

Обеспечение безопасности контейнеров: **Безопасность рабочей нагрузки**

В рамках данного выступления рассматривается использование сканеров уязвимостей, сравнение и примеры работы с ними в различных конфигурациях. В частности, в фокусе выступления – обеспечение безопасности контейнеров в рамках разработки, тестирования и внедрения программных решений, направленных на развитие обеспечения безопасности конвейера DevSecOps.

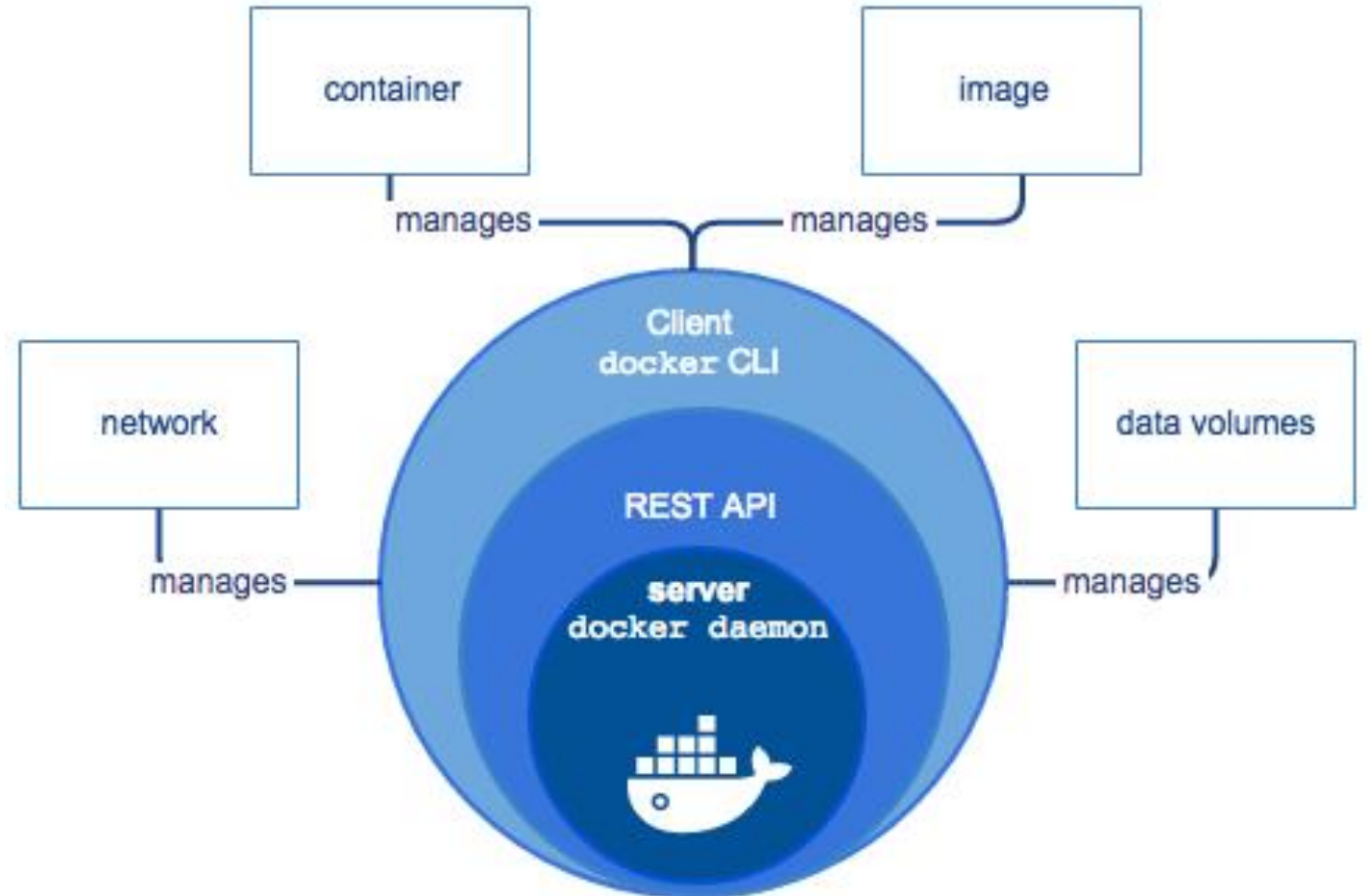
Содержание

1. Внутреннее устройство docker.
2. Docker CLI. Docker daemon.
3. PoC exploits.
4. Побег из контейнера (container breakout vulnerabilities).

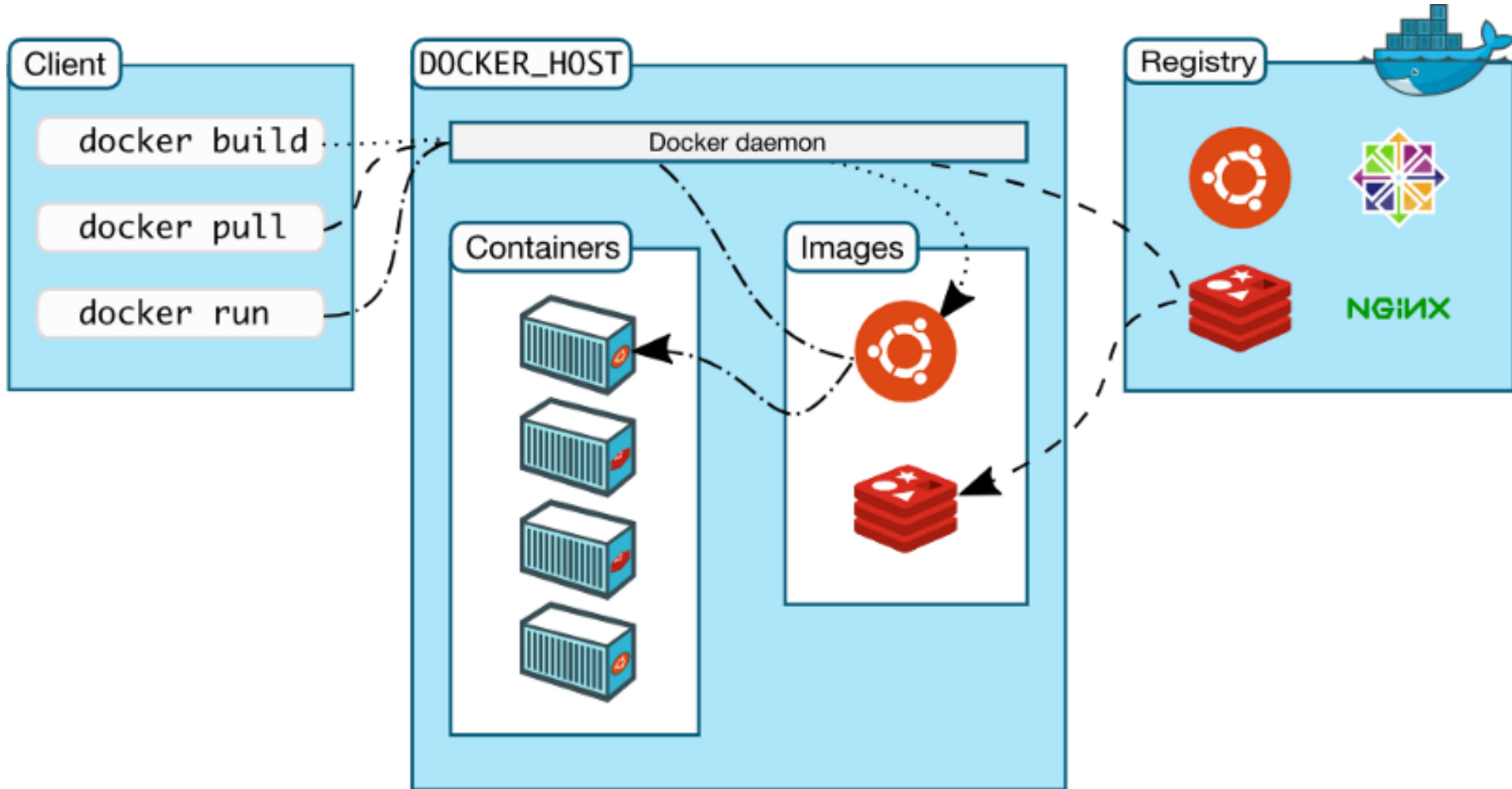
<https://github.com/krol3/container-security-checklist>

