Virtualización vs Contenedores: Ambos buscan aislar procesos y maximizar recursos

Maquinas Virtuales: virtualizan el hardware, usan el hipervisor para repartir CPU/RAM, son ideales para aislamiento total y seguridad robosta

Contenedores: virtualizan el sistema operativo, son ligeros porque comparten kernel del host

Ecosistema Docker: El contenedor es la instancia de ejecucion (la aplicacion + dependencias) y Docker (Plataforma) es el conjunto de herramientas (CLI, Daemon, Builder) que permite crear, empaquetar y distribuir esos contenedores.

Ciclo de Vida: Imagenes y Dockerfile: Construir y ejecutar en cualquier lugar.

1. Dockerfile (La receta): un archivo con instrucciones paso a paso
2. Imagen (Artefacto): El resultado inmutable del dockerfile, funciona como plantilla de solo lectura
3. Contenedor (La instancia): es la imagen cobrando vida

Redes y conectividad: Docker aisla la red pero permite comunicación controlada:

- Brige (Puente): la red estándar, los contenedores se ven por sus nombres (DNS interno) pero estan ocultos al mundo exterior.
- Publicacion de puertos: una brecha que se abre para que el trafico externo llegue al contenedor

Seguridad y Aislamiento: un contenedor no es una caja negra impenetrable

- Namespace: evita conflicto de nombres en variables, funciones o clases
- Cgroups: limita cuanto CPU o memoria puede usar el proceso para evitar que tumbe al servidor

Mejores Practicas de Endurecimiento:

- No ejecuta procesos root dentro del contenedor
- Ejecutar el sistema de archivos como read-only siempre que sea posible
- Analizar las imagenes en busca de fallos de seguridad antes de desplegar (Trivy-Grype)
- Utilizar el principio de mínimo privilegio
- Genera la lista de materiales (SBOM) con sylf de toda librerias o paquetes de la imagen

Docker Compose: Orquestacion local: Compose crea un DNS interno para comunicar contenedores

DevSecOps: healthcheck de contenedores, Limite de recursos para que el contenedor no consuma todos los recursos, no guardar datos sensibles en carpetas sin cifrar