRAMEWORK – CNCF Incubating
- Artifact HUB, Backstage, bitnami, Buildpacks.io, CAPE, CHEF HABITAT, DeployHub, DevSpace, Kaniko, kots, KubeVirt, KUDO, Kui, lagoon, Platform, OCTANT, okteto, On-Prem, Open Application Model, OPENAPI INITIATIVE, Packer, podman, Serverless Workflow, ServiceComb, SKAFFOLD, squash, Tanka, TILT

Continuous Integration & Delivery

- argo – CNCF Incubating
- agola, AppVeyor, AWS CodePipeline, Azure Pipelines, Bamboo, BRIGADE, Buildkite, circleci, Skycap, CloudBees, codefresh, Concourse, D2IQ Dispatch, Drone, flux, GitHub Actions, GitLab, go, Google Cloud Build, harness, hyscale, Jenkins, JENKINS X, keptn, Octopus Deploy, Razee, Screwdriver, semaphore, Spinnaker, TeamCity, TEKTON, Travis CI, weave flagger, werf, DEPLOY

Orchestration & Management

Scheduling & Orchestration

- kubernetes – CNCF Graduated
- Amazon ECS, MESOS, Azure Service Fabric, Crossplane, SWARM, Nomad, VOLCANO

Coordination & Service Discovery

- CoreDNS – CNCF Graduated
- etcd – CNCF Incubating
- ZooKeeper, NACOS, NETFLIX OSS Eureka

Remote Procedure Call

- gRPC – CNCF Incubating
- Apache Thrift, AVRO, DUBBO, SOFARPC, TARS

Service Proxy

- envoy – CNCF Graduated
- CONTOUR – CNCF Incubating
- AVI Networks, BFE, CITRIX, f5, GIMBAL, HAPROXY, inlets, MetalLB, MOSN, NGINX, OpenResty, Porter, Skipper, NOVA, Tengine, traefik

API Gateway

- 3SCALE, Ambassador, APIOAK, APISIX, Gloo, GRAVITEE.IO, Kong, KrakenD, MuleSoft, Sentinel, Tyk, WSO2 API Microgateway

Service Mesh

- LINKERD – CNCF Incubating
- Consul, Grey Matter, Istio, Kuma, maesh, MESHERY, NETFLIX OSS Zuul, Open Service Mesh, Service Mesh Interface, SuperGloo

Runtime

Cloud Native Storage

- ROOK – CNCF Incubating
- ALLUXIO, Arrikto, Azure Disk Storage, ceph, ChubaoFS, CSI, DATERA, DELL EMC, DIAMANTI, DriveScale, GLUSTER, Google Persistent Disk, Hedvig, HITACHI, Hewlett Packard Enterprise, HUAWEI, IBM, INFINIDAT, kasten, LONGHORN, MayaData, MINIO, MooseFS, NetApp, NUTANIX, OpenEBS, OpenIO, portworx, PURE STORAGE, Qumulo, Quobyte, reduxio, ROBIN, SANDSTONE, RING, soda foundation, STORAGEOS, StorPool, SWIFT, TRILIO, TRITON Object Storage, VELERO, XSKY, YRCloudFile, ZENKO

Container Runtime

- containerd – CNCF Graduated
- cri-o – CNCF Incubating
- Firecracker, gVisor, kata, lxd, Singularity, SmartOS

Cloud Native Network

- CNI – CNCF Incubating
- ANTREA, aviatrix, cilium, CNI-Genie, Contiv, CUMULUS, DANM, fd.io, flannel, Guardicore, Kube-OVN, KUBE-ROUTER, LIGATO, MULTUS, Network Service Mesh, nuagenetworks, Open vSwitch, CALICO, tungstenfabric, vmware NSX, weave net

Provisioning

Automation & Configuration

- airship, ANSIBLE, Apollo, AWS CloudFormation, BOSH, Cadence, CFEngine, CHEF INFRA, Cloud Custodian, CLOUDIFY, FOREMAN, JUJU, kiosk, KubeEdge, LinuxKit, MAAS, ManageIQ, openstack, pulumi, puppet, RUNDECK, SALTSTACK, StackStorm, Terraform, vmware vSphere

Container Registry

- HARBOR – CNCF Graduated
- Dragonfly – CNCF Incubating
- Amazon ECR, Azure Registry, Docker Registry, Google Container Registry, IBM Cloud Container Registry, JFrog Artifactory, Kraken, Portus, QUAY

Security & Compliance

- TUF – CNCF Graduated
- falco – CNCF Incubating
- Notary – CNCF Incubating
- Open Policy Agent – CNCF Incubating
- alcide, anchore, aqua, BLACKDUCK, BLOOMBASE, CAPSULE8, Check Point, CHEF INSPEC, clair, CYBERARMOR, Datica, dex, FOSSA, FOSSID, Grafeas, in-toto, kube-bench, kube-hunter, NeuVector, OpenSCAP, PARSEC, portshift, paloalto, snyk, Sonatype Nexus, SONOBUOY, StackRox, sysdig secure, terrascan, TIGERA, TREND MICRO, trivy, WhiteSource, Zettaset

