Manjul Solanke

Improving Container Security in Kubernetes with Trivy

Agenda

Introduction

- What is vulnerability?
- Why is vulnerability scanner is necessary?
- Where to look for Kubernetes Vulnerabilities?
- State of Container and K8s security.

About Trivy

- What is Trivy?
- Trivy : Targets and Scanners
- Demo

What is Vulnerability

vulnerability refers to a weakness or flaw in a system or application that can be exploited by attackers to gain unauthorized access, steal data, or cause harm. Vulnerabilities can be the result of **programming errors, design flaws, or misconfigurations in software** or hardware systems.

Software vulnerabilities

Overview

About the CVE Program

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities.

Vulnerabilities

- Known vulnerabilities
  - ID assigned
- Unknown vulnerabilities
  - Your code
  - Undisclosed

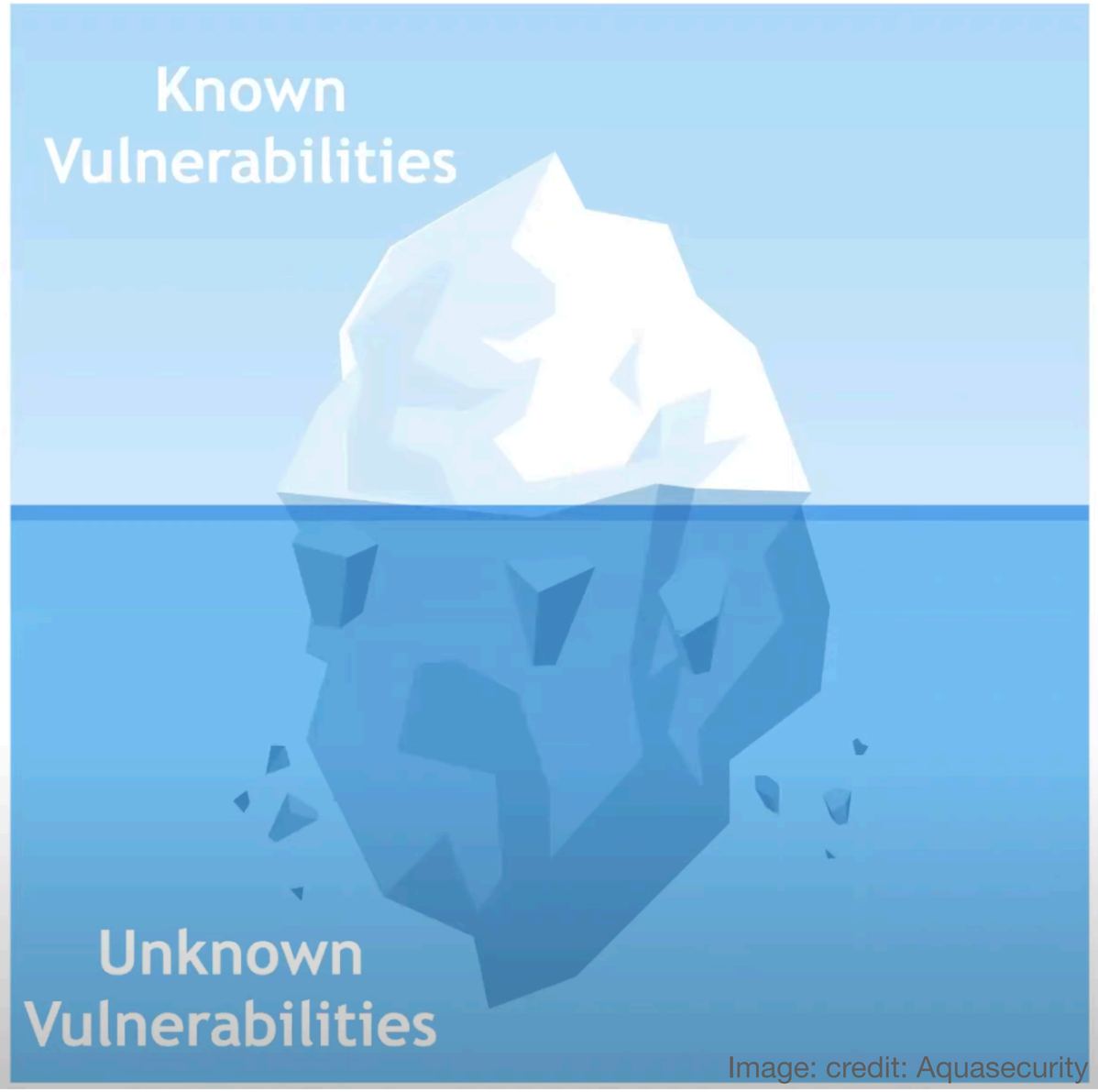


Image: credit: Aquasecurity

Vulnerabilities

- Known vulnerabilities
  - Scanner identifying components with known vulnerabilities
  - e.g. Trivy, Clair, Aqua
- Unknown vulnerabilities
  - Web application vulnerability scanners, fuzzing tools
  - e.g. OWASP ZAP, OSS-Fuzz