Docker

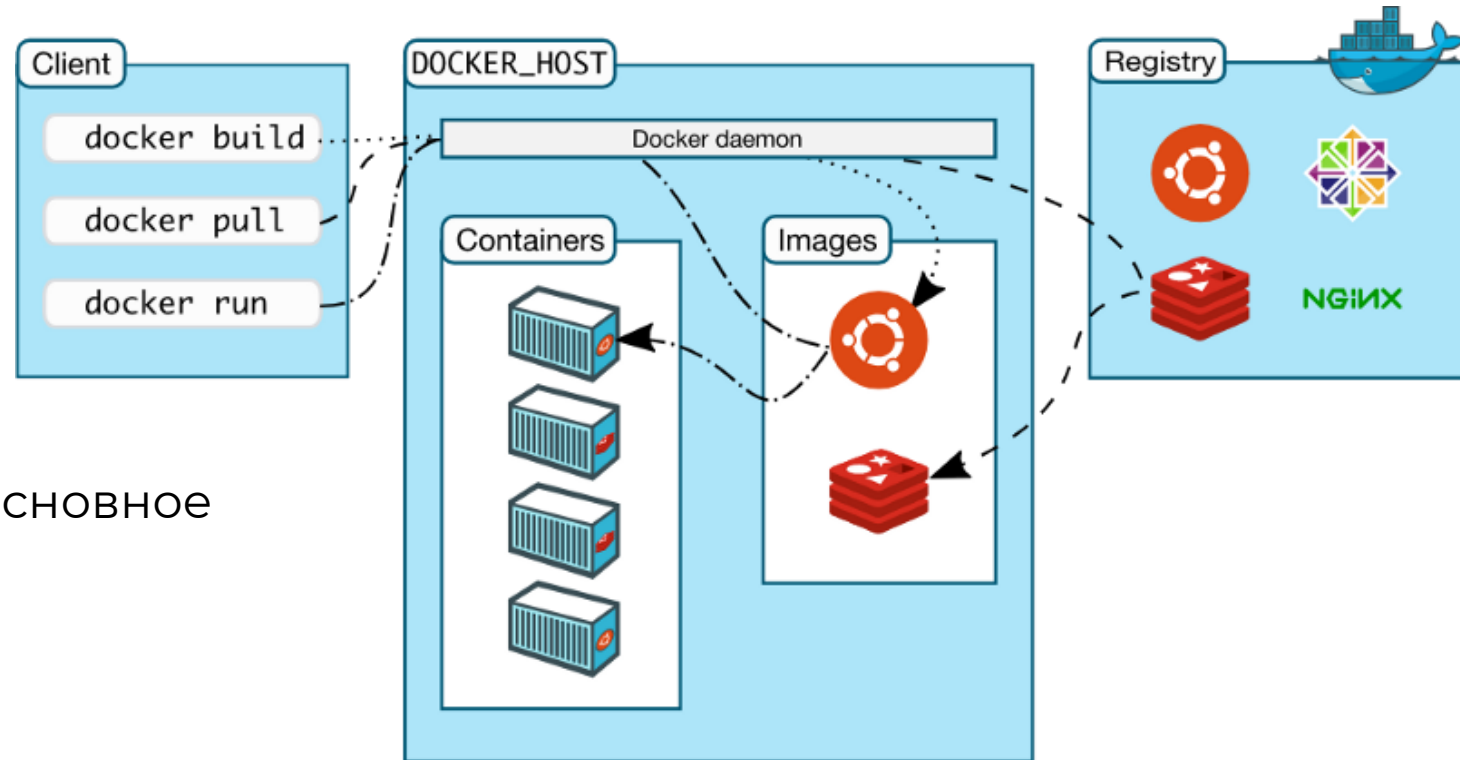
Docker (Docker Engine) - это одна из систем, позволяющих контейнеризировать приложения, предназначена для разработки, развертывания и запуска приложений в контейнерах



