Practical End to End Container Security @ Scale

- Yashvier Kosaraju

Twilio

Who Am I?

- Product Security @ Twilio
- ~6 years in Security
- Amateur Photographer
- Love Hiking
- Scared of heights

linkedin.com/in/yashvier/ 

@yashvi3r 

Agenda

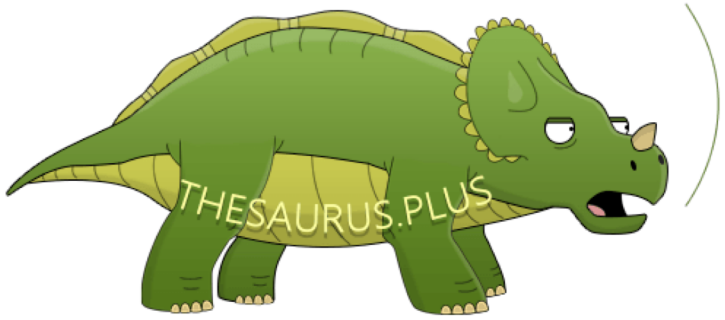
- Introduction
- Why?
- What does Practical Security Mean?
- Why traditional approaches do not work?
- Container Pipeline
- Securing Container Pipeline
- Issues at Scale
- Helpful Resources

Why?

What does practical end to end container security mean?

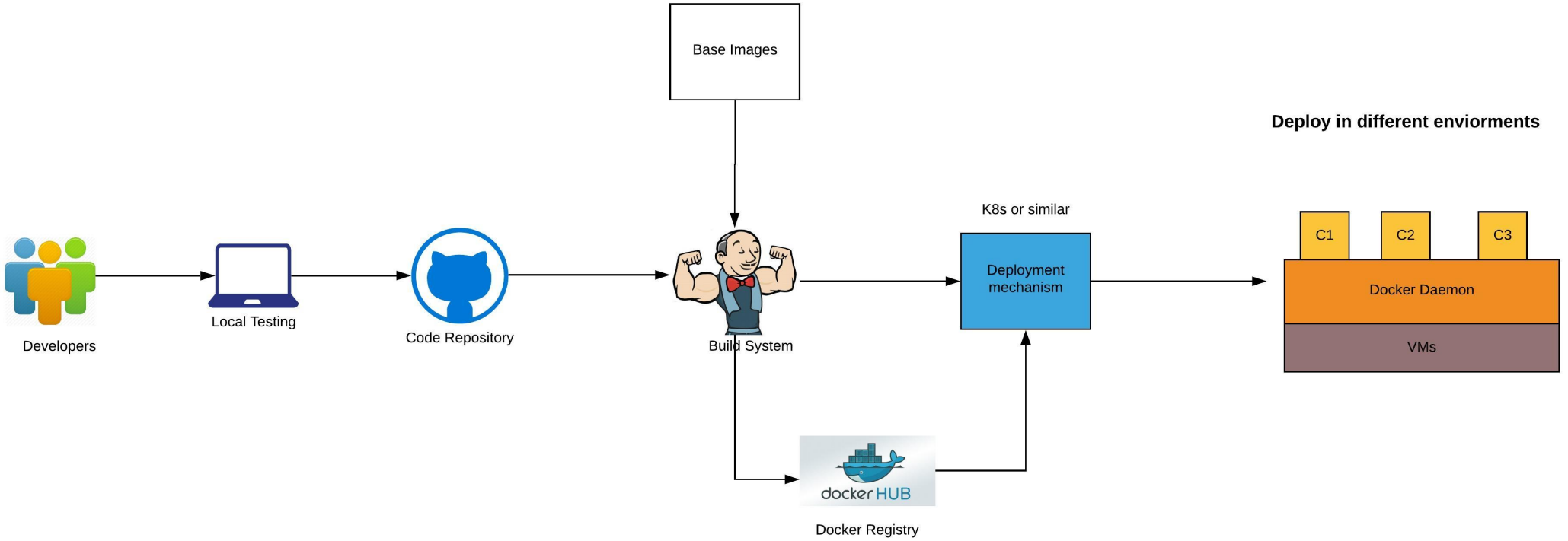
- Enable Developers to move fast
- Achievable
- Maintainable
- Scalable
- Automatable
- Tangible Results

antonyms for practical:
impractical, unrealistic, useless, unworkable,
theoretical, impossible, unattainable, irrational,
inefficient, unreasonable

