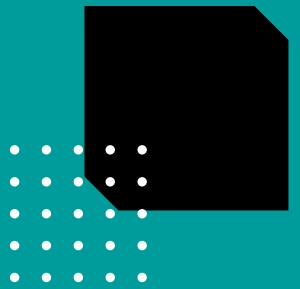
Hands-on especial Containers: Contêiner é Seguro ?



Yago Ésquines

Coordenador de TI em Software Livre

- Mais de 3 anos de 4Linux
- Formado em Ciência da Computação e Segurança da Informação
- DC Comics é melhor que Marvel!
- 42 é a resposta para a vida, o universo e tudo mais e o vim pode provar (`vim -c 'help 42'`)
- **Certificações:**

Linux Professional Institute LPIC-1 LINUX ADMINISTRATOR

Linux Professional Institute LPIC-2 LINUX ENGINEER

CERTIFIED kubernetes ADMINISTRATOR

DevOps ESSENTIALS CERTIFIED ITCERTS

Objetivos

01 Conceito: Há contêiner seguro?

02 Boas Práticas de Segurança para Ambientes Conteinerizados

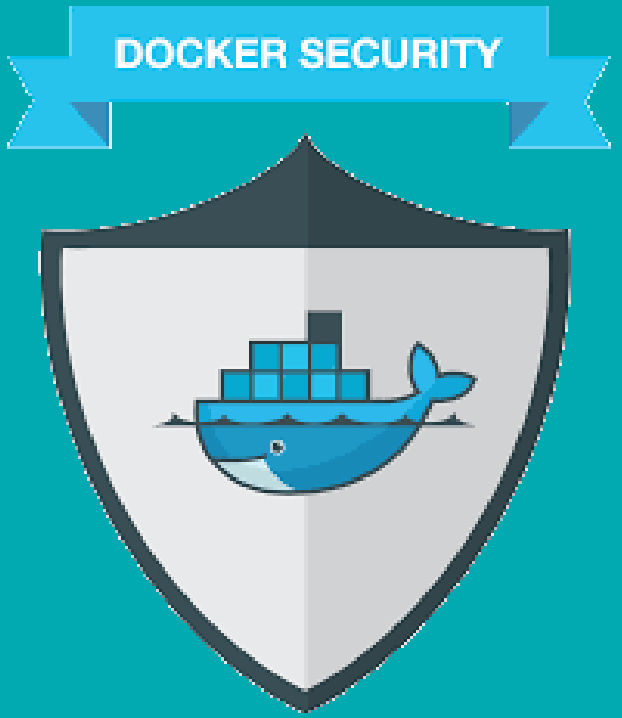
03 Análise de Segurança com Clair e Docker Bench for Security