Docker



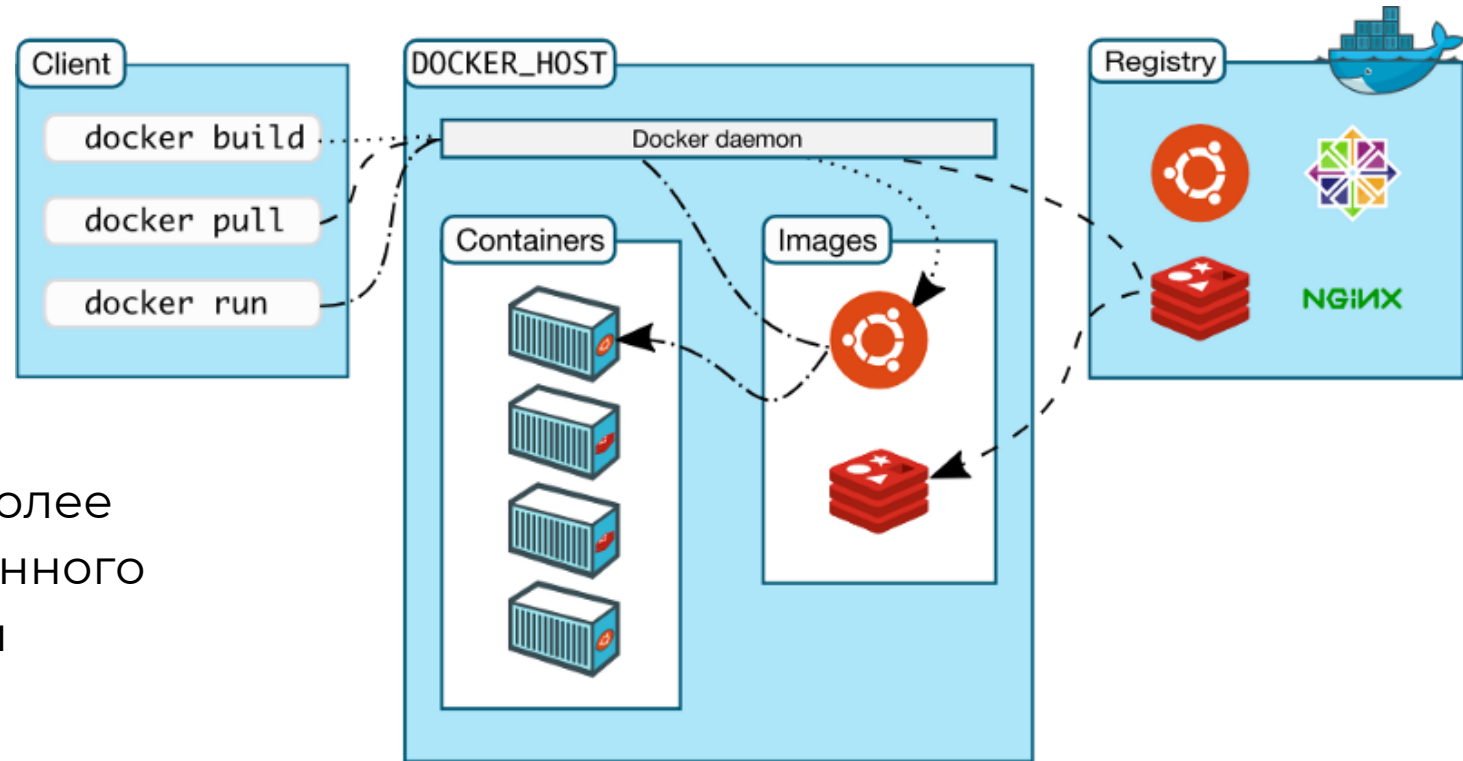
Docker CLI & Daemon



Клиент Docker (Docker Client) — это основное средство, которое используют для взаимодействия с Docker

Демон Docker (Docker Daemon) — это сервер Docker, который ожидает запросов к API Docker. Демон Docker управляет образами, контейнерами, сетями и томами

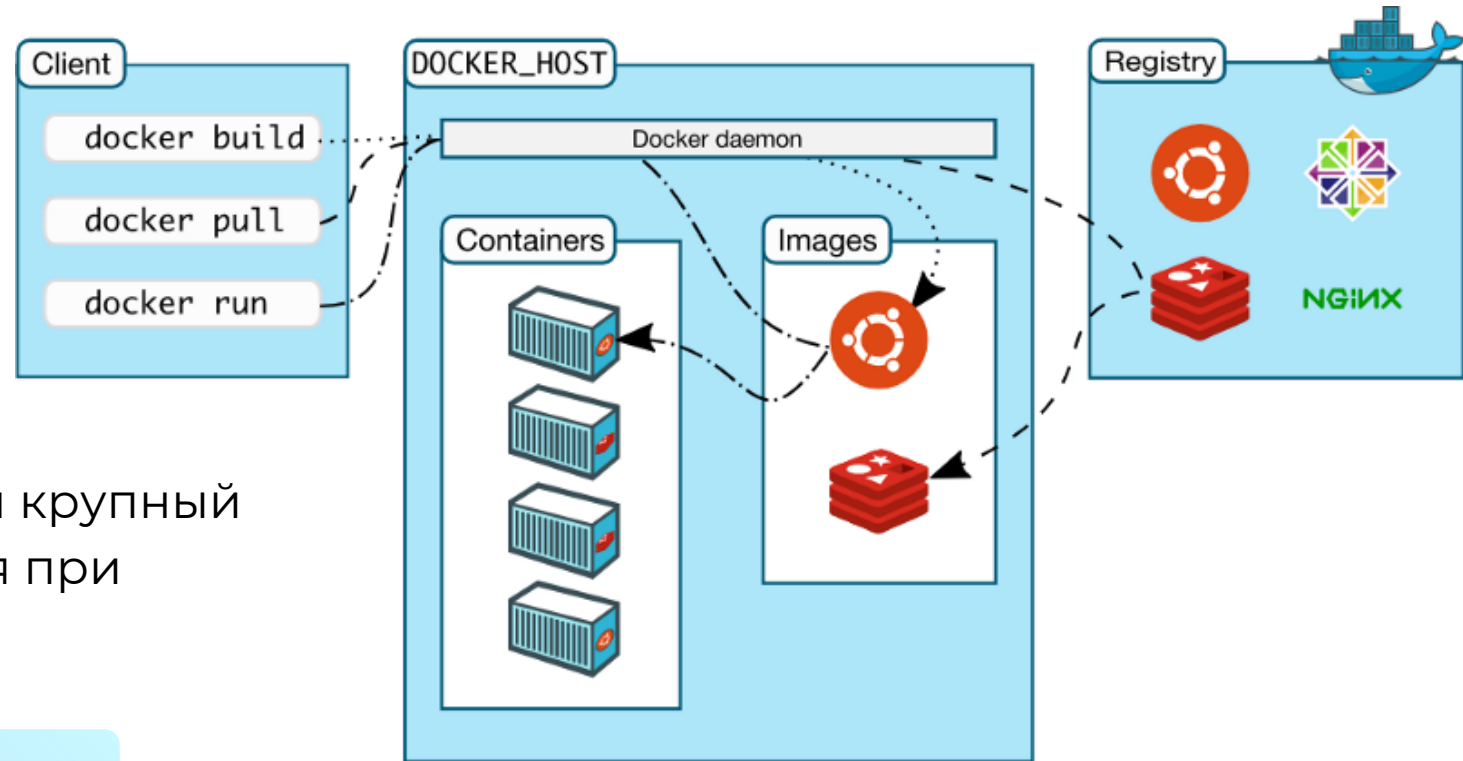
Docker



Тома Docker (Docker Volumes) – наиболее предпочтительный механизм постоянного хранения данных, потребляемых или производимых приложениями.

Реестр Docker (Docker Registry) – удаленная платформа, используемая для хранения образов Docker. В ходе работы с Docker образы отправляют в реестр и загружают из него.

