JUNE 27, 2023

DEVSEC CON THE AMERICAS 4

Container Security - Strengthening the Heart of your Operations

Kunal Verma

Community Manager at Kubesimplify

@kverma_twt

Siddhant Khisty

Community Manager at WeMakeDevs

@i_siddhantk

@kverma_twt

Kunal Verma

Community Manager at Kubesimplify
DevOps & Open Source Advocate
Cloud Native Contributor

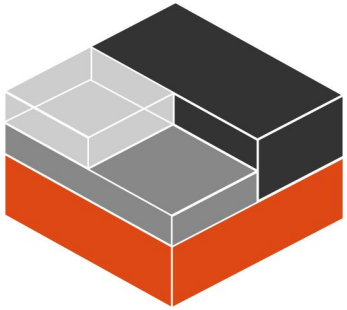
@i_siddhantk

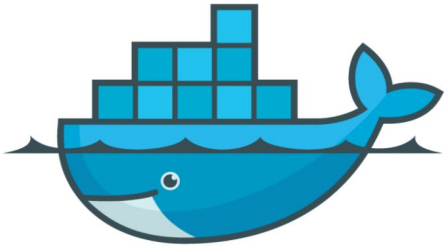
Siddhant Khisty

Community Manager at WeMakeDevs
Loves Tinkering with Computers
Linux and OSS Advocate

What are containers and Why do they matter?

