SOSS
Community
Day India , 2024

Automating Container Security: Docker Scout in CI/CD for Safer Software Supply Chains.

Presentation by
Pradumna Saraf

$ whoami

Pradumna Saraf

- Dev Advocate
- Open Source Developer
- Docker Captain
- Create Content

"Docker Images are **SECURE** by default"

Container

"~~Docker~~ Images are **SECURE** by default"

Container

"~~Docker~~ Images are **SECURE** by default"

"Open Source softwares are SECURE"

Container

"~~Docker~~ Images are **SECURE** by default"

"Open Source softwares are SECURE"

Those are misconceptions

Shifting Testing LEFT Into Development Workflow.

and Security

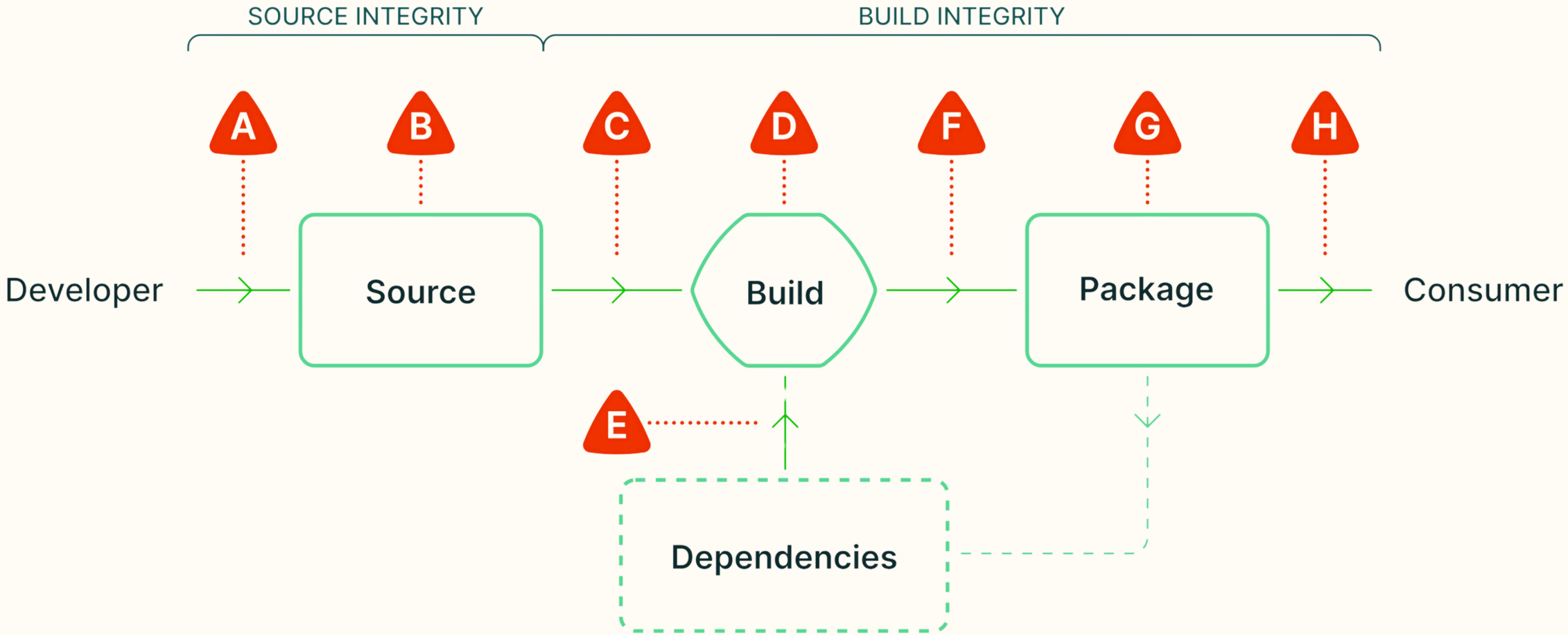
Shifting Testing^LEFT Into Development Workflow.