Docker

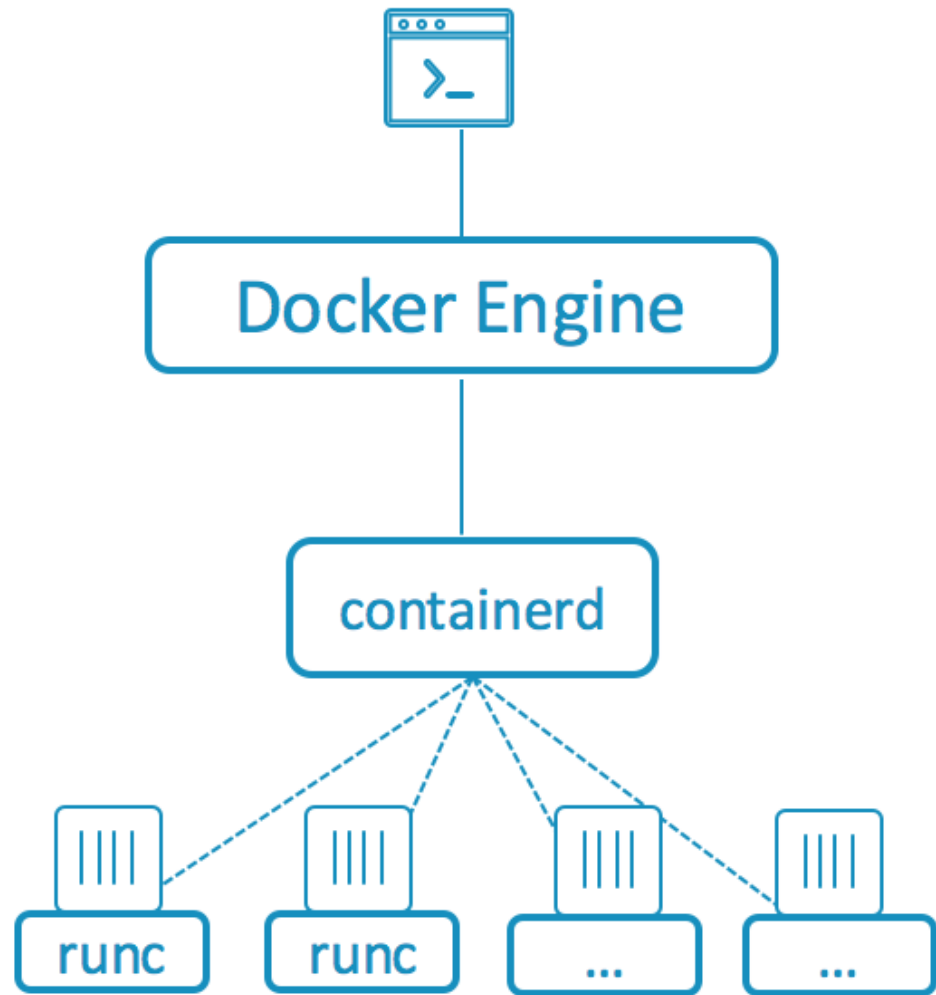


Docker Хаб (Docker Hub) — это самый крупный реестр образов Docker, используется при работе с Docker по умолчанию.

Репозиторий Docker (Docker Repository) – набор образов Docker, обладающих одинаковыми именами и разными тегами.

Теги — идентификаторы образов.