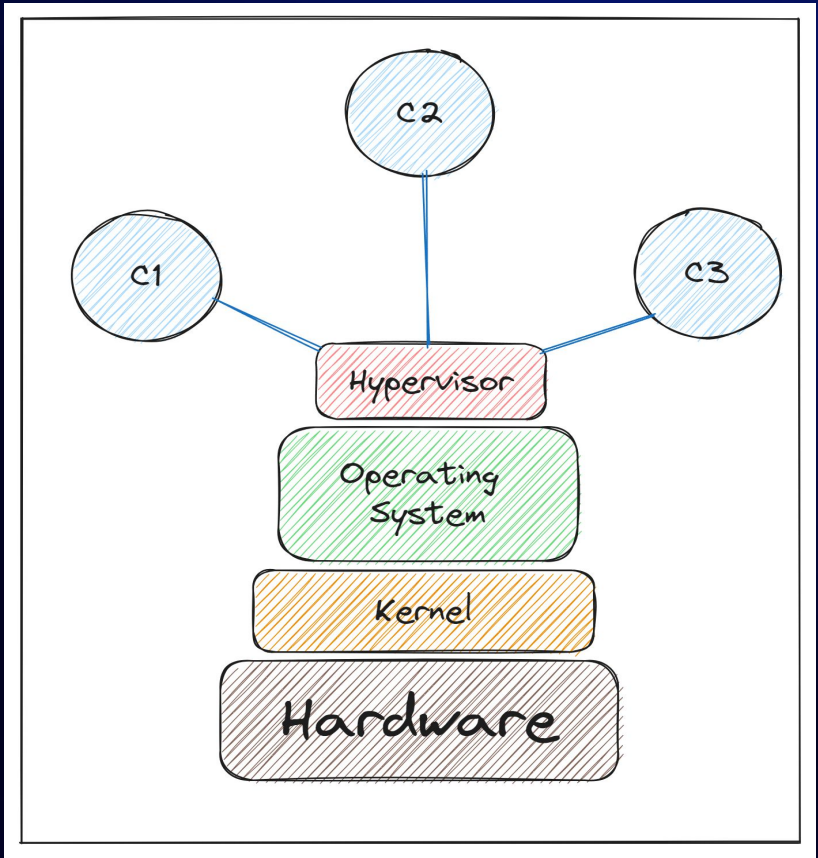

containerd

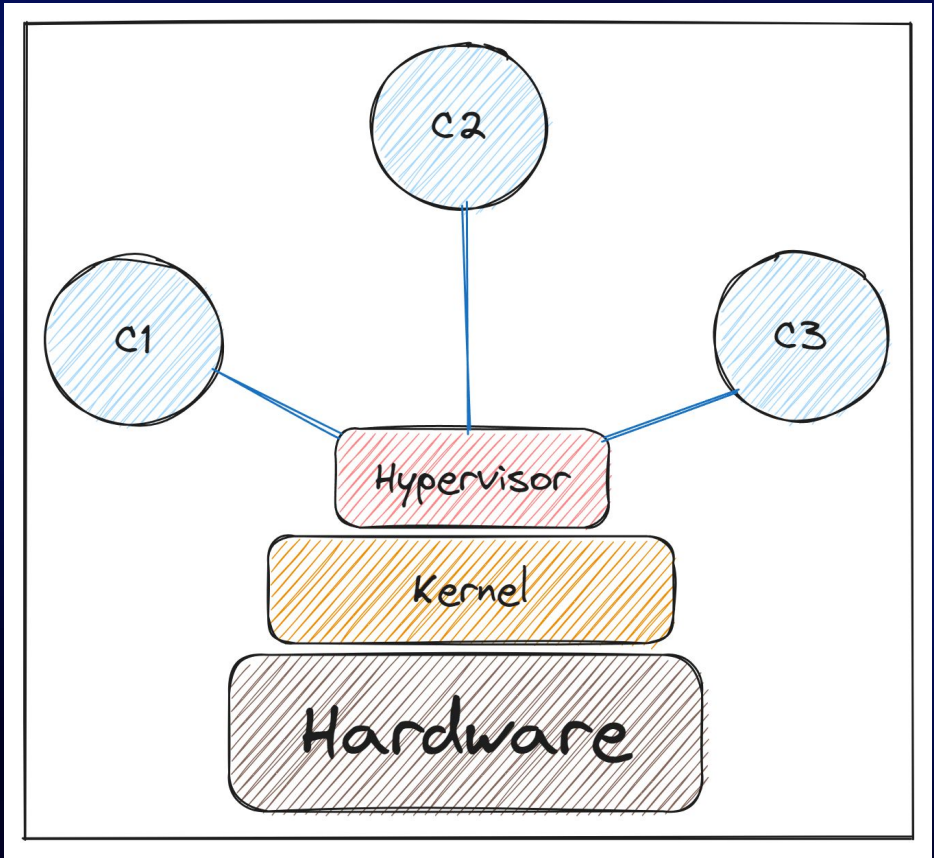


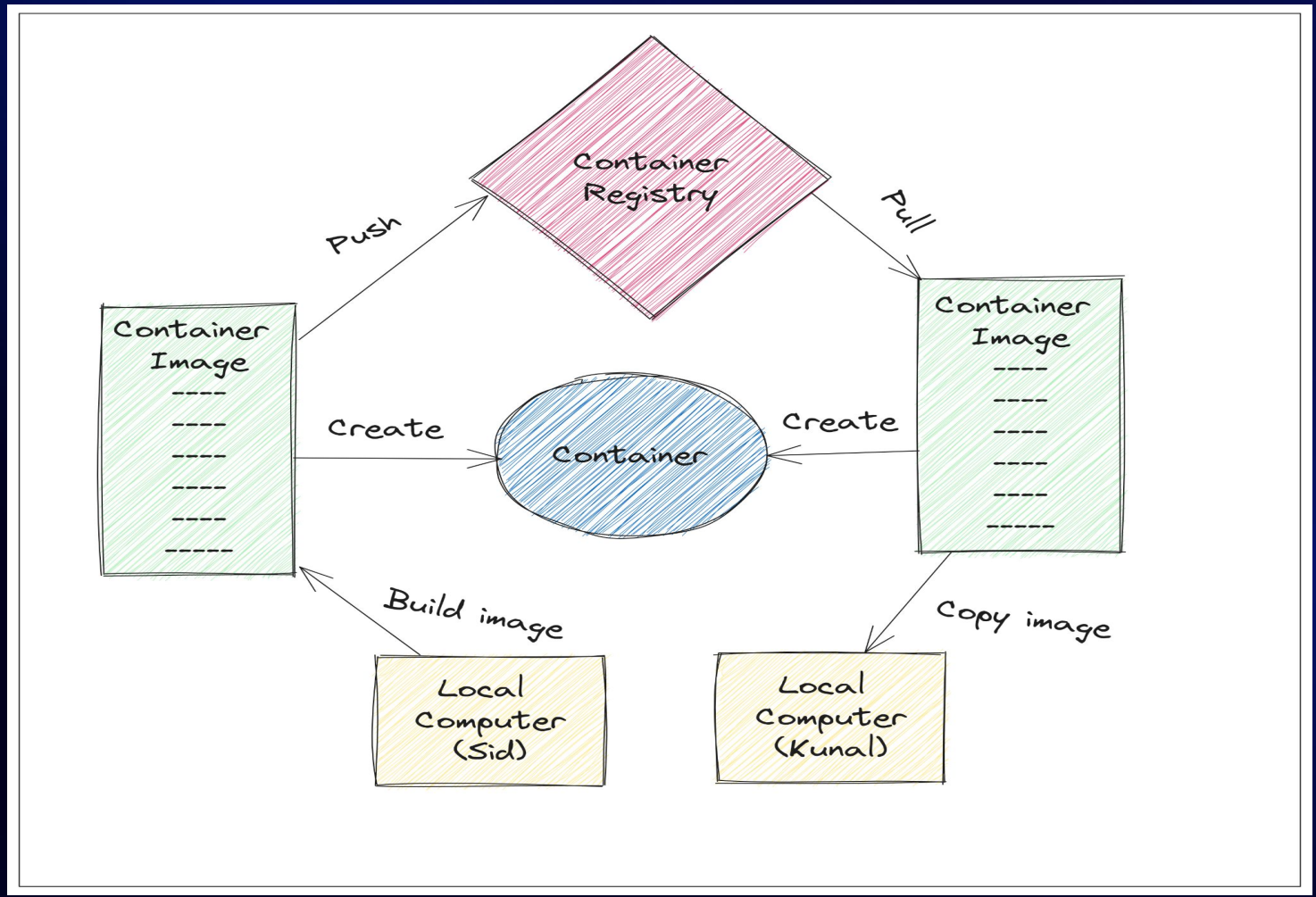



cri-o

Container Architecture






Container Registry
Push
Pull
Container Image
Container Image
Create
Container
Create
Build image
Copy image
Local Computer (Sid)
Local Computer (Kunal)