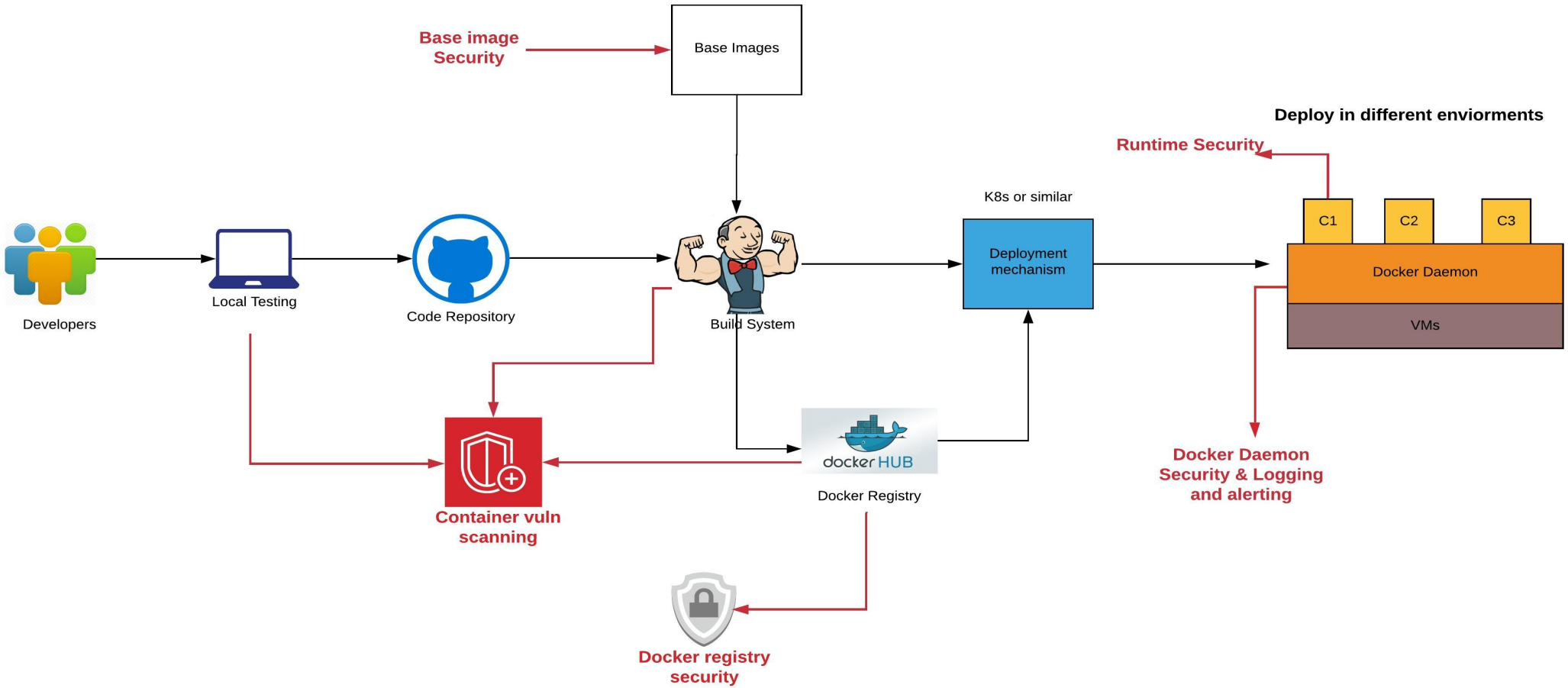


Why traditional approaches do not work?