Docker



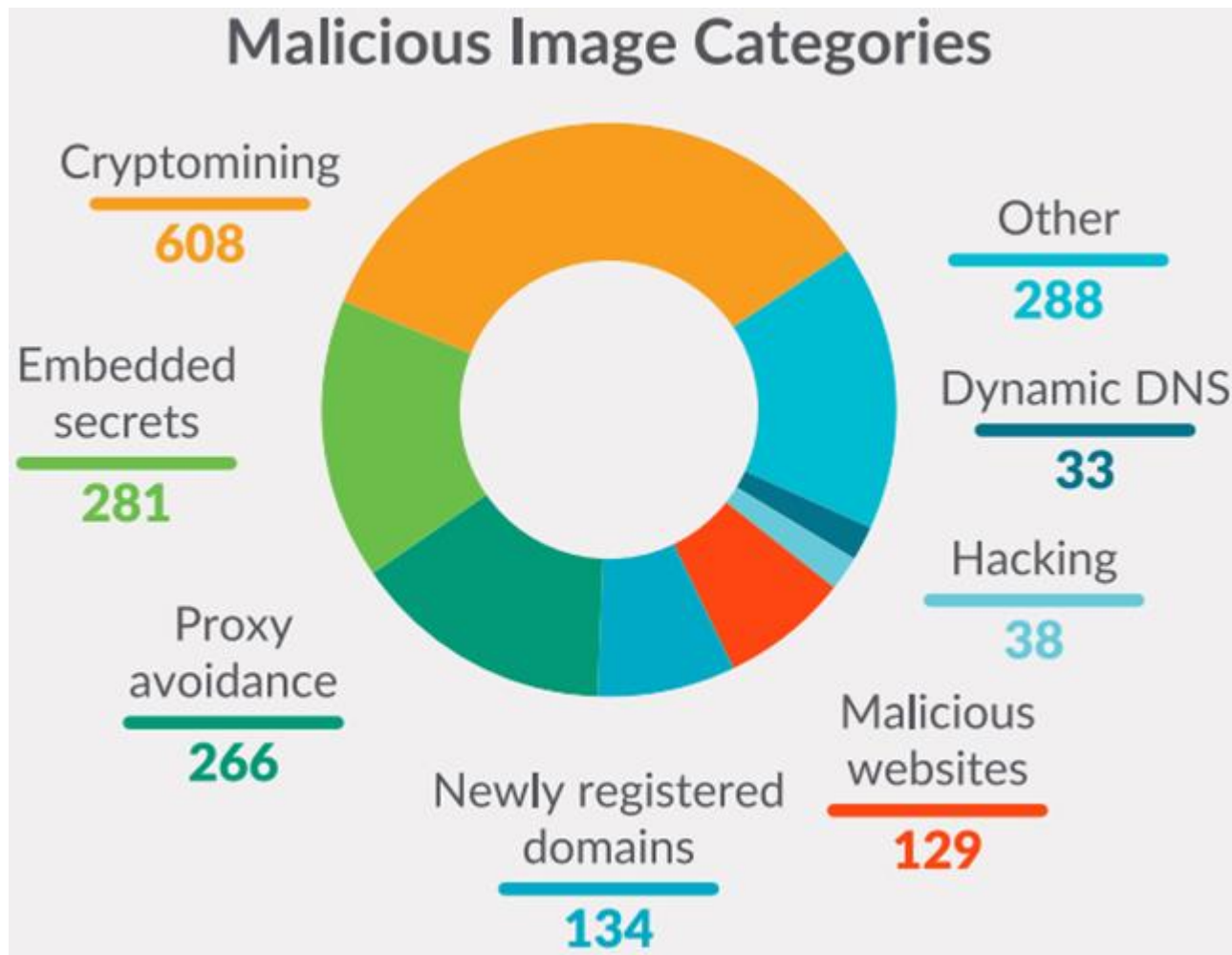
Same Docker UI and commands

User interacts with the Docker Engine

Engine communicates with containerd

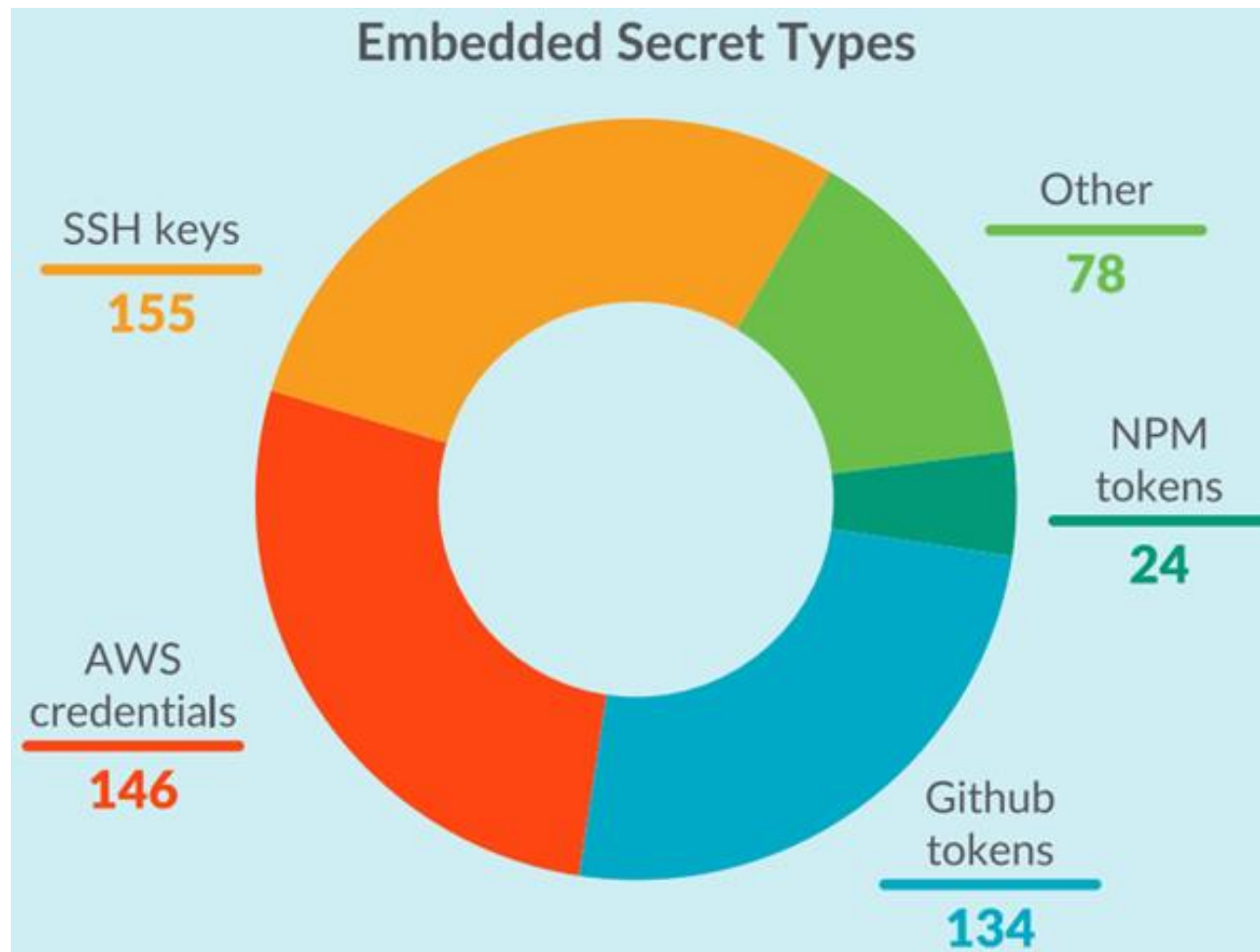
containerd spins up runc or other OCI compliant runtime to run containers

Безопасно ли?



<https://sysdig.com/blog/analysis-of-supply-chain-attacks-through-public-docker-images/>

Безопасно ли?



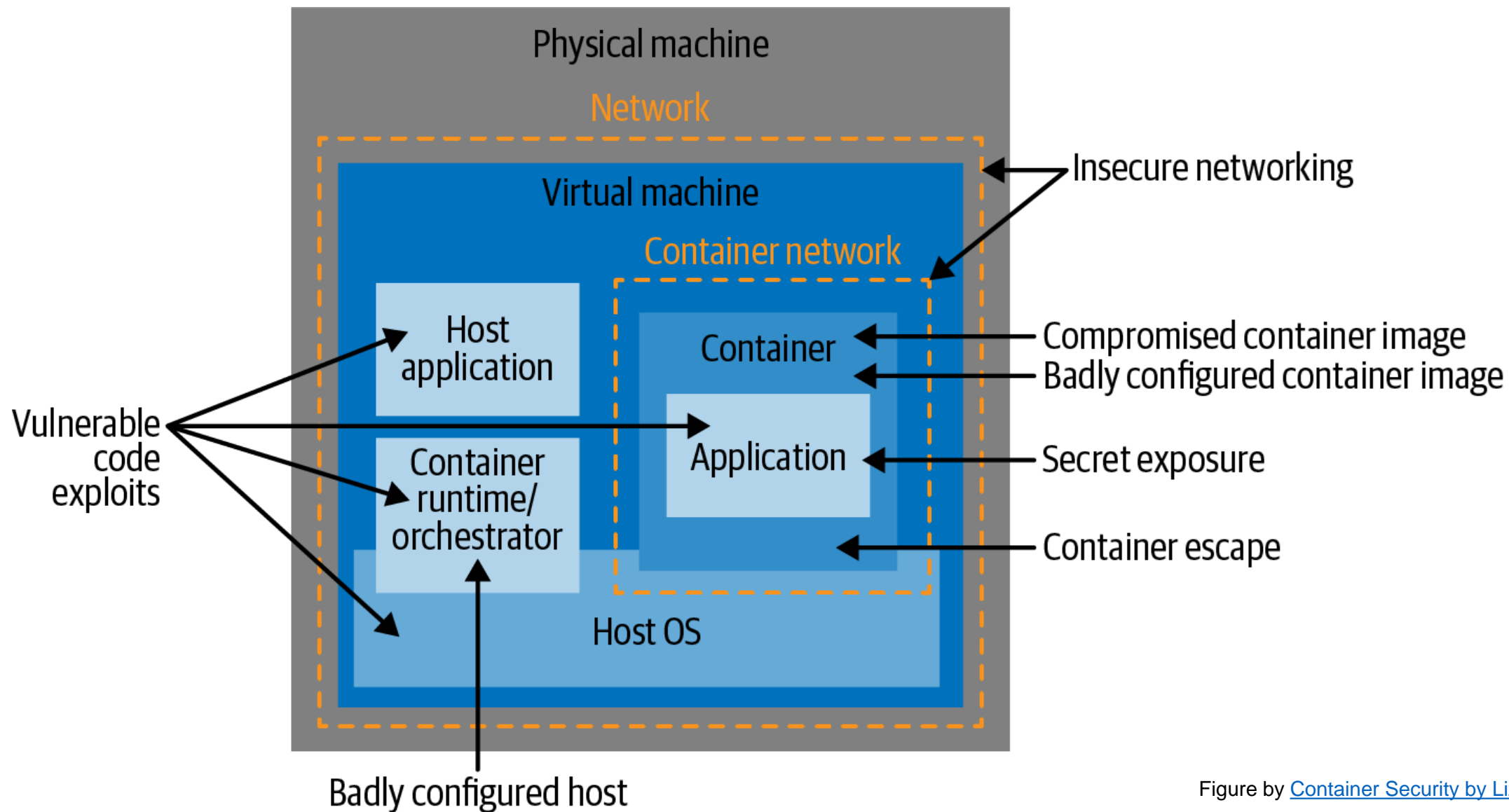
<https://sysdig.com/blog/analysis-of-supply-chain-attacks-through-public-docker-images/>

Безопасно ли?