Key Management

- spiffe – CNCF Incubating
- SPIRE – CNCF Incubating
- Athenz, CYBERARK CONJUR, KEYCLOAK, OAuth2 Proxy, ORY / Hydra, POMERIUM, Square Keywhiz, Teleport, Vault

Platform

Certified Kubernetes - Distribution

- Agile Stacks, CANONICAL, caicloud, CloudBees, cisco, D2IQ, DaoCloud, DIAMANTI, docker, EasyStack, elastisys, ERICSSON, Flexkube, FURY, Giant Swarm, Gravity, H3C, HPE, HyperCloud, IBM Cloud, JD.COM, Joyent, K8S, K8sPlus, kubedee, Kubic, kublr, LOKOMOTIVE, D2IQ, METALK8S, MicroK8s, MIRANTIS, MORPHEUS, NetApp, NOKIA, ORACLE, PLATFORM9, RANCHER, OPENSHIFT, ROBIN, ROOST, spectro cloud, SUSE, SYMPLEGMA, TEAMSUN, Typhoon, VMware Tanzu, weaveworks, WIND RIVER CLOUD PLATFORM

Certified Kubernetes - Hosted

- Microsoft Azure, Alibaba Cloud, aws, BAIDU AI CLOUD, catalyst cloud, Maestro, DigitalOcean, eBaoCloud, ELASTX, Google Kubernetes Engine, HUAWEI, INNOVO CLOUD, inspur, JD Cloud & AI, JD.COM, Kingsoft Cloud, Linaro, linode, nirmata, NUTANIX, ORACLE, OVHcloud, QINGCLOUD, RAFAY, Red Hat OpenShift Dedicated, Red Hat OpenShift on IBM Cloud, SAMSUNG SDS, SAP, Scaleway, SERVERSTACK, STARLINGX, SysEleven, Tencent Cloud, UCLOUD, aventus ag, ZTE

Certified Kubernetes - Installer

- CableLabs, cybozu, Gardener, Google Cloud, kops, kubeadm, KubeOperator, KubeOne, KUBESPRAY, MAGNUM, Meeondog, puppet, RANCHER, TALOS

PaaS/Container Service

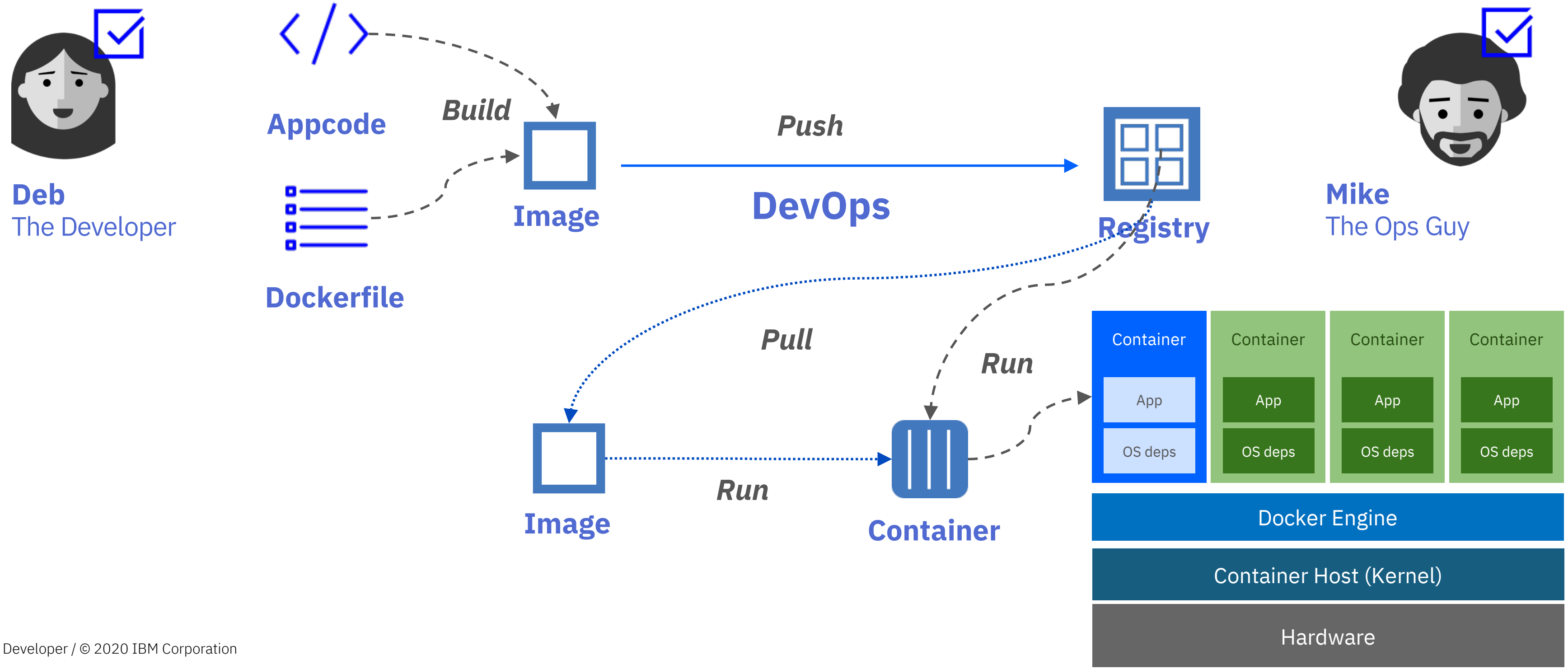
- akka, ATOMIST, APPLICATION RUNTIME, Flynn, heroku, JHipster, No Code, PaaSta, platform.sh, portainer.io, RIO, Scalingo, Tsuru, YELLOWDOG

