

Container Infrastructure Analysis with Trivy



Zach Roof

Lead Security Engineer

@zachroofsec www.zachroofsec.com





trivy

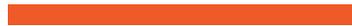




trivy

Primary Maintainer:

Teppei Fukuda



**A Simple and Comprehensive Vulnerability Scanner for
Containers, Suitable for CI**





Detects vulnerabilities within:

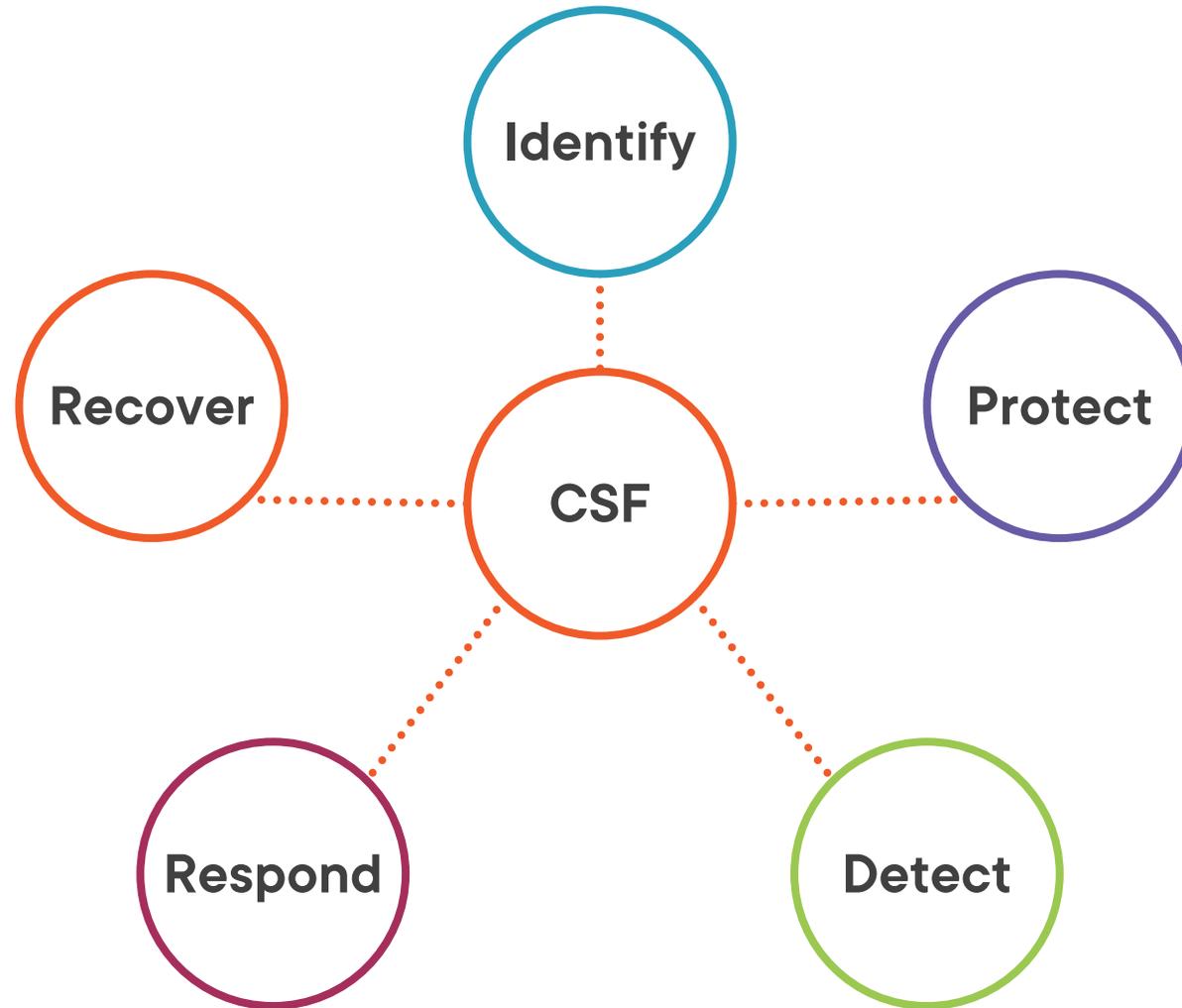
- OS Packages
- Application Dependencies