SLSA - Threat Model

SLSA - Threat Model

("salsa")

Source: https://github.com/slsa-framework/slsa



A Submit unauthorized change

B Compromise source repo

C Build from modified source

D Compromise build process

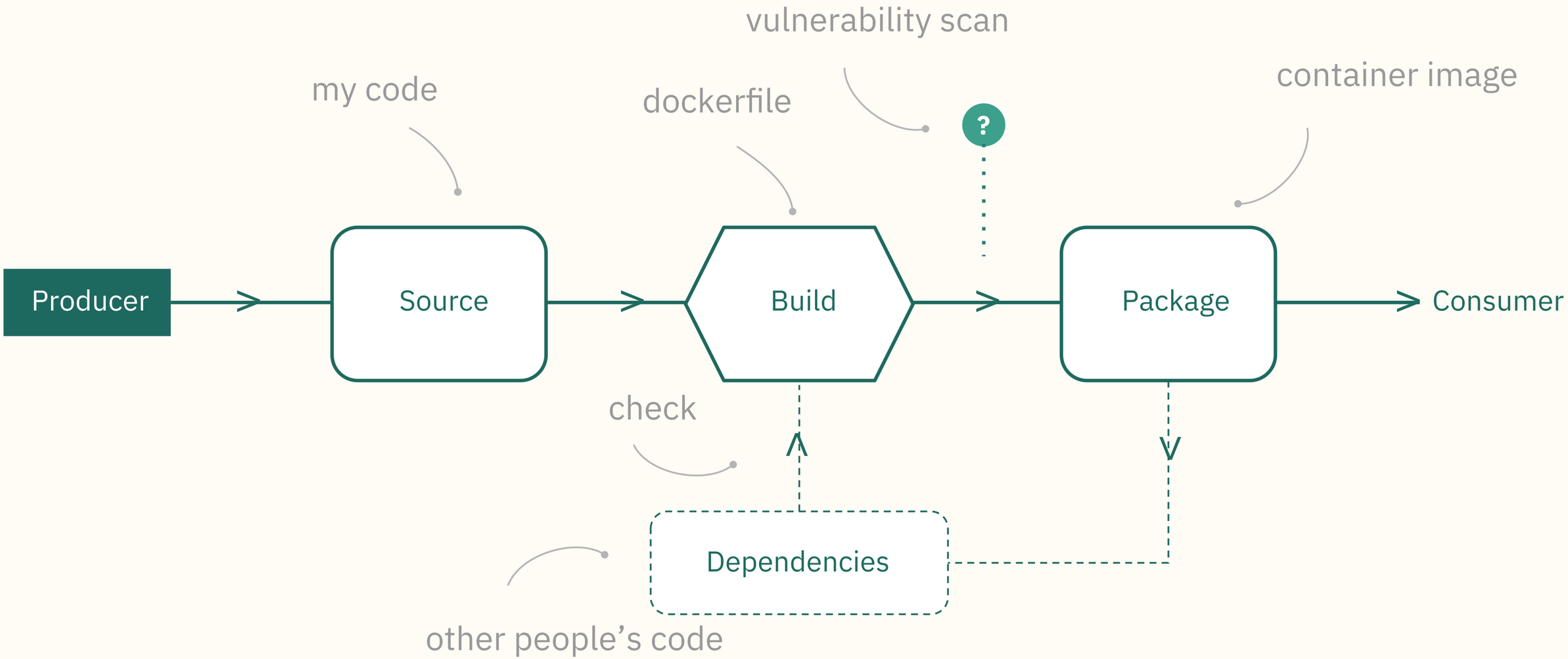
E Use compromised dependency

F Upload modified package

G Compromise package repo

H Use compromised package

Source: https://slsa.dev/spec/v0.1/threats



Source: Docker team

Enter docker scout

Enter docker scout

- Compiles an inventory of components, also known as a Software Bill of Materials (SBOM). The SBOM is matched against a continuously updated vulnerability database to pinpoint security weaknesses.

Source: https://docs.docker.com/scout

Enter docker scout

- Compiles an inventory of components, also known as a Software Bill of Materials (SBOM). The SBOM is matched against a continuously updated vulnerability database to pinpoint security weaknesses.

- It’s a standalone service and platform that you can interact with using Docker Desktop, Docker Hub, the Docker CLI, and the Docker Scout Dashboard. Docker Scout also facilitates integrations with third-party systems, such as container registries and CI platforms.

Source: https://docs.docker.com/scout

Demo

https://github.com/Pradumnasaraf/soss-scout-demo

Connect With Me

links.pradumnasaraf.dev

Pradumna Saraf

Who is Pradumna Saraf ?