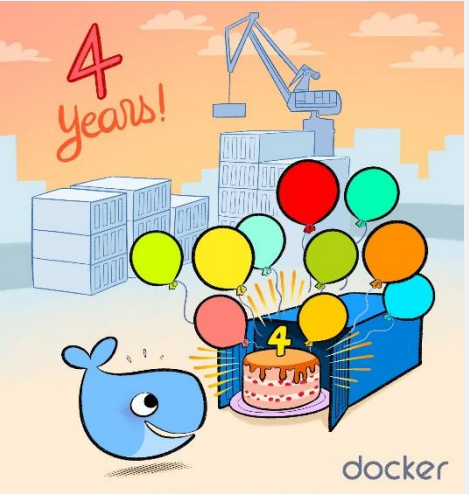


VOS DONNÉES
SONT CE QUE VOUS AVEZ
DE PLUS PRECIEUX

UNE SÉCURITÉ D'AVANCE

SECLUD

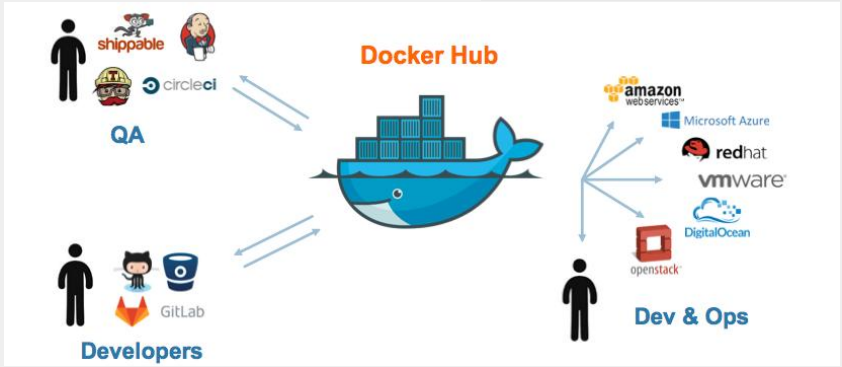
Sécurité Docker

Frédéric DONNAT – Directeur Technique et Co-Fondateur
fred@secludit.com
Téléphone 06 59 98 30 77

Agenda

1. Socle Docker
   - ✓ Infrastructure, Serveur Hôte (OS)
   - ✓ Docker Secure Deployment Guideline
   - ✓ CIS Benchmark : Docker bench Security

2. Image Docker
   - ✓ Registry : Docker Hub
   - ✓ Sécurité propres image docker
   - ✓ Scan : Docker Scanning Services, TwistLock trust, Clair



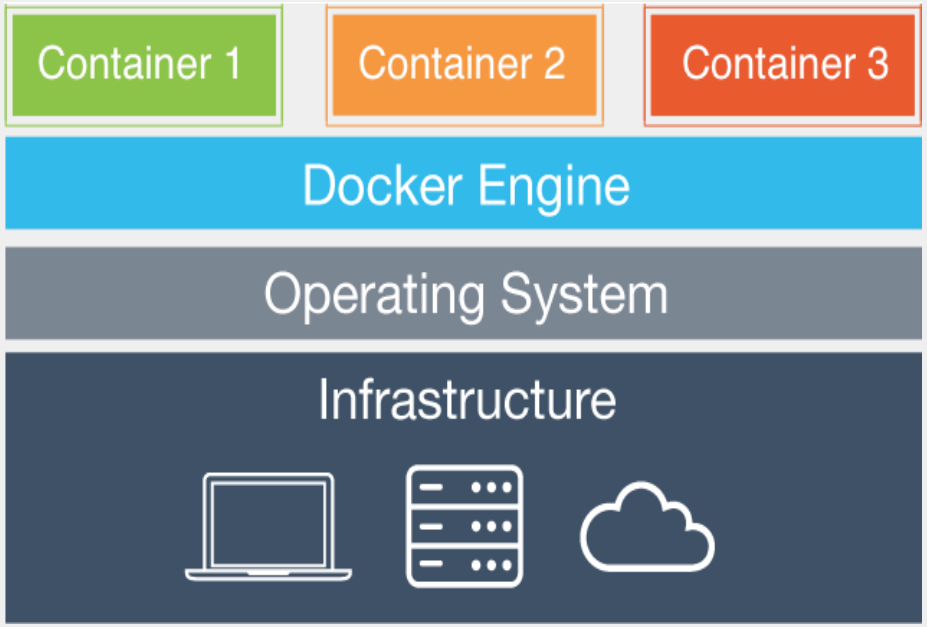
3. Ecosystème Docker : Non abordé ici
   - ✓ Kubernetes, Mesos, Swarm, etc…

SECLUDIT

Socle Docker

1. Contraintes
   - ✓ Infrastructure, Server host (OS)
   - ✓ Docker est un « root » daemon
   - ✓ Docker « daemon » socket

2. Sécurité
   - ✓ Bonnes pratiques : Docker Secure Deployment Guidelines
     - ✓ Sécurité du noyau : AppArmor, GRSEC, …
     - ✓ Isolation réseau
     - ✓ Authentification et Autorisation
     - ✓ Canal sécurisé
     - ✓ Traçabilité : Logs, Audit
   - ✓ CIS Benchmark : Docker bench Security