Deployment process in a container world



Adding security…



Base Image Security

Malicious Docker Containers Earn Cryptomining Criminals $90K

17 Backdoored Docker Images Removed From Docker Hub

By Catalin Cimpanu June 13, 2018 02:40 PM 0

The Docker team has pulled 17 Docker container images that have been backdoored and used to install reverse shells and cryptocurrency miners on users' servers for the past year.

Top ten most popular docker images each contain at least 30 vulnerabilities

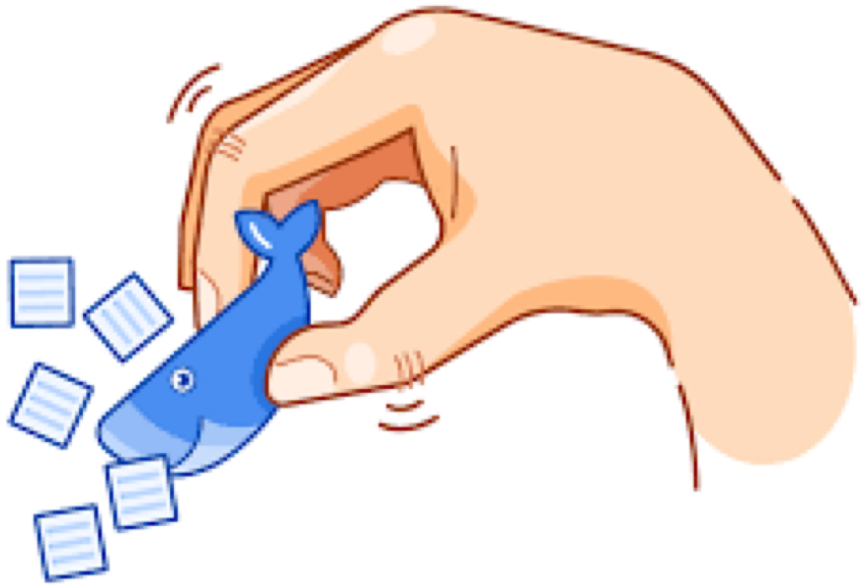
FEBRUARY 26, 2019 | IN ECOSYSTEMS, OPEN SOURCE | BY LIRAN TAL

Base Image Security

- Whitelist small set of trusted Images

Base Image Security

- Whitelist small set of trusted Images
- Keep your base images small
  (distroless images anyone?)



Base Image Security

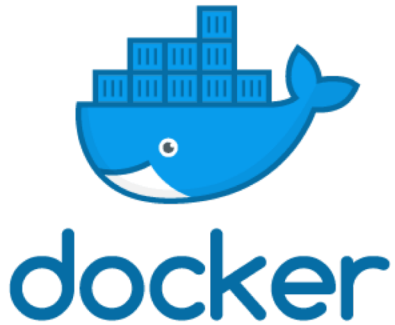
- Whitelist small set of trusted Images
- Keep your base images small (distroless images anyone?)
- Regularly patch base images

Base Image Security

- Whitelist small set of trusted Images
- Keep your base images small (distroless images anyone?)
- Regularly patch base images
- Update all Dockerfiles to use the new base image
  - Latest vs latest_tag