04 Podman x Docker, Who Wins?

Conceito: Há contêiner seguro?_

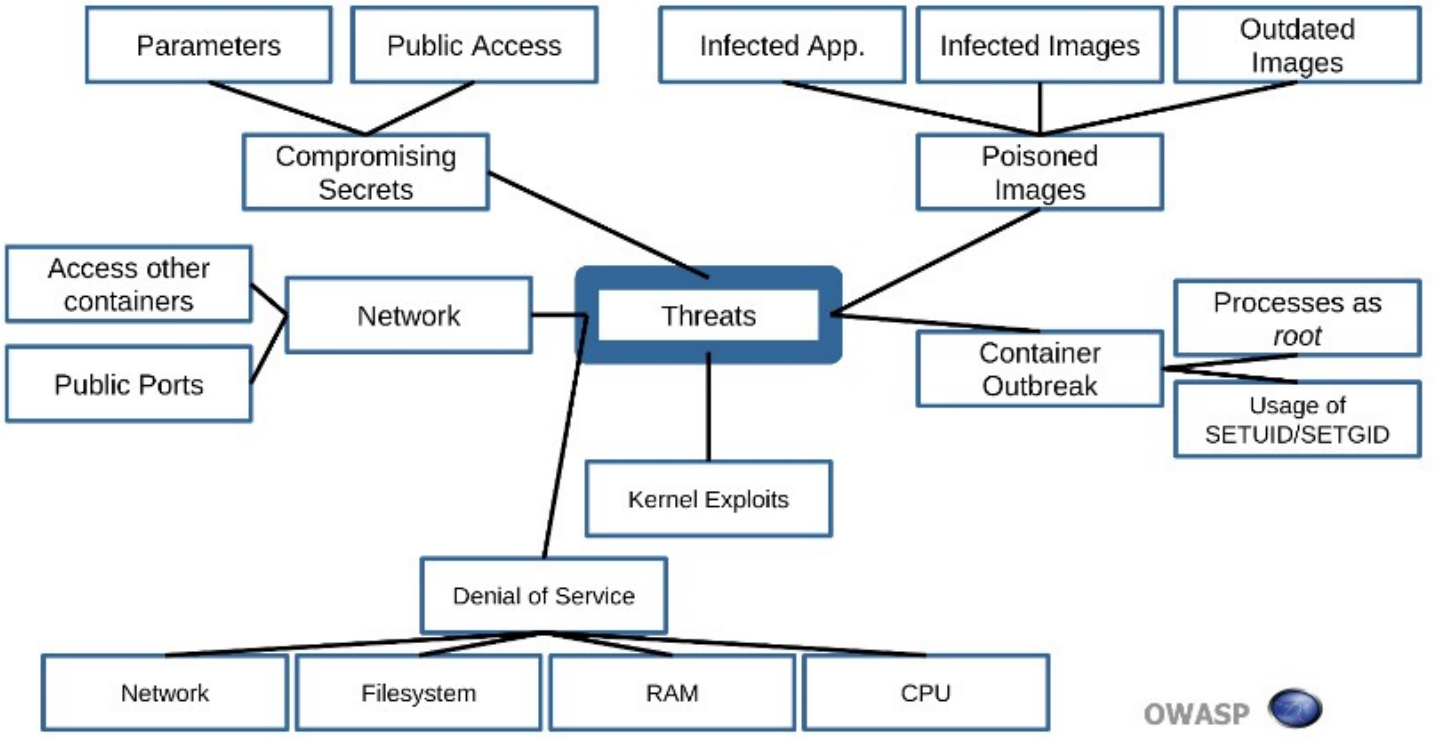
- **Pontos de Mercado:**
  - Contêiner estão cada vez mais populares
  - Estão sendo utilizados amplamente no mercado de TI.

- **Preocupação**
  - Quais são os ataques que um ambiente conteinerizado por receber ?
  - Imagens de containers, mesmo as oficiais, são 100% confiáveis?
  - Ambientes com Conteinerização precisam de um atenção nas configurações?



Fonte: https://owasp.org/www-project-docker-top-10/

Conceito: Há contêiner seguro?_



NÃO HÁ CONTÊINER 100% SEGURO

Fonte: https://owasp.org/www-project-docker-top-10/

Boas Práticas de Segurança para Ambientes Conteinerizados_

#0	Keep Host and Docker up to date
#1	Do not expose the Docker daemon socket
#2	Set a user
#3	Limit capabilities (Grant only specific capabilities, needed by a container)

Fonte: https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html

Boas Práticas de Segurança para Ambientes Conteinerizados_

#4	Add –no-new-privileges flag
#5	Disable inter-container communication (--icc=false)
#6	Use Linux Security Module **First of all, do not disable default security profile!**
#7	Limit resources

Fonte: https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html

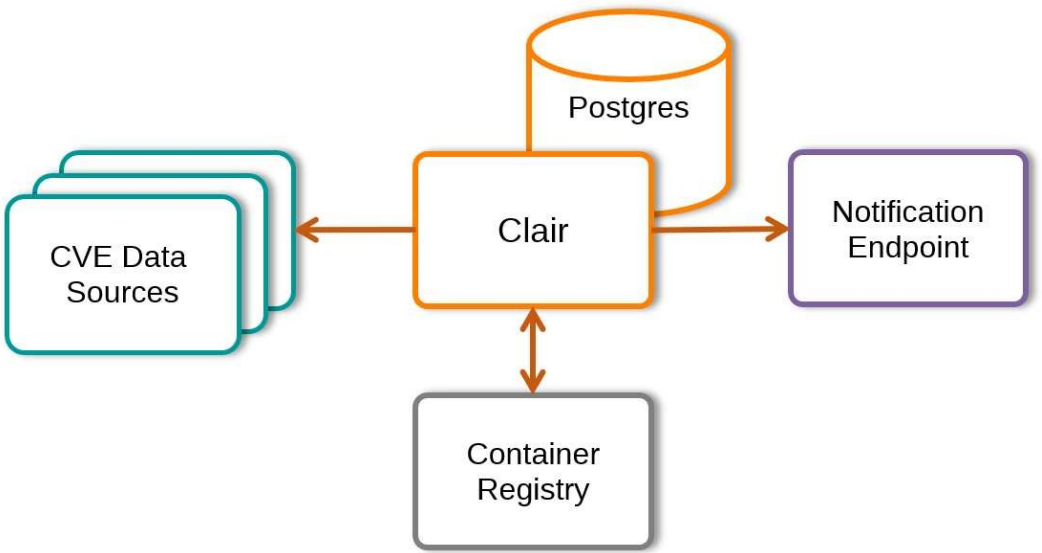
Boas Práticas de Segurança para Ambientes Conteinerizados_