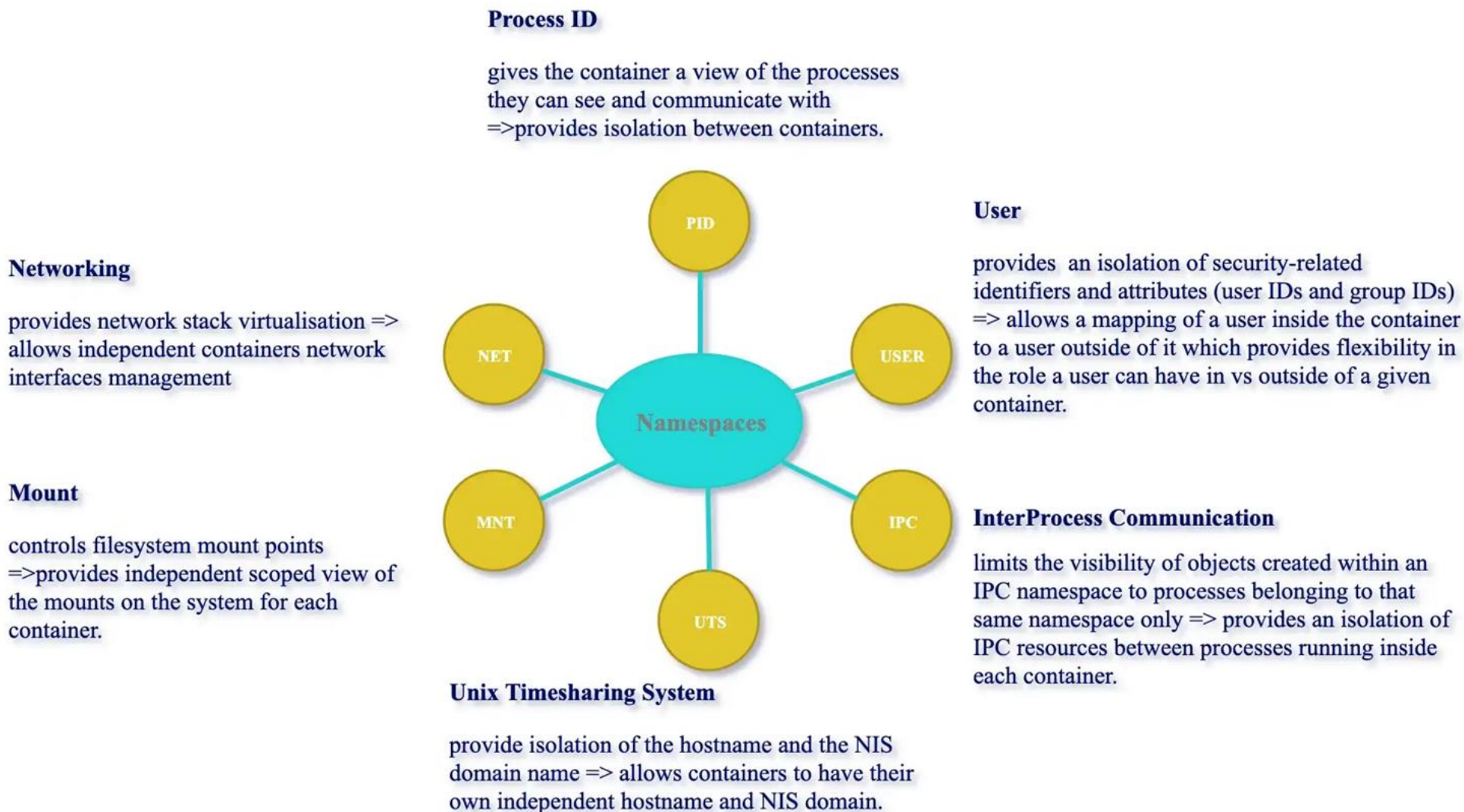
Image Name	Image Digest	Downloads
ynprpagamentitk/liferay	3978fb1b4d9581fddbd44f44901e87f9f8baf7942c74d5820c573c06cc83f861	281
arrghgluiistk/drupal	9ab7485664242c00db8ec6e0ea2b829320a7762107527a8c66d1754ec730c8b8	213
eiprtvchdcom/drupal	c7490c9e2a437e111968e96529cef80bc0d92a7040b656e2404114837e270941	131
vesnpsexga/joomla	3978fb1b4d9581fddbd44f44901e87f9f8baf7942c74d5820c573c06cc83f861	118
ganodndentcom/drupal	380898334e75e10cc1e5cf4c574d46e57f8b32f52552924fc1f5c158a7fb3291	55
dogigeronracom/drupal	50c1685bfcd67435188e74c8b5321de32f44f0c613fc2eebdbff3020273e690a	37
pumevnezdiroorg/drupal	bf9c24747d7c2903cf931a0a321f37c44fe6236dc40679d4cec3743384943e40	31

<https://sysdig.com/blog/analysis-of-supply-chain-attacks-through-public-docker-images/>