IBM Developer / © 2020 IBM Corporation

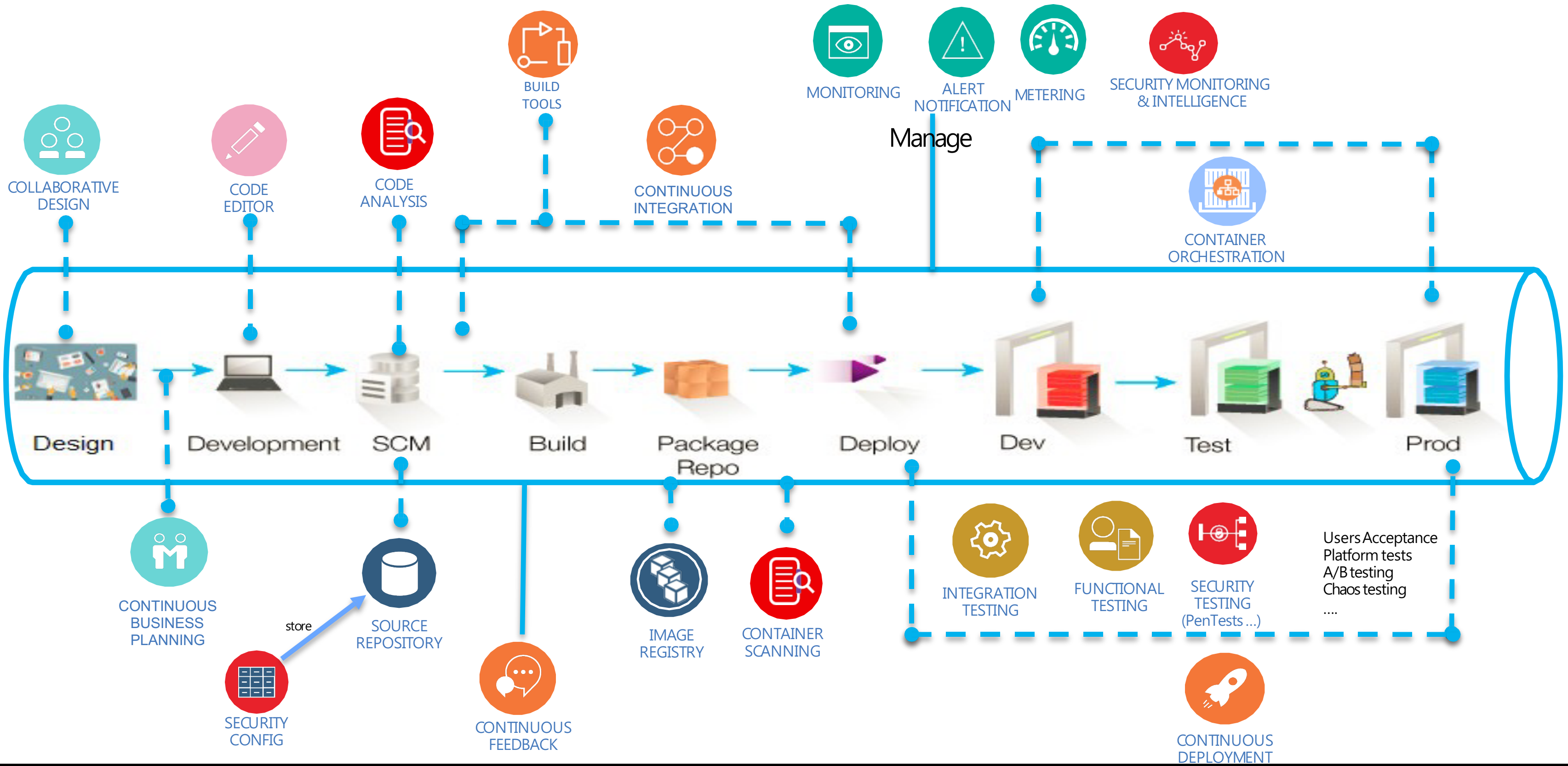
Kubernetes Certified Service Provider

Kubernetes Training Partner

Basic deployment process

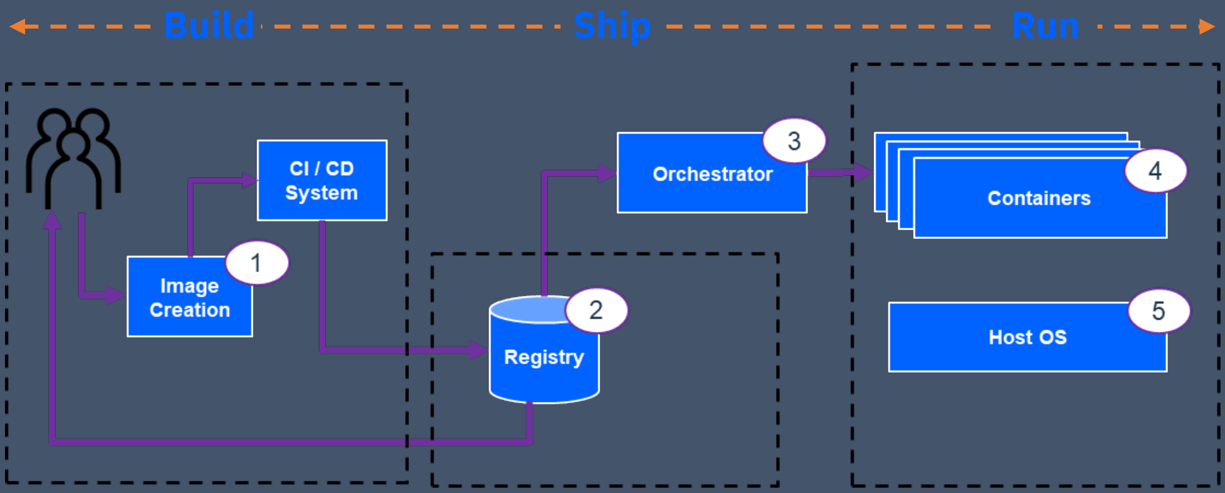


DevSecOps: integrate security into your DevOps process



Five major risk areas of container environment

- Image
- Registry
- Orchestration
- Containers
- Host OS



Build

Ship

Run

CI / CD System

Image Creation

1

Registry

2

Orchestrator

3

Containers

4

Host OS

5

Image creation, testing and accreditation

Image storage and retrieval

Container deployment and management

Container Security

Container security includes securing the containers, the containerized application stack, the container pipeline (build-ship-run) and the infrastructure containers rely on, and integrate with security tools and security policies.

10 Key elements of container security:

1. **Multitenant host**: deploying multiple apps on single shared host: secure host kernel from containers and containers from each other. Drop privileges to least privilege possible; run as user not root; use Linux namespaces, SELinux (enforce mandatory access controls (MAC) for every user, application, process, and file), Cgroups, capabilities (lock down root in a container), and seccomp profiles to restrict available system calls; use lightweight operating system and optimized host;
2. **Container content**: trusted base images, e.g. Universal Base Images (UBI); container security monitoring and security scanning like OpenSCAP;
3. **Container registries**,
4. **Building containers**: Source-to-Image (S2I); integrated Jenkins; integration RESTful APIs; SAST, DAST; vulnerability scanning; separate container layers;
5. **Deployment**: automated, policy-based deployment; Security Context Constraints (SCC) as Pod Security Policy and Container Security Policy.
6. **Container orchestration**: capacity; shared resources management like network and storage; container health, e.g. CloudForms; scaling; integrated OAuth server; multitenancy security;
7. **Network isolation**: network namespaces; pod-network, software defined network (SDN) and SDN plugins (ovs-subnet, ovs-multitenant, ovs-networkpolicy); SDN solutions like Calico; Network Policy;
8. **Storage**: PV with access modes; use annotations on PVs to add group IDs (gid); use SELinux to secure mounted volume; encrypt data-in-transit;
9. **API management for Microservices**: 3Scale, API Connect, Loopback, OpenAPIs;
10. **Federated clusters**: including federated secrets, federated namespaces and Ingress objects.

Source: https://www.redhat.com/cms/managed-files/cl-container-security-openshift-cloud-devops-tech-detail-f7530kc-201705-en.pdf