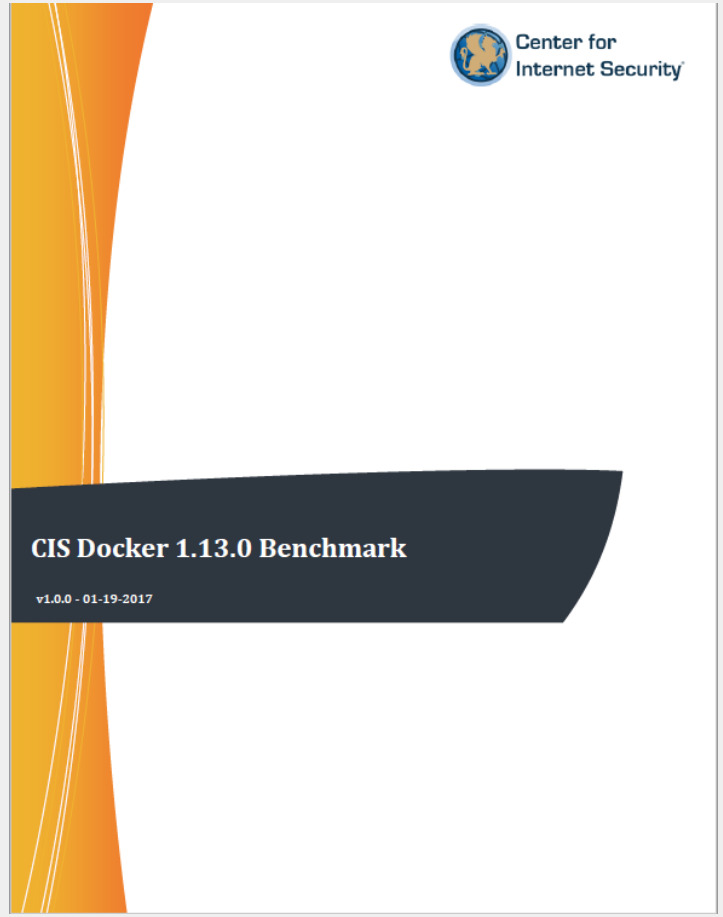
SECLUDIT

Center for Internet Security®

Docker CIS Benchmark

- 6 Chapitres
  - ✓ Configuration du serveur hôte
  - ✓ Configuration du « daemon » docker
  - ✓ Fichiers de configuration du daemon » docker
  - ✓ Image de « container » et fichier de « build »
  - ✓ Exécution de « container »
  - ✓ Opérations de sécurité pour Docker

- 104 Règles
  - ✓ 1.1 Partition dédiée pour les « containers »
  - ✓ 2.1 Restriction du traffique entre « containers »
  - ✓ 6.1 Faire des audits régulières du système hôte et des « containers »



SECLUDIT

Exemple : Docker CIS Benchmark

Description

5.4 Do not use privileged containers (Scored)

Profile Applicability:

- Level 1 - Docker

Description:

Using the `--privileged` flag gives all Linux Kernel Capabilities to the container thus overwriting the `--cap-add` and `--cap-drop` flags. Ensure that it is not used.

Rationale:

The `--privileged` flag gives all capabilities to the container, and it also lifts all the limitations enforced by the device cgroup controller. In other words, the container can then do almost everything that the host can do. This flag exists to allow special use-cases, like running Docker within Docker.

Impact:

Linux Kernel Capabilities other than defaults would not be available for use within container.

Test

Audit:

```
docker ps --quiet --all | xargs docker inspect --format '{{ .Id }}: Privileged={{
.HostConfig.Privileged }}'
```

The above command should return `Privileged=false` for each container instance.

Solution

Remediation:

Do not run container with the `--privileged` flag.

For example, do not start a container as below:

```
docker run --interactive --tty --privileged centos /bin/bash
```

Image Docker

1. Contraintes
   - ✓ Docker Hub / Docker Image
   - ✓ Partage d'Image
   - ✓ Attaque sur le server Hôte via le container :
     - ✓ DoS
     - ✓ Elévation de privilèges
     - ✓ Partage de ressources et données

2. Sécurité
   - ✓ Principe de « moindre privilège »
     - ✓ Accès, Autorisation, Ressources
   - ✓ Nettoyage : Logs, Clés, Historique, …
   - ✓ Audit des images : Docker Scan

SECLUDIT

Sécurité Docker : Liens utiles

- Guides :
  - https://docs.docker.com/engine/security/security/
  - https://docs.docker.com/docker-cloud/builds/image-scan/
  - https://github.com/GDSSecurity/Docker-Secure-Deployment-Guidelines
  - https://benchmarks.cisecurity.org/tools2/docker/CIS_Docker_1.13.0_Benchmark_v1.0.0.pdf

- Outils :
  - https://github.com/dev-sec/cis-docker-benchmark
  - https://github.com/coreos/clair/
  - https://github.com/cr0hn/dockerscan
  - https://cloud.docker.com/

SECLUDIT

SECLUDIT

Questions ?