Sécuriser l’hôte Docker - CIS Benchmarks

- Benchmark officiel avec >250 pages de règles
- Sections : hôte, démon, fichiers conf, images, conteneurs, opérations, Swarm
- CIS Benchmarks (https://www.cisecurity.org/cybersecurity-best-practices/)

CIS Benchmarks

- Plus de 250 pages dédiées, avec les règles de bonnes pratiques à mettre en œuvre, pour le CIS Benchmark inhérent à la version communautaire de Docker.
- Dans ce document, les vérifications sont découpées en plusieurs grandes parties :

  - configuration de l'hôte Docker ;
  - configuration du démon Docker ;
  - fichiers de configuration du démon Docker ;
  - images et fichiers de build ;
  - configuration des conteneurs Runtime ;
  - opérations de sécurité pour Docker ;
  - configuration de Docker Swarm.

Docker Bench for Security

- Outil officiel sur GitHub (Apache-2.0)
- https://github.com/docker/docker-bench-security
- Conteneur prêt-à-l'emploi pour exécuter les checks
- Exemple : docker run docker-bench-security

```
docker run --rm --net host --pid host --userns host --cap-add
audit_control \
    -e DOCKER_CONTENT_TRUST=$DOCKER_CONTENT_TRUST \
    -v /etc:/etc:ro \
    -v /usr/bin/containerd:/usr/bin/containerd:ro \
    -v /usr/bin/runc:/usr/bin/runc:ro \
    -v /usr/lib/systemd:/usr/lib/systemd:ro \
    -v /var/lib:/var/lib:ro \
    -v /var/run/docker.sock:/var/run/docker.sock:ro \
    --label docker_bench_security \
    docker-bench-security
```

Erreurs communes - Audit du démon Docker

- Dockerd tourne en root → doit être audité
- Configurer auditd avec règles spécifiques

```
## Audit Docker demon
-w /usr/bin/docker -p wa
-w /var/lib/docker -p wa
-w /etc/docker -p wa
-w /lib/systemd/system/docker.service -p wa
-w /lib/systemd/system/docker.socket -p wa
-w /etc/default/docker -p wa
-w /etc/docker/daemon.json -p wa
-w /usr/bin/docker-containerd -p wa
```

- Tracer les modifications critiques

Erreurs communes - Centralisation des logs

- Logs Docker doivent être envoyés vers un SIEM
- Par défaut : json-file (local)
- Configurer syslog, Elasticsearch, etc.
- Pour vérifier si vous avez cette configuration activée, exécutez la commande :

  docker info -format '{{ .LoggingDriver }}'

- Rediriger vers un serveur de gestion des logs.

  dockerd --log-driver=syslog --log-opt syslog-address=tcp://x.x.x.x

Erreurs communes - Restriction des privilèges

- Empêcher no_new_priv=false
- Activer

  dockerd --no-new-privileges

- Pour vérifier si vous avez activé cette option, effectuez la commande :

  ps -ef | grep dockerd

Audit du système avec Lynis

- Outil GPL-3.0 pour auditer Linux et autres OS

  git clone github.com/CISOfy/lynis

  ./lynis audit system