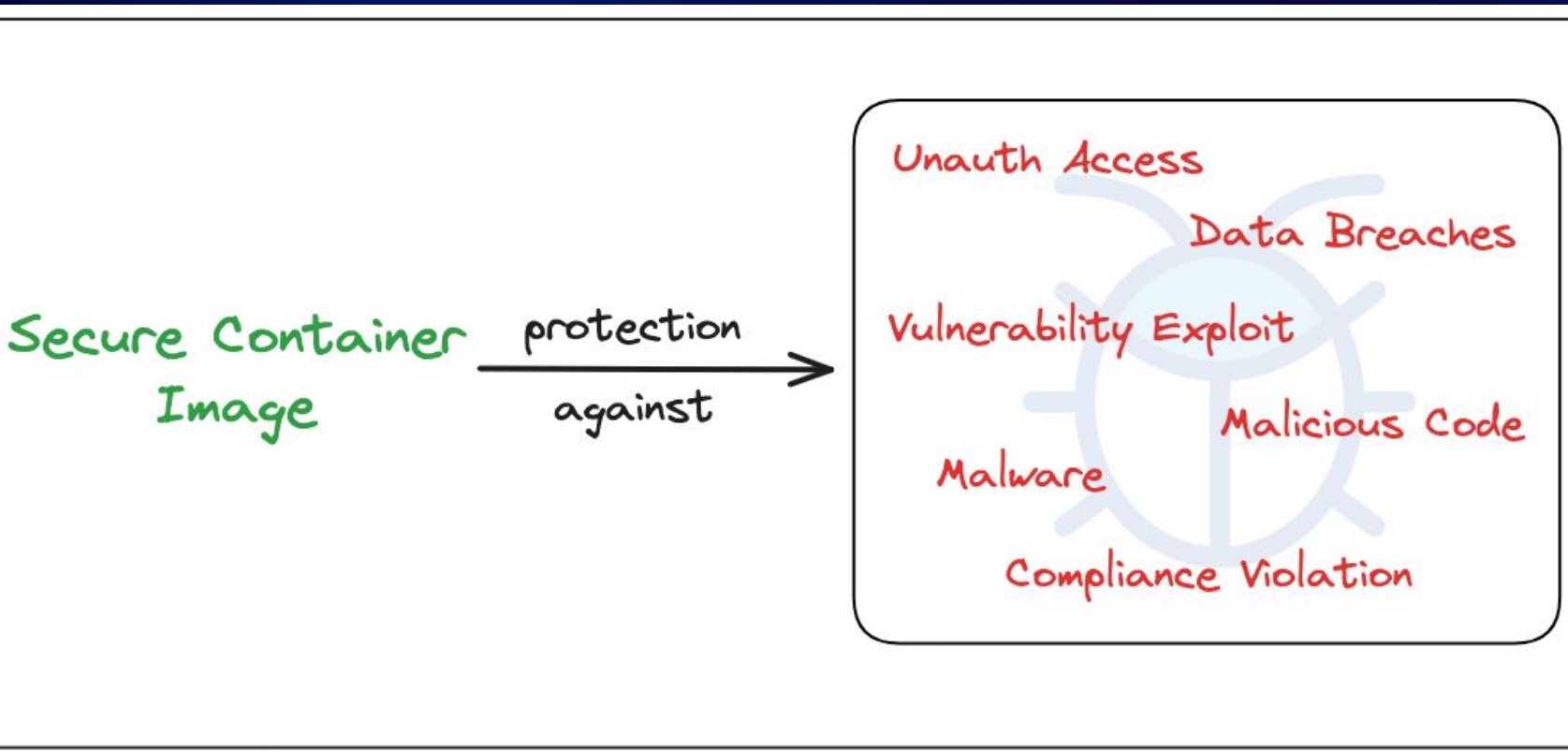
JUNE 27, 2023

DEVSEC CON THE AMERICAS 4

Image Security

Securing Container Images - Why?

- **Goal:** Build a strong foundation
- Images == **Building blocks** of containerised apps
- **Insecure images** lead to:
  - Vulnerabilities
  - Malware
  - Outdated software components


Secure Container Image
protection against
Unauth Access
Data Breaches
Vulnerability Exploit
Malicious Code
Malware
Compliance Violation

How?