Container Registry Security

Google Cloud Platform



Container Registry Security

Container Registry Security

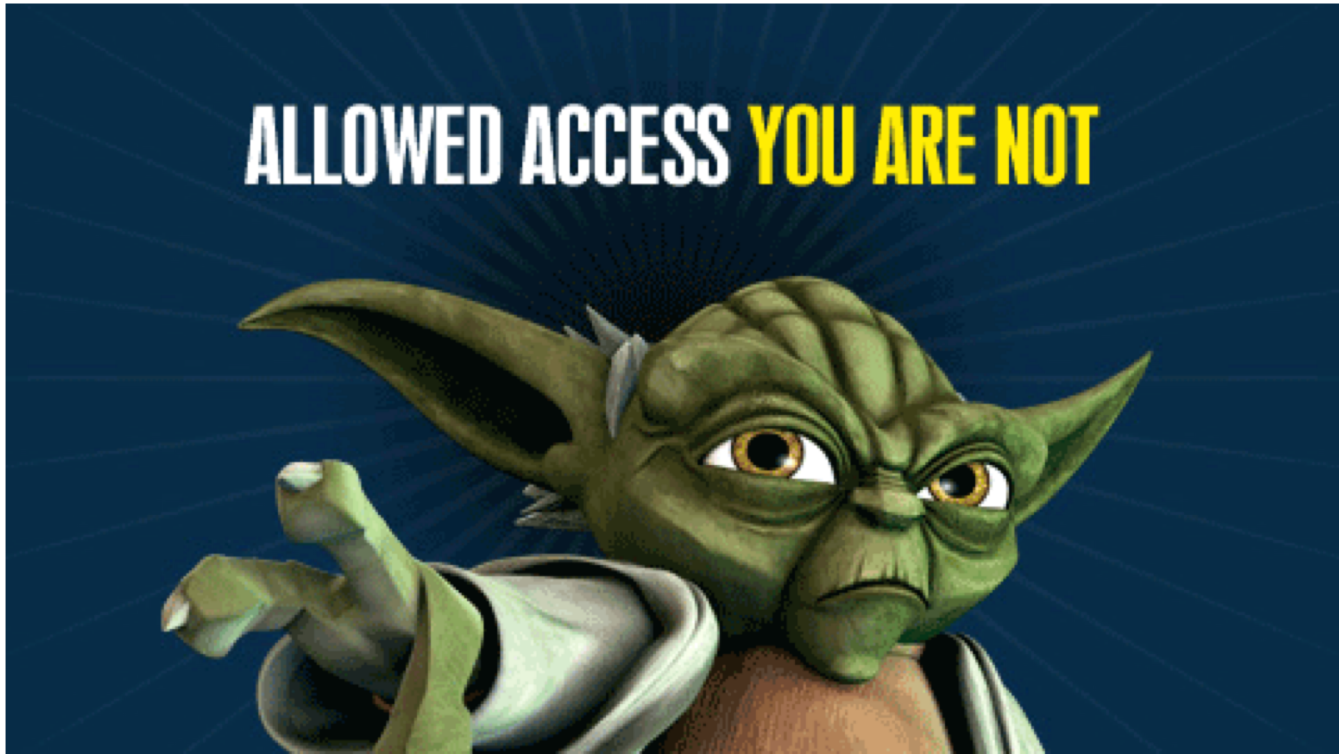
- Securing your container registry

Container Registry Security

- Securing your container registry
  - Use a private registry

Container Registry Security

- Securing your container registry
  - Use a private registry
  - Role Based Access Control



Container Registry Security

- Securing your container registry
  - Use a private registry
  - Role Based Access Control
  - Use a V2 docker registry