Fast

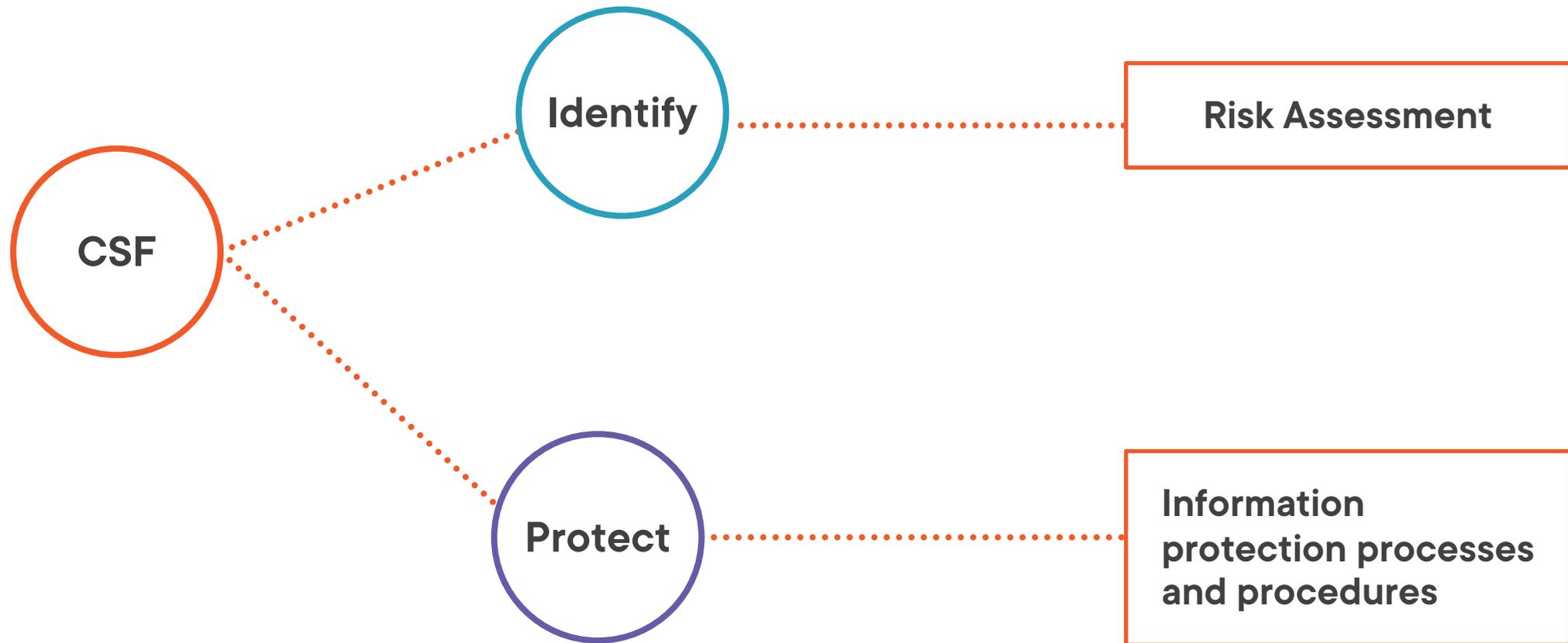
Build Integration



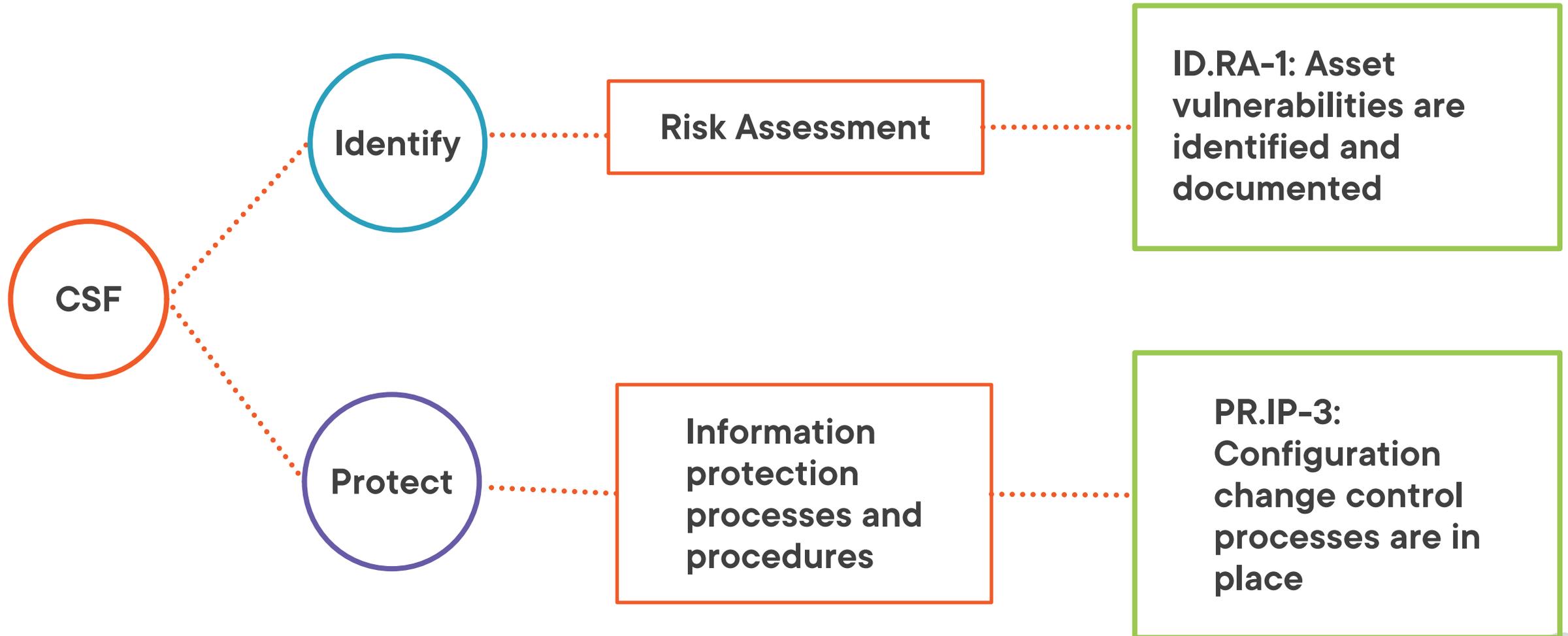
NIST Cybersecurity Framework (Core)