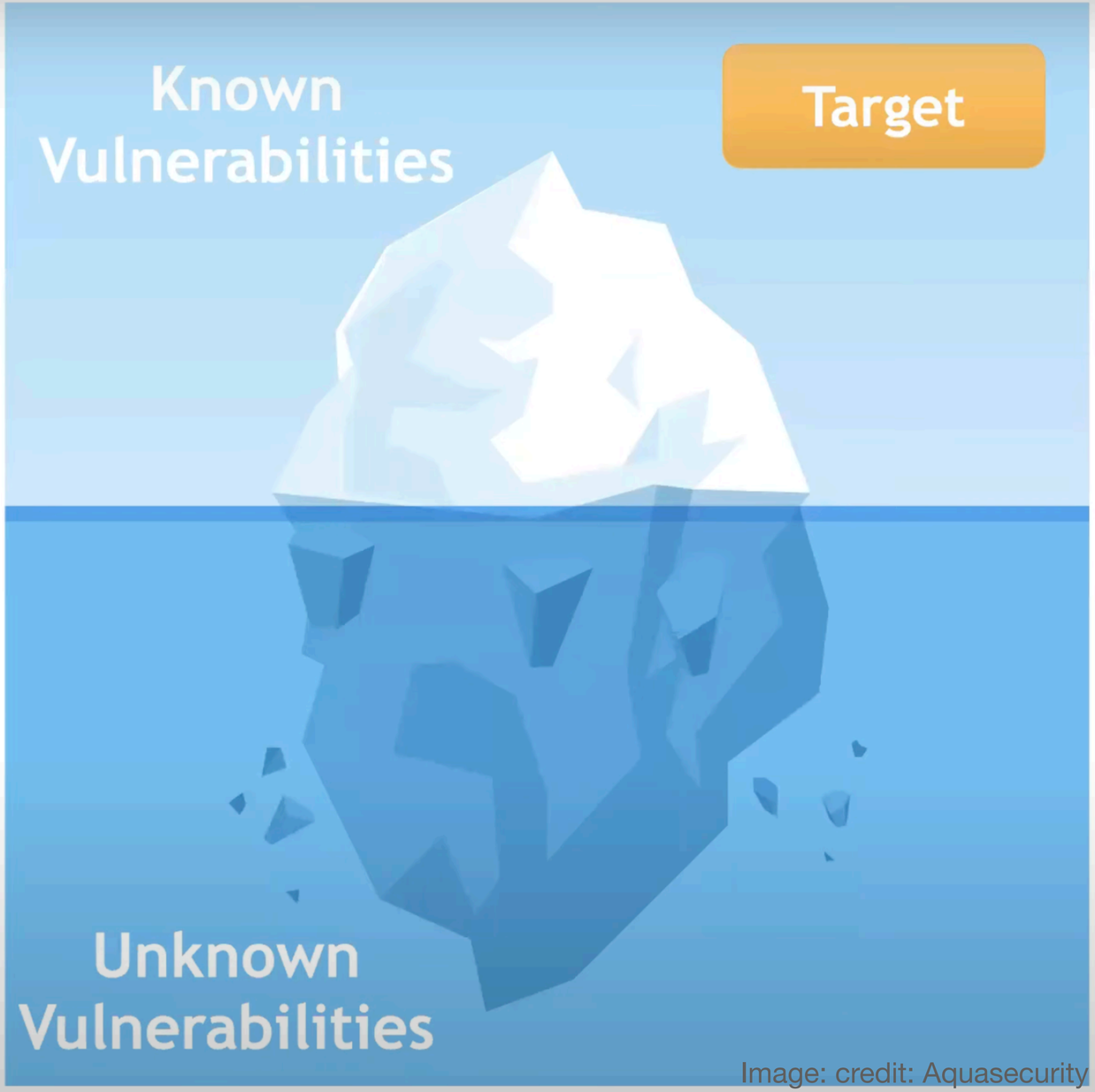


Image: credit: Aquasecurity

Containers, images and vulnerabilities

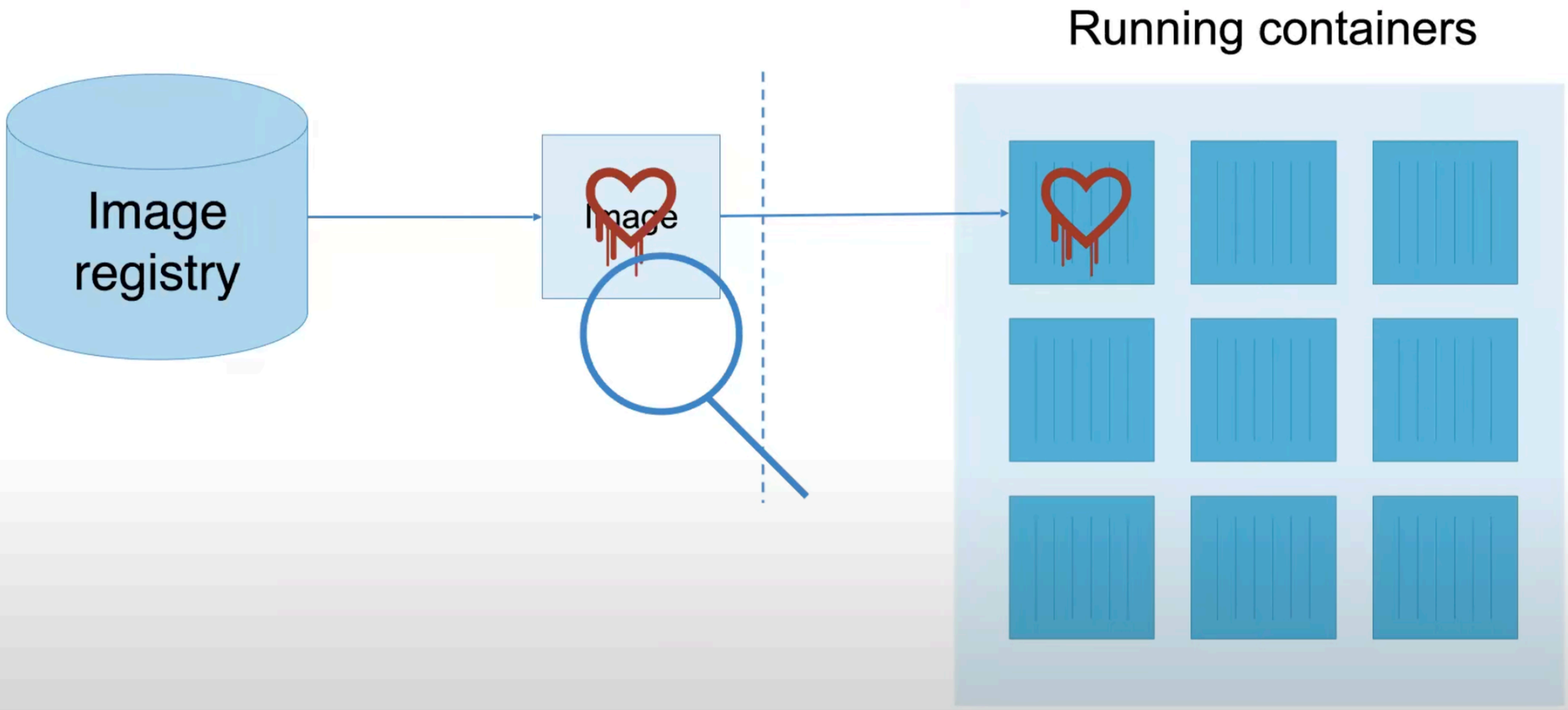


Image: credit: Aquasecurity

Key findings

- Kubernetes continued to cement itself as a critical infrastructure component in the modern software stack.