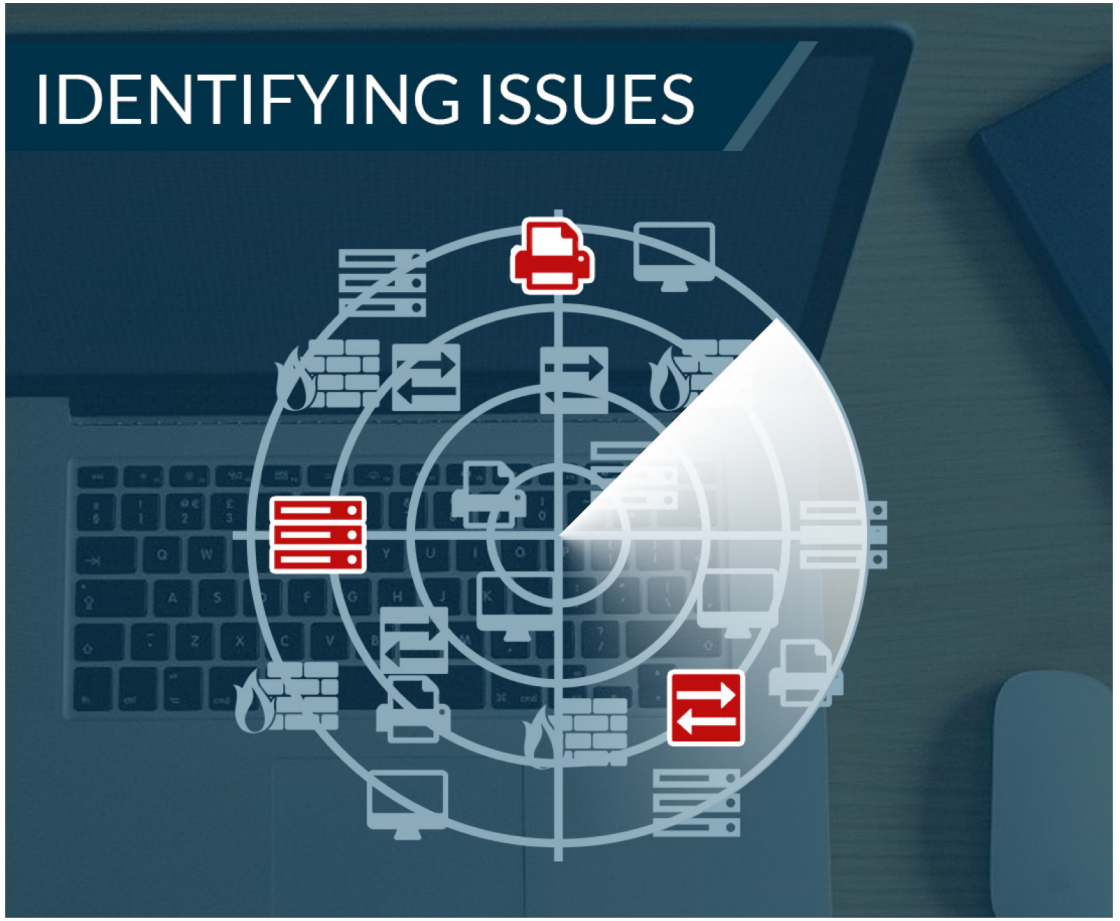
Container Registry Security

- Securing your container registry
  - Use a private registry
  - Role Based Access Control
  - Use a V2 docker registry
  - Use a secure registry

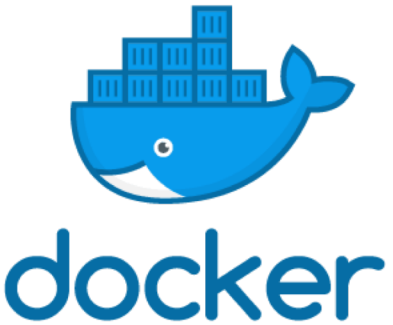
Container Registry Security

- Securing your container registry
  - Use a private registry
  - Role Based Access Control
  - Use a V2 docker registry
  - Use a secure registry
  - Docker Content Trust (DCT)

Vulnerability Scanning



Vulnerability Scanning



Vulnerability Scanning

- Strategies for using vuln scanning in containers

Vulnerability Scanning

- Strategies for using vuln scanning in containers:
  - Add them to your build process

Vulnerability Scanning

- Strategies for using vuln scanning in containers:
  - Add them to your build process
    - Have the option of breaking builds when high/critical issues are found

Vulnerability Scanning

- Strategies for using vuln scanning in containers:
  - Add them to your build process
    - Have the option of breaking builds when high/critical issues are found
    - Scan results shown in the build system

Vulnerability Scanning

- Strategies for using vuln scanning in containers:
  - Add them to your build process
    - Have the option of breaking builds when high/critical issues are found
    - Scan results shown in the build system
  - Enable scanning in your docker registry

