What Are You Willing to Digest?

Multi-Arch Container Image Security

Understanding the snowflake risk surfaces of multi-architecture setups and automating security across pipelines.

Evans Yeboah Jr.

Security @ EliseAI

What are Containers?

But who handles all these containers?

The ease of multi architecture container images can’t be matched

and neither can their security problems!

Containers make your life easier

But what are they doing to your host?

Packages, based on the platform can contain hidden issues when unscanned, exposing your to a variety of vulnerabilities

So let’s walk through an example

Simple Image

```
evansyeboahjr.@Evanss-MacBook-Air presentation_files % cat Dockerfile
FROM debian:bullseye-slim

RUN apt-get update && \
    apt-get install -y libexpat1=2.2.10-2+deb11u5
```

Install simple XML reading package

Build for amd64 & arm64 platforms

```
evansyeboahjr.@Evanss-MacBook-Air presentation_files % docker buildx build --platform linux/arm64
 -t poc:arm64 --load .
```

```
evansyeboahjr.@Evanss-MacBook-Air presentation_files % docker buildx build --platform linux/amd64
 -t poc:amd64 --load .
```

Using grype for vulnerability analysis

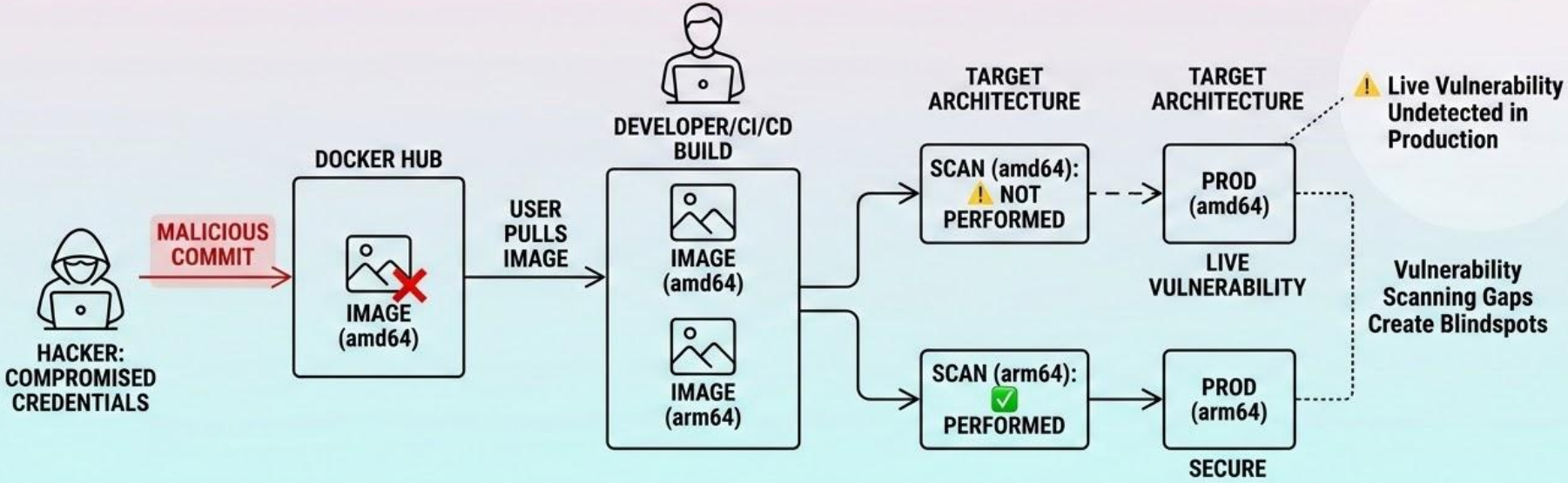
```
evansyeboahjr.@Evanss-MacBook-Air presentation_files % grype poc:arm64 > arm64.txt
```

```
evansyeboahjr.@Evanss-MacBook-Air presentation_files % grype poc:amd64 > amd64.txt
```