#8	Set filesystem and volumes to read-only
#9	Use static analysis tools (Clair!)
#10	Set the logging level to at least INFO
#11	Lint the Dockerfile at build time

Fonte: https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html

#clair: Identificando Vulnerabilidades_

- Objetivo de Clair é fazer a análise de vulnerabilidades em imagens de contêineres.
- Tem retroalimentação de vulnerabilidades conhecidas (CVEs)
- Permite uma maior comunicação para o ajuste de possíveis riscos dentro dos contêiners.
- **Estrutura do Clair:**



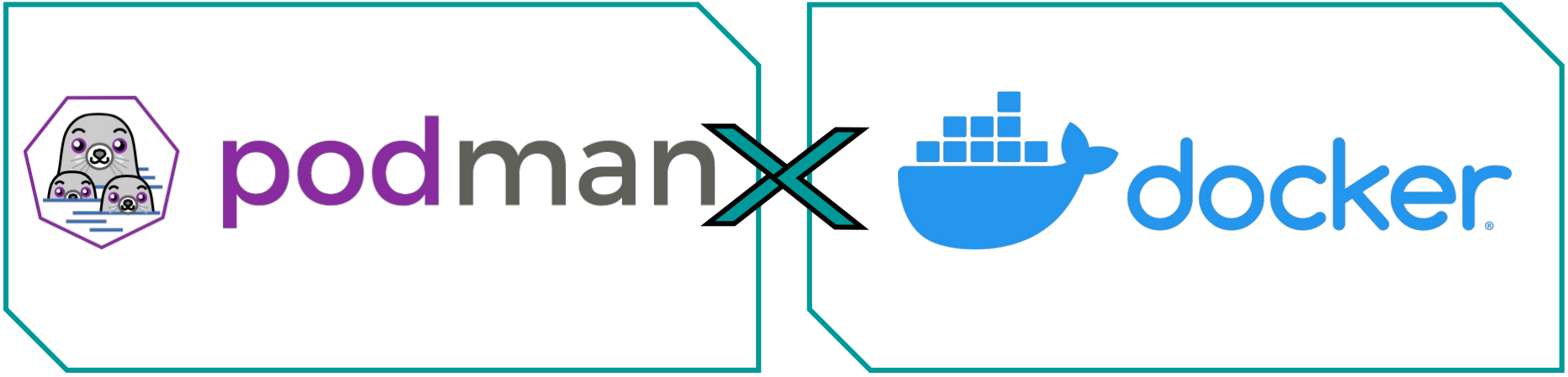
Docker Bench for Security_

Docker Bench for Security é um script executado nos ambientes docker que faz a avaliação se o ambiente está ou não em conformidade com o guia de boas práticas da CIS Docker Benchmark.

- **Execução:**

```
[node1] (local) root@192.168.0.8 ~ 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/docker-bench-security
```

Podman x Docker, Who Wins?_



CONFIE NA 4LINUX

Mais de **70.000 alunos** treinados em mais de 4800 empresas diferentes.

Mais de **1000 projetos** implementados em mais de 380 clientes.

Entre em contato

S

P

T: +55 11. 2125-4747

T: +55 11. 2125-4748

W: +55 11. 96429-0501

Rua Vergueiro, 3057

Vila Mariana, SP

04101-300