Amazon ECR

Vulnerability Scanning

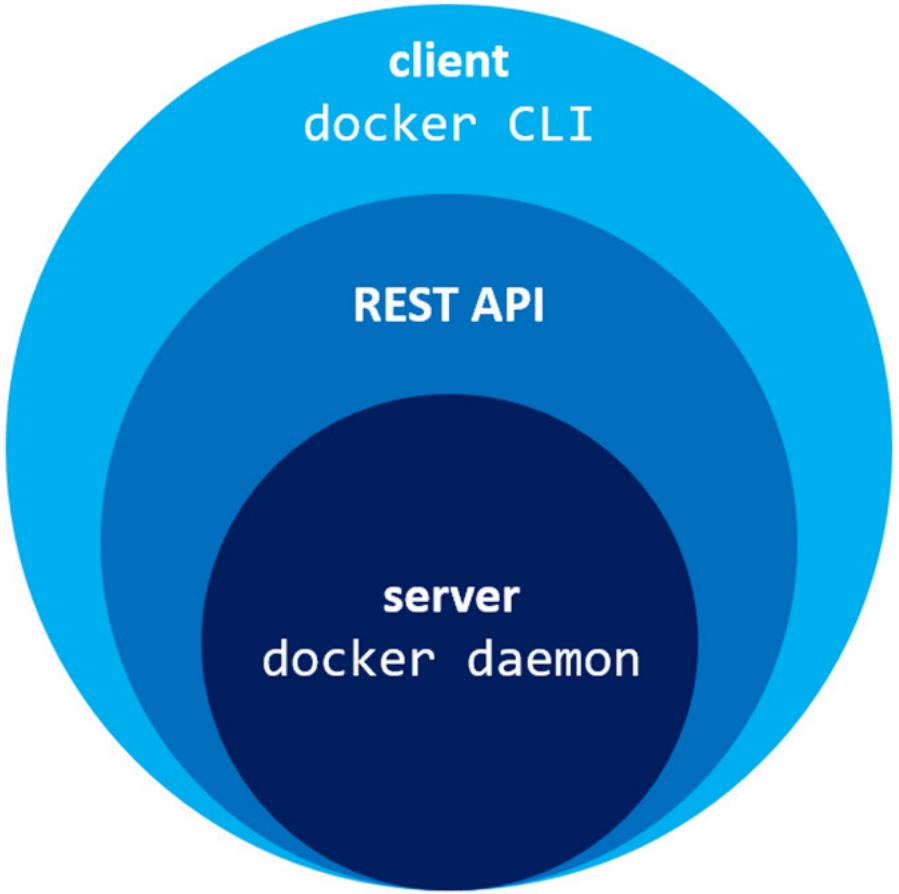
- Strategies for using vuln scanning in containers:
  - Add them to your build process
    - Have the option of breaking builds when high/critical issues are found
    - Scan results shown in the build system
  - Enable scanning in your docker registry
  - Self Service – pre build

Vulnerability Scanning

- Selecting a scanner?
  - Vulnerability sources
  - Deployment model
  - Scan times
  - Feature-set
  - $$$
  - Do an actual POC

Docker Daemon Security

- What is the Docker Daemon ?



Docker Daemon Security

Security related options in the Daemon Config

- Restrict Inter Container Communication (ICC)
- Set appropriate logging level
- Do not enable insecure registries
- Enable auth for Docker Daemon
- Set ulimits
- Enable user namespaces
- Enable cgroups
- Disable legacy registries
- Enable live restore
- Disable experimental features
- Restrict containers from acquiring new privileges
- Enable seccomp profiles

Docker Runtime Security

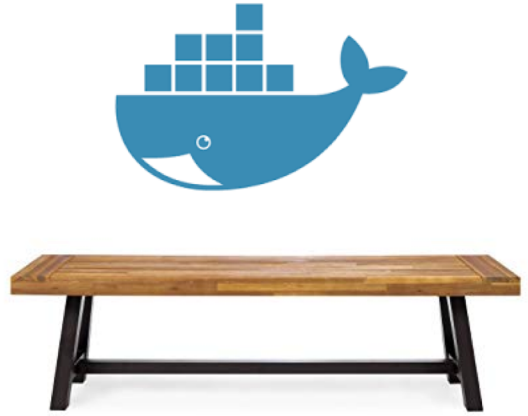
- Enable App Armor profiles
  - https://github.com/genuinetools/bane