JUNE 27, 2023

DEVSEC CON 4

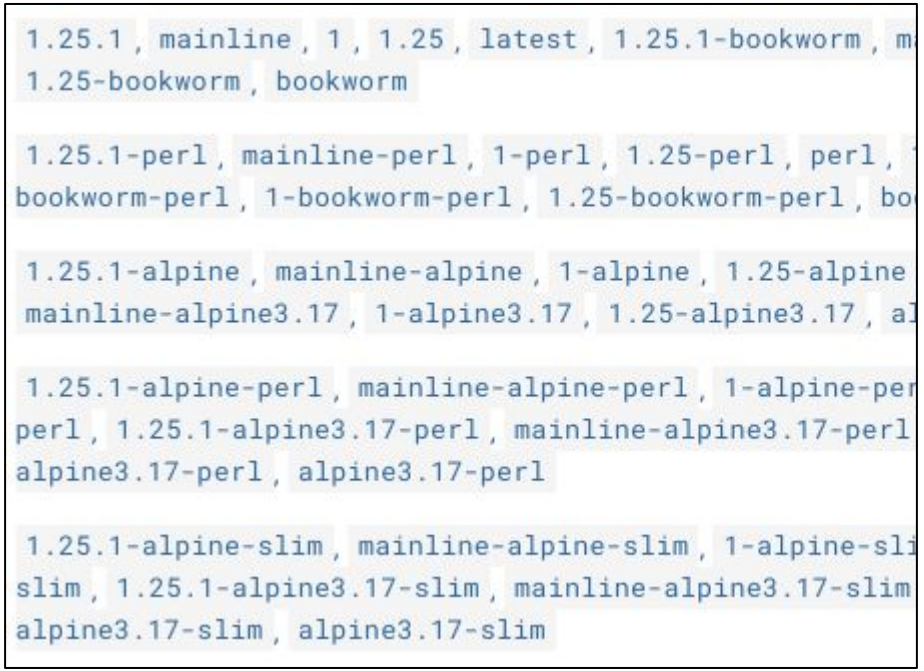
THE AMERICAS

5 Ques. Checklist

Question 1

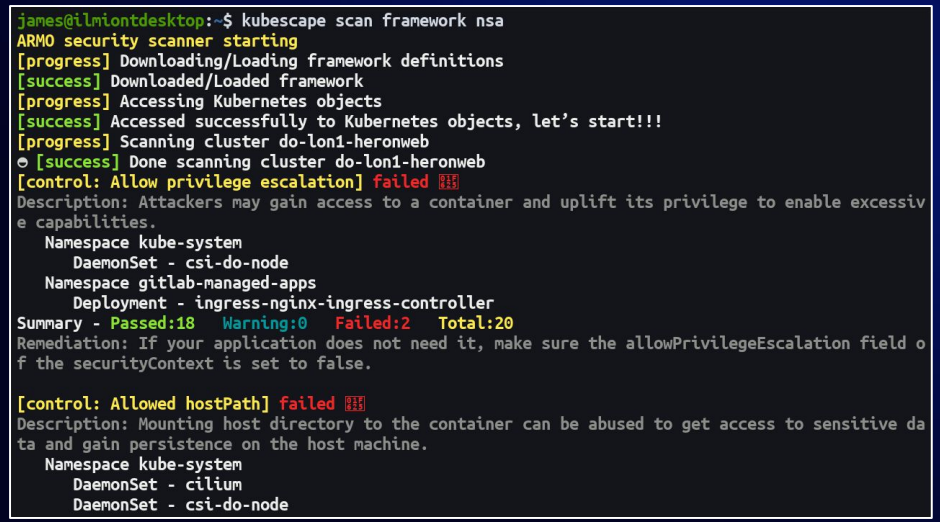
Are the container images up-to-date?

- Use ~~**latest**~~ **stable releases**
- Check for available **security patches** or **updates**



Question 2

Are container images scanned regularly?

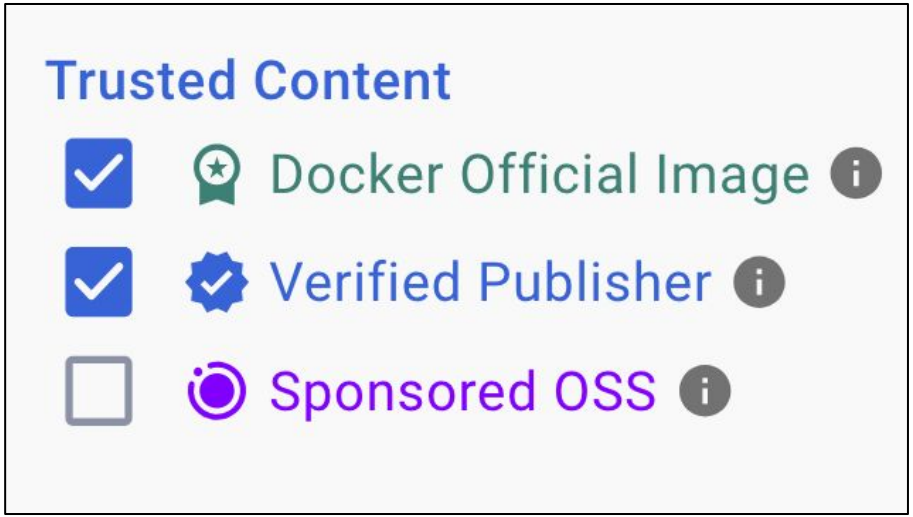


- Scanning for **vulnerabilities** using tools like **Kubescape**
- Process to **address the discovered security issues**

Question 3

Are container images verified?

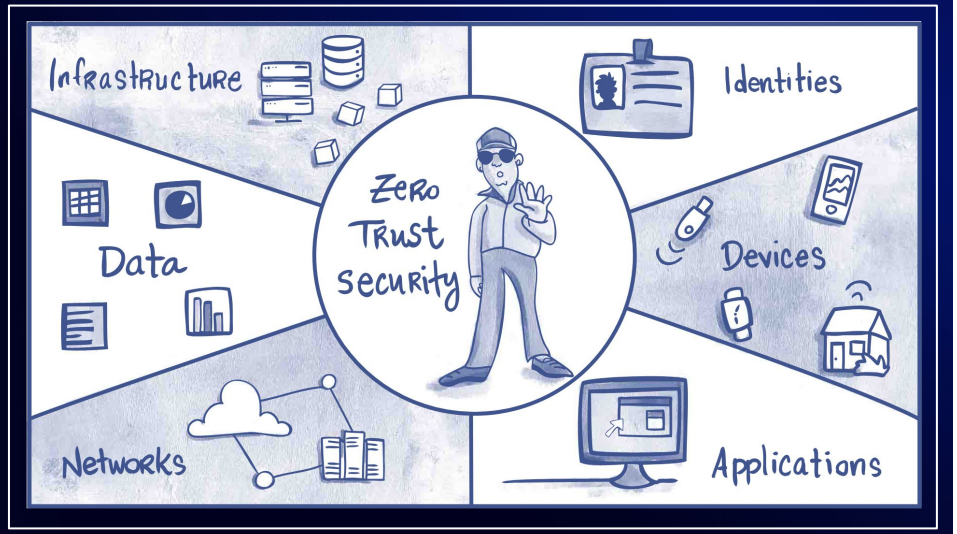
- From **reputable** & **trusted sources**
- Verify **integrity** & **authenticity** (before deploying)



Question 4

Are container images signed?