- According to Red Hat's "2022 state of Kubernetes security report", 93% of those surveyed last year reported at least one incident impacting a Kubernetes environment.

- Out of the total security incidents reported, 53% were due to misconfigurations, and 38% were due to the exploitation of vulnerabilities.

Key findings

53%
Detected a misconfiguration in Kubernetes in last 12 months

57%
Worry the most about securing workloads at runtime

51%
Require developers to use validated images

78%
Have a DevSecOps initiative in either beginning or advanced stages

43%
Consider "DevOps" as the role most responsible for Kubernetes security

55%
Delayed or slowed down application deployment due to security concern

Manjul Solanke

Where to look for Kubernetes Vulnerabilities?

Here is the list of sources to look for Kubernetes vulnerabilities:

CVE MITRE database

Kubernetes official CVE feed

CVE Details

Github Security Advisories

Trivy

- The most widely used open source security scanner is Trivy, which is reliable, quick, and simple to use. Discover weaknesses and **IaC setup** errors using Trivy, as well as **SBOM discovery**, **Cloud scanning, Kubernetes security issues, and more.**
- Trivy is Open Source Vulnerability Scanner.
- 16.4K stars on Github

aqua trivy

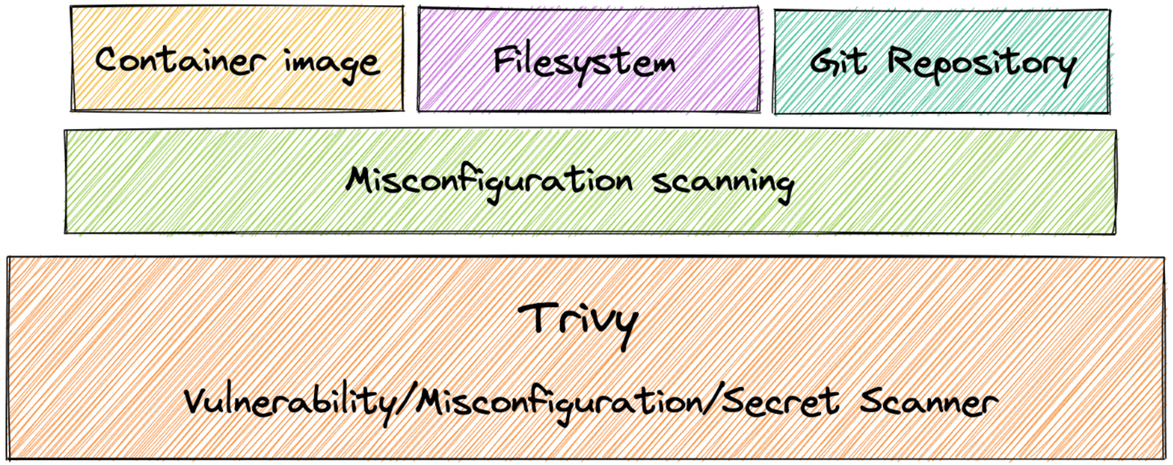
Targets and Scanners

Targets (what Trivy can scan):