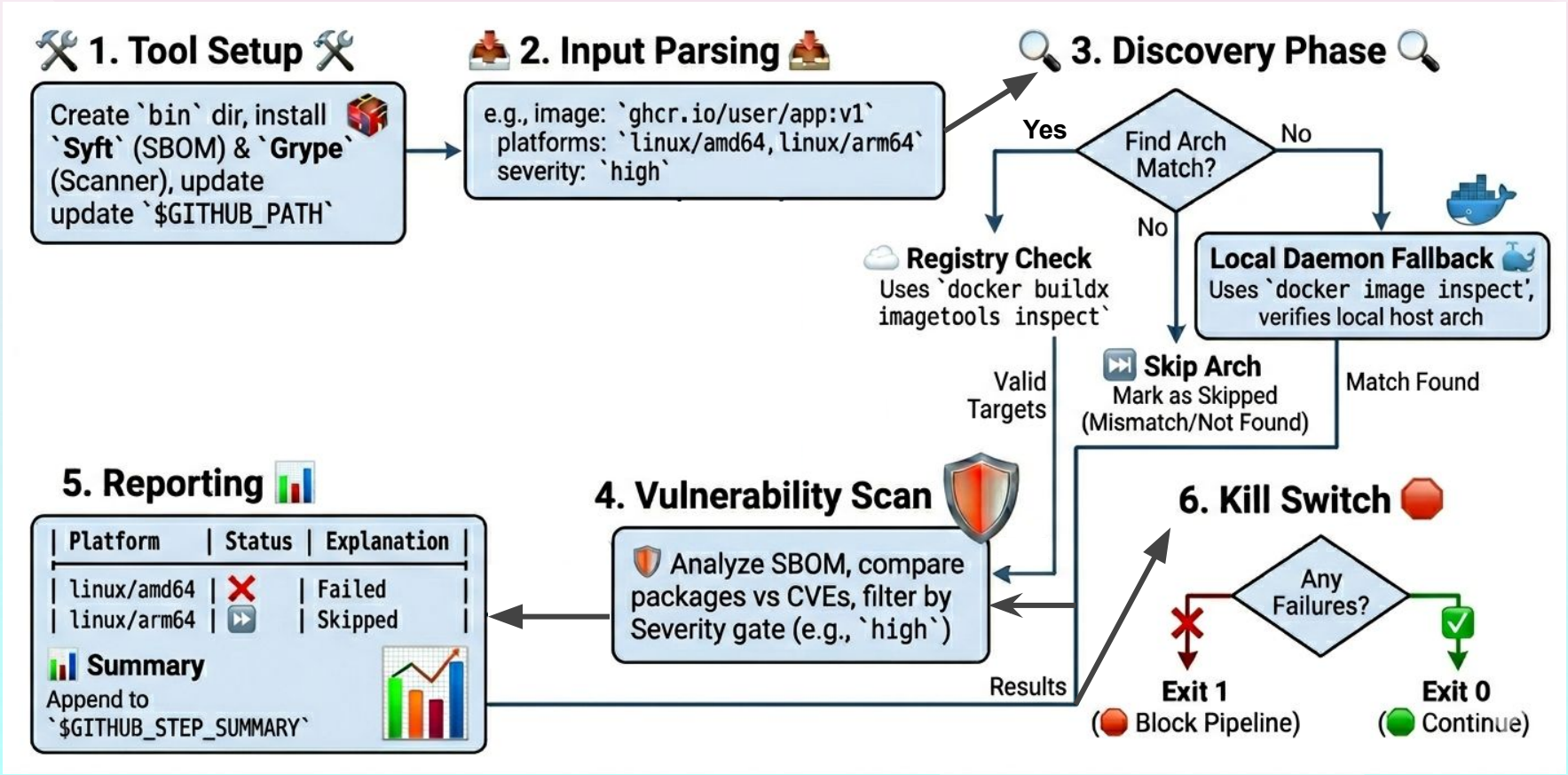
And a quick diff

```
evansyeboahjr.@Evanss-MacBook-Air presentation_files % diff arm64.txt amd64.txt
85c85
< coreutils             8.32-4                  (won't fix)       deb   CVE-2016-2781
---
> coreutils             8.32-4+b1               (won't fix)       deb   CVE-2016-2781
135c135
< coreutils             8.32-4                                    deb   CVE-2025-5278
---
> coreutils             8.32-4+b1                                 deb   CVE-2025-5278
158c158
< coreutils             8.32-4                                    deb   CVE-2017-18018
---
> coreutils             8.32-4+b1                                 deb   CVE-2017-18018
```

So what’s the big deal?


HACKER: COMPROMISED CREDENTIALS
MALICIOUS COMMIT
DOCKER HUB
IMAGE (amd64)
USER PULLS IMAGE
DEVELOPER/CI/CD BUILD
IMAGE (amd64)
IMAGE (arm64)
TARGET ARCHITECTURE
SCAN (amd64): ⚠ NOT PERFORMED
SCAN (arm64): ✅ PERFORMED
TARGET ARCHITECTURE
PROD (amd64)
LIVE VULNERABILITY
PROD (arm64)
SECURE
⚠ Live Vulnerability Undetected in Production
Vulnerability Scanning Gaps Create Blindspots

Multi Architecture Image Scan - GitHub Action



aqua trivy

KICS by Checkmarx

LiteLLM

TANSTACK

MISTRAL AI_

AXIOS

OpenSearch

Ongoing Supply Chain Attack

Thank You!

Multi Arch Scan Action

LinkedIn