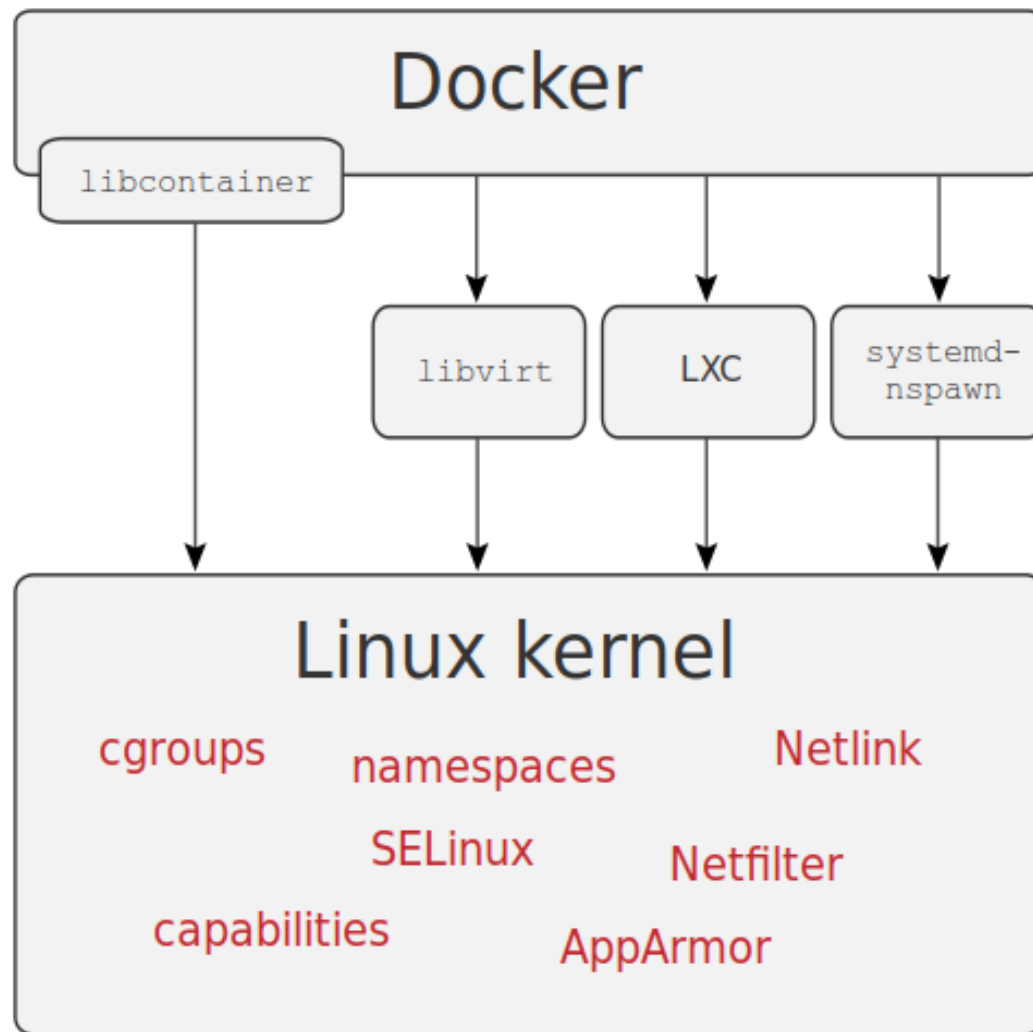
Обеспечение безопасности контейнеров



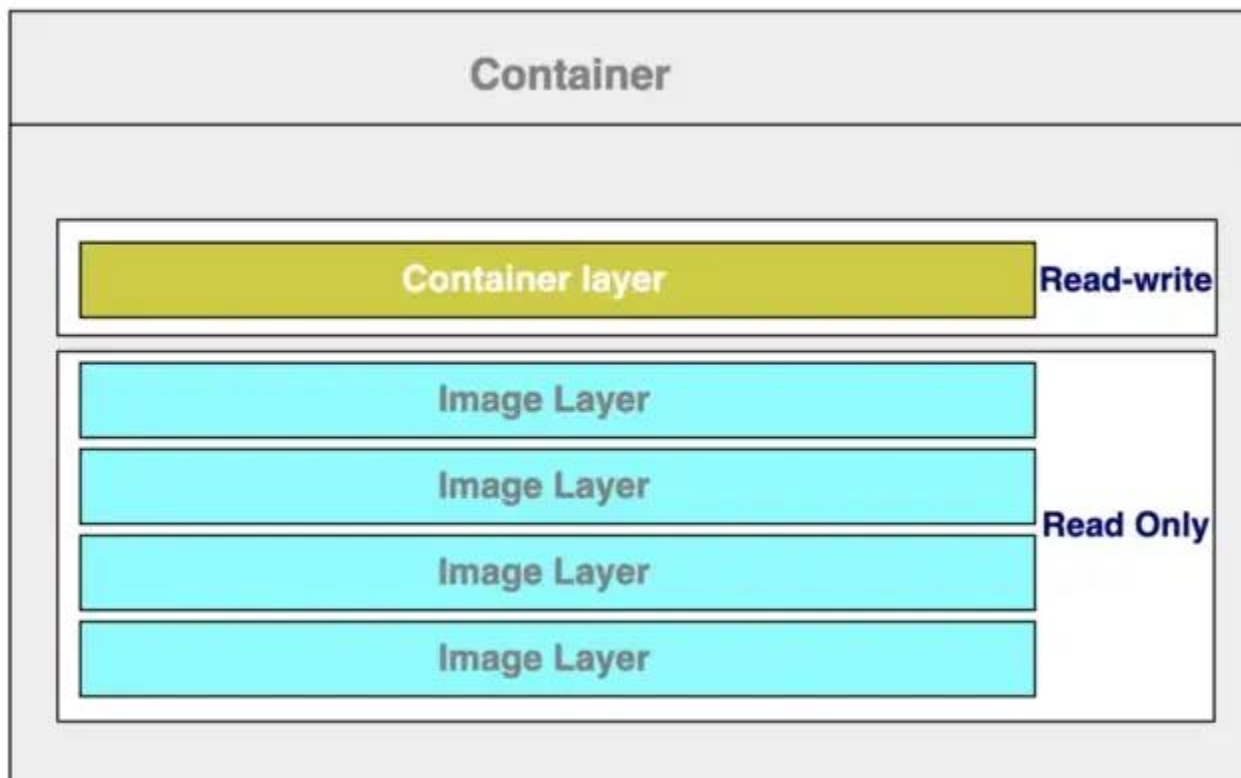
Обеспечение безопасности контейнеров



Обеспечение безопасности контейнеров



Обеспечение безопасности контейнеров



<https://faun.pub/deep-dive-into-docker-architecture-ddb343594056>

Docker

1. Low-Level Container Runtimes:

- [runC](#)
- [crun](#)
- [containerd](#)

Docker

2. High-Level Container Runtimes

- [Docker Engine](#)
- [Podman](#)
- [CRI-O](#) - OCI-based implementation of Kubernetes Container Runtime Interface
- [Mirantes Container Runtime](#)

Docker

3. Sandboxed and Virtualized Container Runtimes

- [gVisor](#)
- [nabla-containers](#)
- [kata-containers](#)

Docker

Runtime Security

- IOC (Indicator Of Compromise)
- Zero Days attack
- Compliance requirement
- Recommended in highly dynamic environments