- Implement **image signing** using tools like **cosign**
- Process to verify **digital signatures** & **ensure integrity**



Question 5

Is a Zero-trust model being implemented?

- Follow a **zero-trust approach**
- Implement strict **access controls** & **auth. mechanisms**

JUNE 27, 2023

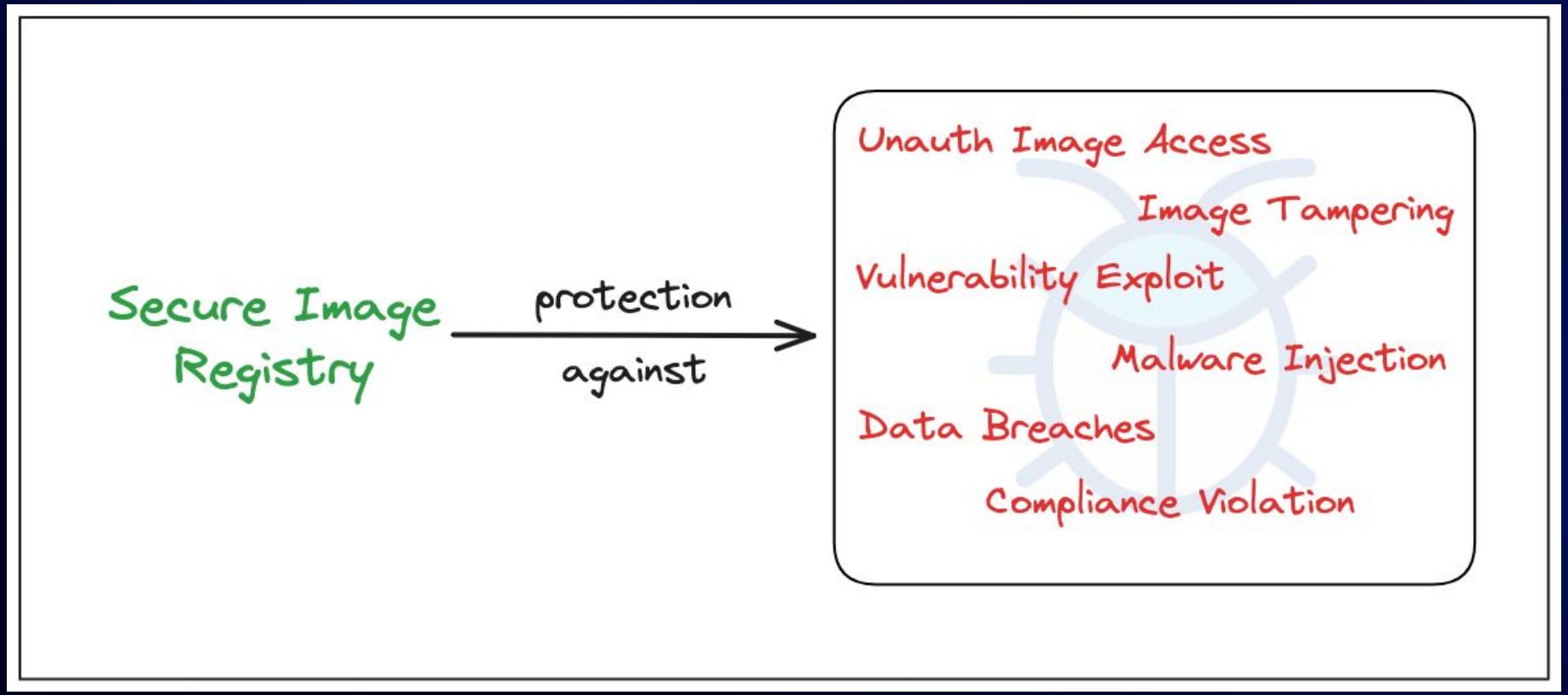
DEVSEC CON 4

THE AMERICAS

Image Registry

Securing Image Registries - Why?

- Secure registry == safeguard from **unauth. access** or **misuse**
- Reduce risk of **deploying compromised images**
- Ensure **compliance** & **trustworthiness**


Secure Image Registry
protection
against
Unauth Image Access
Image Tampering
Vulnerability Exploit
Malware Injection
Data Breaches
Compliance Violation

How?

JUNE 27, 2023

DEVSEC CON 4

THE AMERICAS

4 Ques. Checklist

Question 1

Is the image registry public or private?

