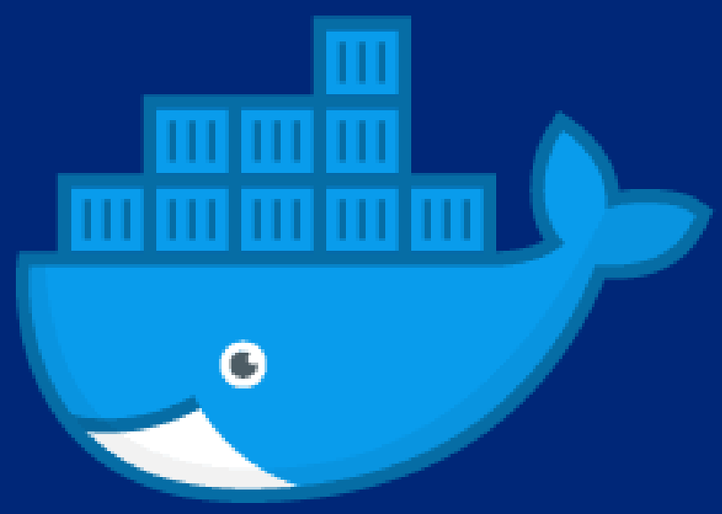
ClickIT
DevOps & Software Development



Docker Security Best Practices

ClickIT
DevOps & Software Development

KEEP DOCKER HOST AND DOCKER ENGINE UP TO DATE ALONG WITH YOUR DOCKER IMAGES

Docker containers run on the Docker engine available on host machines. These host machines could be Linux/Mac or Windows. The Docker Engine can be one of the available versions. It is vital to use its latest, stable version, which updates the known issues from the previous releases. The same applies to the host Operating System.

ClickIT
DevOps & Software Development

AVOID STORING CONFIDENTIAL DATA IN DOCKERFILE INSTRUCTIONS

You can use environment variables within the Docker containers using ENV or ARGS instructions. While setting up environment variables, you should make a note that one should never assign secrets, credentials, passwords, etc to variables in Dockerfile or should not hardcode in any command.

ClickIT
DevOps & Software Development

AVOID USING AN UNTRUSTED IMAGE REGISTRY

Whenever you pull an image from an untrusted publisher, do not forget to verify the source registry, and the Dockerfile used to build the image, and also carefully choose the base image for your Dockerfile, i.e. the FROM instruction.

ClickIT
DevOps & Software Development

LIMIT CONTAINER RESOURCES

When Docker containers are compromised, attackers may try to use the host machine resources to perform malicious activity. Also, if a particular container starts utilizing all the resources from the host machine, other containers residing in the same place may get impacted due to resource unavailability. To avoid such situations, it is recommended to set resource limits on Docker containers.

ClickIT
DevOps & Software Development

SCAN IMAGES DURING DEVELOPMENT

Docker images are built from Dockerfiles, and Dockerfiles contain instructions to use the base image, install packages, start applications, etc. Dockerfile may also contain credentials hardcoded in it by mistake.

Scanning images for security vulnerabilities helps you solve them before they arise in the Production environment.

ClickIT
DevOps & Software Development

Secure your Docker Container with ClickIT's highly experienced LATAM team

CONTACT US