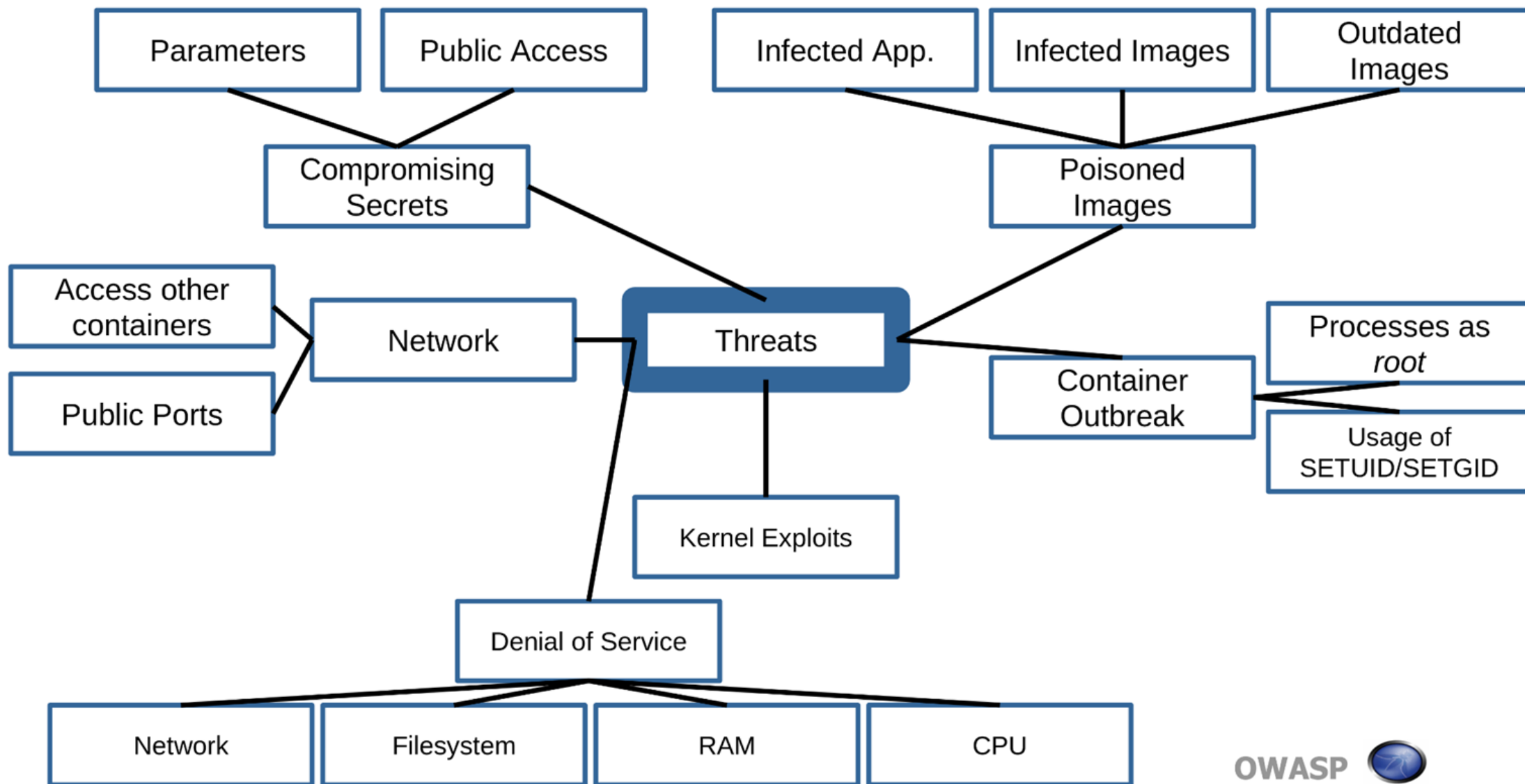
Обеспечение безопасности контейнеров

Container Security Checklist: From the image to the workload

https://cloudsecdocs.com/container_security/defensive/containers/docker_focus_areas/

https://cloudsecdocs.com/container_security/defensive/containers/secure_dockerfiles/#hardening-kernel

Обеспечение безопасности контейнеров

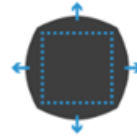


Обеспечение безопасности контейнеров

TYPES OF SECURITY THREATS AND HOW TO AVOID THEM



KERNEL EXPLOITS
If a container can cause a kernel panic or similar, it will bring down the whole host.



DENIAL OF SERVICE (DOS) ATTACKS
All containers share kernel resources. If one container monopolizes access to a resource, it will starve out the other containers.



CONTAINER BREAKOUTS
If an attacker can breakout of a container, they can gain access to the host and other containers.



POISONED IMAGES
Images may be injected with trojan or virus infected software. Or they may simply be running outdated, known-vulnerable versions of software.



COMPROMISED SECRETS
API keys and database passwords must be kept secure to prevent attackers gaining access.

SEGREGATE CONTAINER GROUPS WITH VMs					
DEFANG SETUID/SETGID BINARIES	○			○	
BE AWARE OF CPU SHARES		○			
VERIFY IMAGES				○	
SET CONTAINER FILE SYSTEM TO READ-ONLY	○	○	○		○
SET A USER	○		○		○
DO NOT USE ENVIRONMENT VARIABLES TO SHARE SECRETS					○
DO NOT RUN CONTAINERS WITH THE --privileged FLAG	○		○		○
TURN OFF INTER-CONTAINER COMMUNICATION	○	○	○		
SET VOLUMES TO READ-ONLY	○		○		
SET MEMORY LIMITS		○			
DO NOT INSTALL UNNECESSARY PACKAGES IN THE CONTAINER	○		○		

https://cloudsecdocs.com/container_security/theory/threats/docker_threat_model/

PoC exploit (Proof-of-Concept) - атака на компьютер или сеть, которая выполняется только для того, чтобы доказать, что это можно сделать.

Эксплойт для проверки концепции обычно не причиняет вреда, но показывает, как злоумышленник может взломать сеть или воспользоваться уязвимостью в программном обеспечении или, возможно, в оборудовании.

Docker Glossary

1. Освободить
непривилегированные
учетные данные

2. Выделение
привелигированные
учетных данные в
освободившейся
памяти

3. Становление рутом

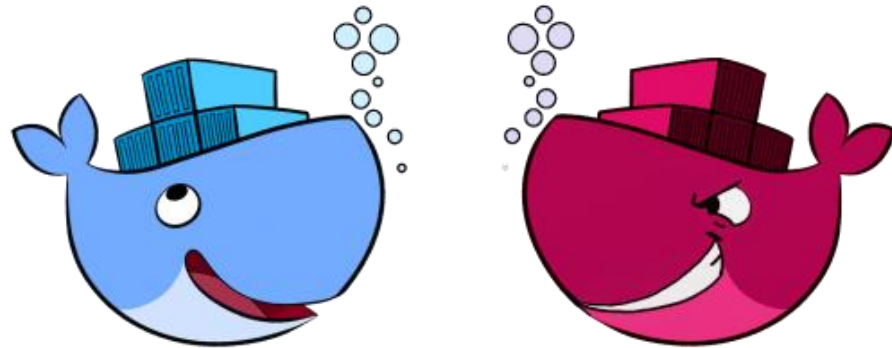
https://www.container-security.site/attackers/container_breakout_vulnerabilities.html

Docker Glossary

<https://docs.docker.com/glossary/>

Docker

<https://github.com/DockerSecurityPlayground/DSP>



Docker
Security Playground



СПАСИБО ЗА ВНИМАНИЕ!