- Use **private image registry**
- If public, **assess** the **potential risks** + **implement security measures**

Question 2

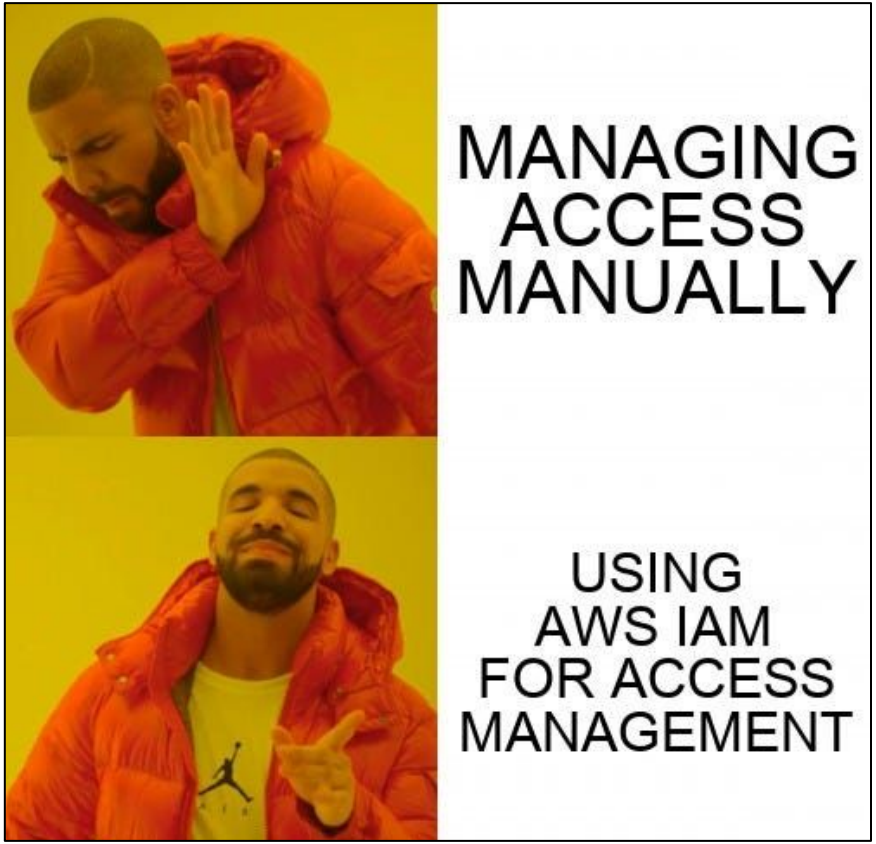
Is the image registry server secure?

- **Restricted network access** to the server
- Regular **patching**, **hardening** & **monitoring**

Question 3

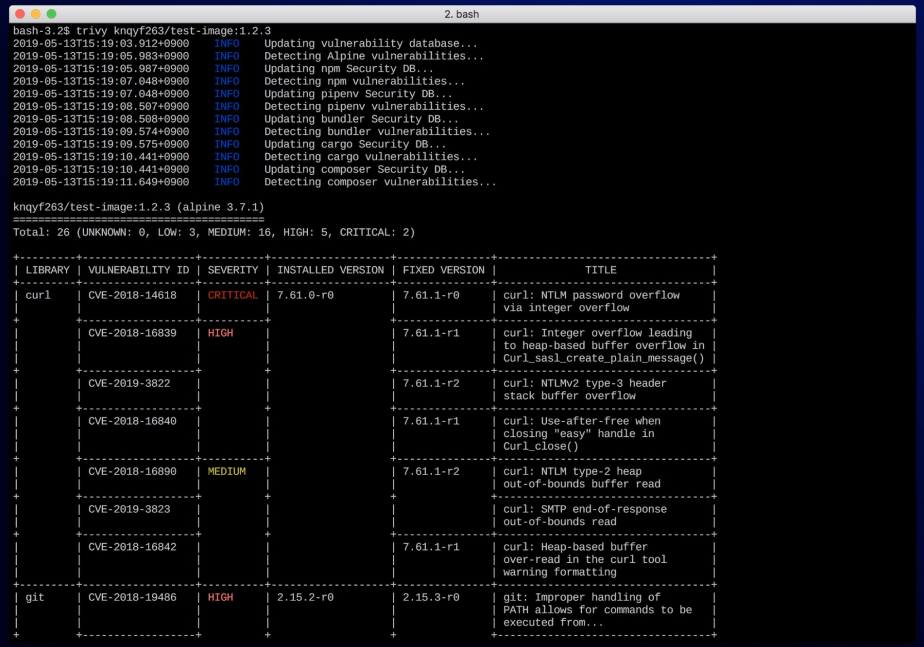
Are access controls properly configured?

- **Granular access controls** for **push**, **pull** & **modify** images
- **Auth. mechanism** to allow **only authenticated users**



Question 4

Are vulnerabilities being monitored?



- **Regularly monitor** stored container images
- Integrate **vulnerability scanning** tools such as **trivy**

