

\$ Docker an toàn?



Khoá container trước khi lên prod, theo 1 → 6.

1 Bỏ quyền root

USER 10001:10001

Cuối Dockerfile: thôi chạy root.

docker run -u 1000:1000

Ép UID/GID ngay lúc chạy.

docker exec <c> id

Thấy uid=0 là đang chạy root.

2 Rootfs chỉ đọc

docker run --read-only

Kẻ tấn công không ghi được file.

--tmpfs /tmp:size=64m

Chỗ ghi tạm nằm trên RAM.

docker diff <c>

File nào đã bị thêm/sửa/xoá?

3 Cắt quyền kernel

--cap-drop=ALL

Bỏ toàn bộ Linux capabilities.

--cap-add=NET_BIND_SERVICE

Chỉ cấp lại đúng quyền cần.

**--security-opt **
no-new-privileges

Chặn leo quyền qua setuid.

4 Giới hạn tài nguyên

--memory=512m --cpus=1

Một container không nuốt cả host.

--pids-limit=200

Chặn fork bomb trong container.

docker stats --no-stream

So mức dùng thật với giới hạn.

5 Quét CVE với trivy

**trivy image **

CVE trong gói OS và thư viện.

**trivy image --exit-code 1 **
**--severity CRITICAL **

Fail pipeline khi có CVE nặng.

trivy config .

Dockerfile/K8s YAML cấu hình sai?

6 Image sạch, không lộ

**docker inspect -f **
**'{{.Config.User}}' **

Kết quả rỗng = mặc định root.

RUN --mount=type=secret

Secret lúc build, không vào layer.

**dive **

Soi từng layer, tìm file thừa.

Checklist 6 dòng trước khi lên prod

USER ≠ root (uid 0)

--read-only + tmpfs

cap-drop ALL, thêm lẻ

limits mem · cpu · pids

trivy 0 CRITICAL

docker.sock cấm mount

<c> = container · = image

Vibe DevOps · Build · Run · Fix