- Configure SELinux

- Do not run privileged containers
- Run containers as read-only

Docker CIS Benchmark

- CIS Benchmark:
  - https://www.cisecurity.org/benchmark/docker/
- Auditing Docker configurations using Docker-bench
  https://github.com/docker/docker-bench-security
  - Evaluates various settings with CIS standards
  - Checks for dozens of common best-practices



```
# ------------------------------------------------------------------------------
# Docker Bench for Security v1.3.3
#
# Docker, Inc. (c) 2015-
#
# Checks for dozens of common best-practices around deploying Docker containers in production.
# Inspired by the CIS Docker Community Edition Benchmark v1.1.0.
# ------------------------------------------------------------------------------

Initializing Fri Jul 14 09:18:42 UTC 2017


[INFO] 1 - Host Configuration
[WARN] 1.1  - Ensure a separate partition for containers has been created
[NOTE] 1.2  - Ensure the container host has been Hardened
[PASS] 1.3  - Ensure Docker is up to date
[INFO]      * Using 17.06.0 which is current
[INFO]      * Check with your operating system vendor for support and security maintenance for Docker
[INFO] 1.4  - Ensure only trusted users are allowed to control Docker daemon
[INFO]      * docker:x:992:vagrant
[WARN] 1.5  - Ensure auditing is configured for the Docker daemon
[WARN] 1.6  - Ensure auditing is configured for Docker files and directories - /var/lib/docker
[WARN] 1.7  - Ensure auditing is configured for Docker files and directories - /etc/docker
[WARN] 1.8  - Ensure auditing is configured for Docker files and directories - docker.service
[INFO] 1.9  - Ensure auditing is configured for Docker files and directories - docker.socket
[INFO]      * File not found
[INFO] 1.10 - Ensure auditing is configured for Docker files and directories - /etc/default/docker
[INFO]      * File not found
[INFO] 1.11 - Ensure auditing is configured for Docker files and directories - /etc/docker/daemon.json
[INFO]      * File not found
[WARN] 1.12 - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-containerd
[WARN] 1.13 - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-runc


[INFO] 2 - Docker daemon configuration
[WARN] 2.1  - Ensure network traffic is restricted between containers on the default bridge
[PASS] 2.2  - Ensure the logging level is set to 'info'
[PASS] 2.3  - Ensure Docker is allowed to make changes to iptables
[PASS] 2.4  - Ensure insecure registries are not used
```

Kubernetest CIS Benchmark

- CIS Benchmark
  - https://www.cisecurity.org/benchmark/kubernetes/
- Kube Bench
  - https://github.com/aquasecurity/kube-bench

Logging & Alerting

- Docker supports various log drivers

- Interesting alerts:
  - Alert if a shell is spawned in a running container
  - Alert if a certain file is copied from a running container
  - Etc

Realtime Alerting in Containers

- Enterprise Solutions
  - Twistlock,Aqua,Sysdig secure

- OpenSource Solutions
  - Sysdig Falco

@Scale

- Potential issues while scaling
  - Extra load on your container registry
  - Scans will increase build time
  - Vulns with no patches available
  - Deleting old tags
  - Scanner DB scaling
    - Build tests adding to scans
    - Individual user builds

Some Resources

- CIS benchmarks
- List of Docker Security Resources
  - https://github.com/veggiemonk/awesome-docker
- Kube-hunter
  - https://github.com/aquasecurity/kube-hunter
- NCC container security whitepaper
  - https://www.nccgroup.trust/us/our-research/understanding-and-hardening-linux-containers/
- GDS docker guidelines
  - https://github.com/GDSSecurity/Docker-Secure-Deployment-Guidelines
- Dockerfile best practices
  - https://docs.docker.com/develop/develop-images/dockerfile_best-practices/

THANK YOU FOR LISTENING!

ANY QUESTIONS?