JUNE 27, 2023

DEVSEC CON 4 THE AMERICAS

Build Process

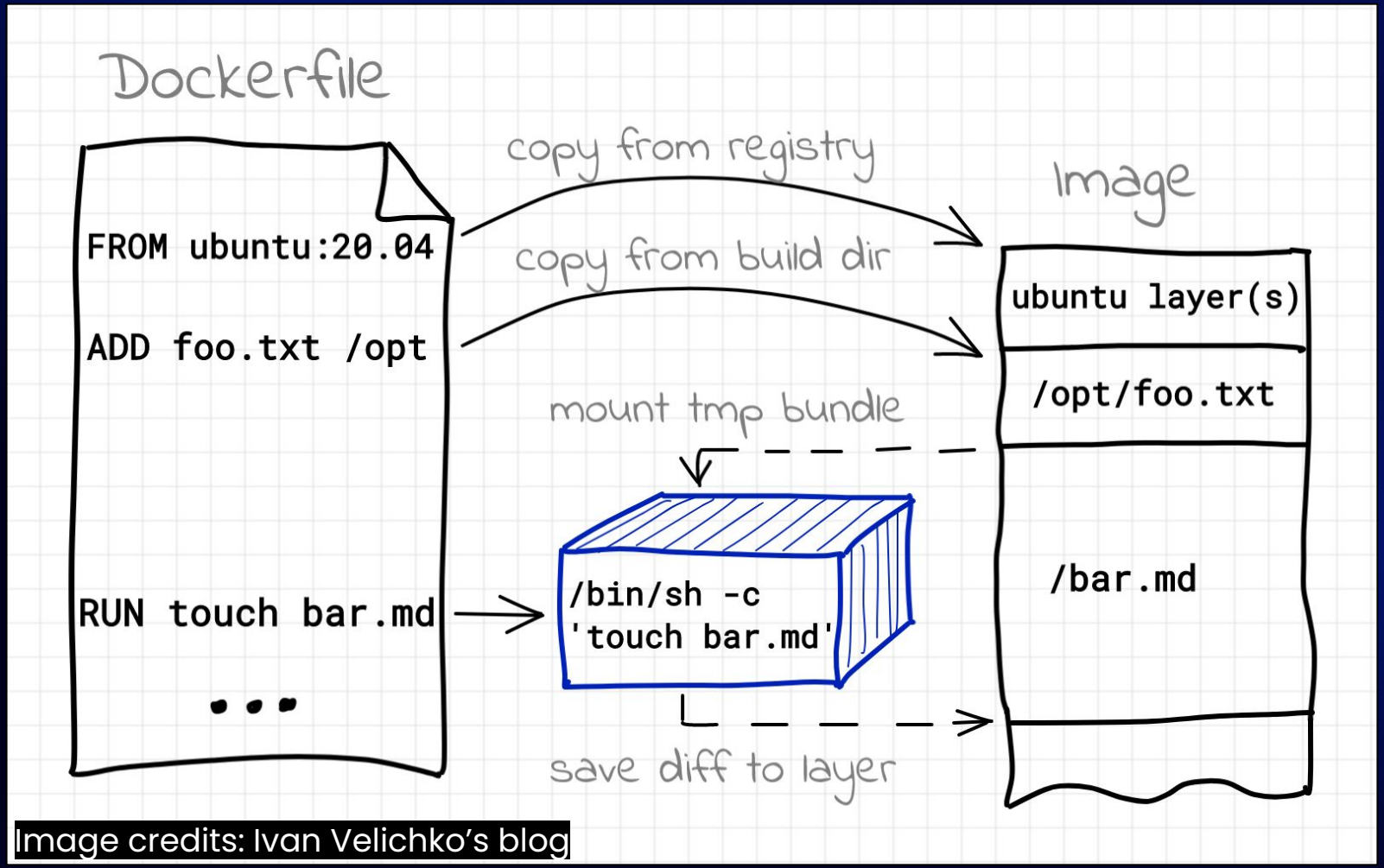


Image credits: Ivan Velichko's blog

The biggest security Red flag

docker-compose.yml

```yaml
version: "alpine"
services:
  web:
    build: .
    container_name: web-container
    privileged: true
    ports:
      - "8080:8080"
  golang:
    image: "golang:alpine"

```

Attackers have a huge playground

- Reduce your attack surface
- Lightweight base images
- Multi-stage builds

```
# Base image Stage 1
FROM ubuntu:16.04 as stage1

RUN apt-get update
RUN apt-get -y install make curl
RUN curl http://xyz.com/abc.tar.gz -O
RUN tar zxf abc.tar.gz && cd abc
RUN make DESTDIR=/tmp install

# Stage 2
FROM alpine:3.10

COPY --from=stage1 /tmp /abc

ENTRYPOINT ["/abc/app"]
```

Why Alpine?

```
ubuntu $ docker image ls
REPOSITORY   TAG        IMAGE ID       CREATED          SIZE
ubuntu       16.04      b6f507652425   22 months ago    135MB
alpine       3.10       e7b300aee9f9   2 years ago      5.58MB
ubuntu $
```