- Container Image
- Filesystems
- git Repository
- VM
- Kubernetes
- AWS

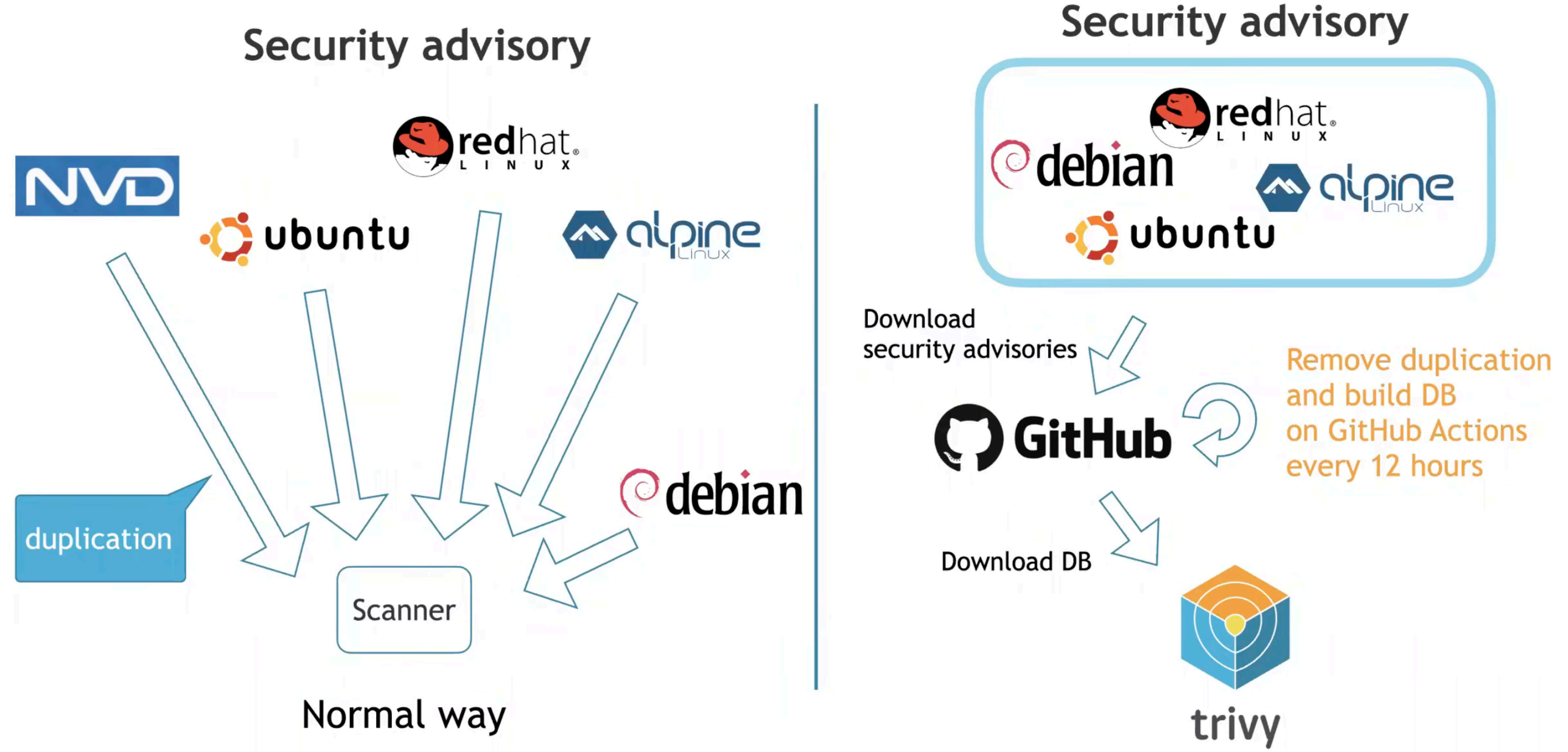
Scanners (what Trivy can find there):

- Known Vulnerabilities (CVEs)
- IaC issues and misconfigurations
- Sensitive information and Secrets
- Software licenses
- SBOM



Detect comprehensive vulnerabilities

- System Package Manager
  - apt
  - yum
  - apk
- Application Package Manager
  - Bundler
  - Composer
  - Pipenv
  - Poetry
  - npm
  - yarn
  - Cargo



Manjul Solanke

Image: credit: Aquasecurity

Demo -

https://github.com/manjulsolanke/trivy-demo/blob/main/README.md

Thank You

Manjul Solanke