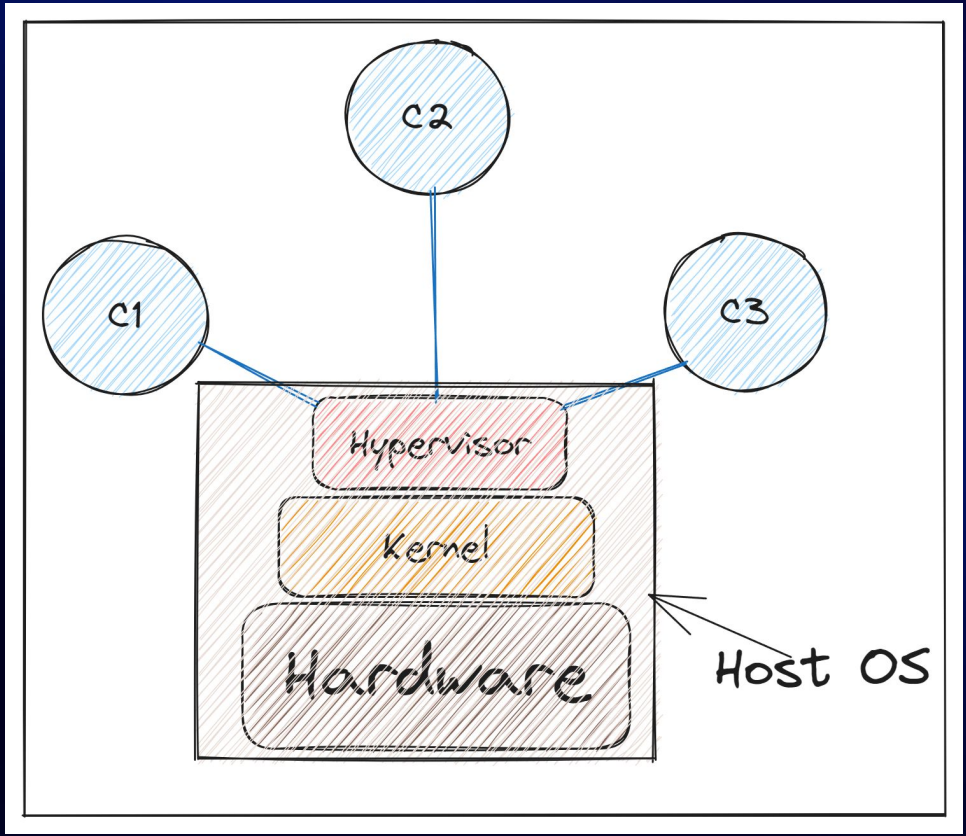
JUNE 27, 2023

DEVSEC CON 4 THE AMERICAS

Secure the Host

The greatest point of failure

Where do containers run?



Lightweight Host OS – Reduce Attack Surface

Set up robust access control

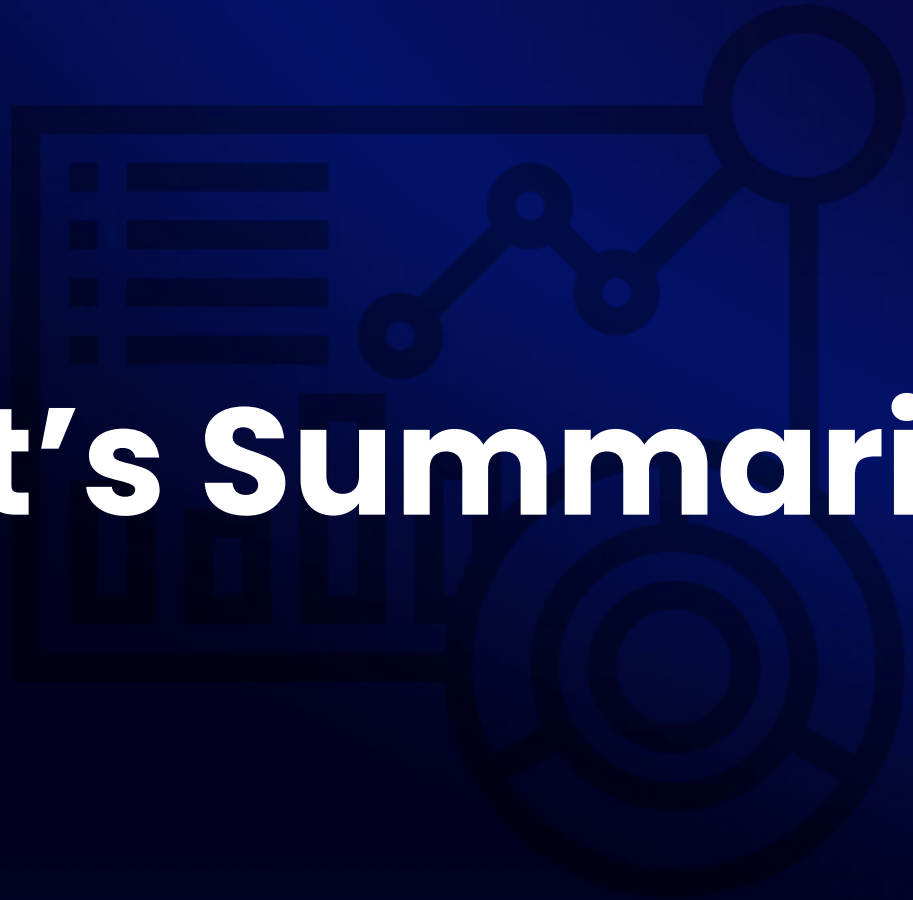
- Use firewalls to block access
- Set robust access control
- Scan for threats regularly


JUNE 27, 2023
DEVSEC CON
THE AMERICAS
Tools

How to Choose?
- Parameters to Consider

- Vulnerability Scanning
- Image integrity & verification
- Runtime protection
- Compliance and Audit Capabilities


Static Vulnerability Analysis
clair
Sysdig Secure - Container Runtime Security
sysdig
Snyk Container - Vulnerability scan + monitoring
snyk
Image Signing
sigstore
cosign
Vulnerability Scanning for Images + Image Registry
Kubescape
by ARMO
Run-time Security
Falco
Vulnerability Scanning
aqua
trivy



JUNE 27, 2023

DEVSEC CON 4

THE AMERICAS

Let’s Summarize!

Takeaways

- [x] Image security
- [x] Registry security
- [x] Secure the build process
- [x] Host Security
- [x] Tools to make life easier

Additional Resources

JUNE 27, 2023

DEVSECCON THE AMERICAS 4

Thank You

Kunal Verma

Community Manager at Kubesimplify

@kverma_twt

Siddhant Khisty

Community Manager at WeMakeDevs

@i_siddhantk