NIST Cybersecurity Framework



NIST Cybersecurity Framework



MITRE ATT&CK

Data Analysis Type

Network Analysis

Infrastructure Analysis

Application Analysis

OS Analysis

File Analysis

Threat Intelligence

Incident Management



MITRE ATT&CK

Data Type

Network Analysis

Infrastructure Analysis

Application Analysis

OS Analysis

File Analysis

Threat Intelligence

Incident Management

T1195:

Supply Chain Compromise

T1525:

Implant Container Image



MITRE SHIELD

T1195:

Supply Chain Compromise

DTE0014 - Decoy Network: A defender can install any suspect hardware or software on an isolated system or network and monitor for non-standard behaviors. (DUC0020)

T1525:

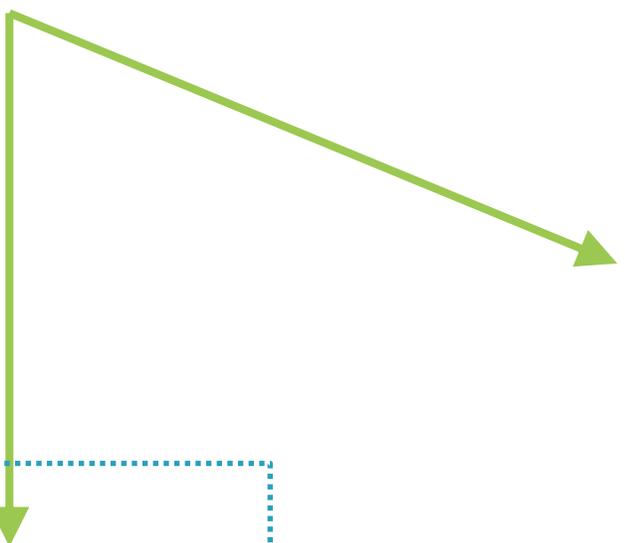
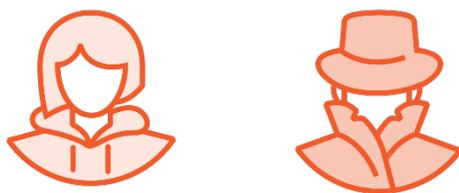
Implant Container Image

DTE0007 - Behavioral Analytics: A defender can monitor user interactions with images and containers to identify ones that are added or altered anomalously. (DUC0168)

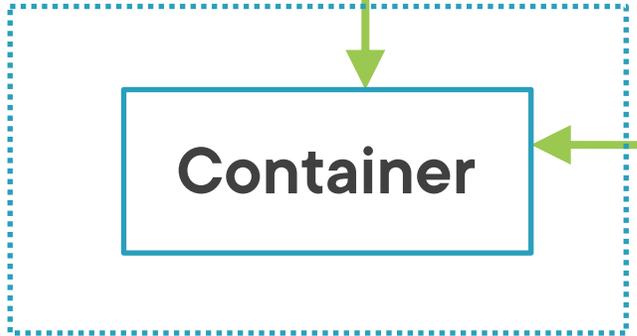


Architecture

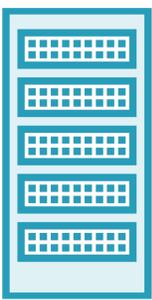
Attackers



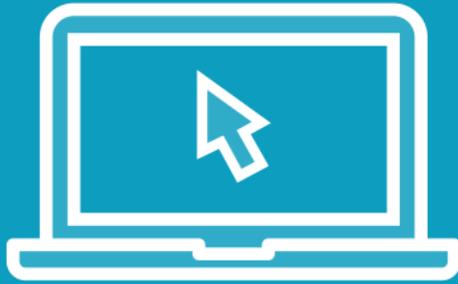
Server



Docker Image Registry



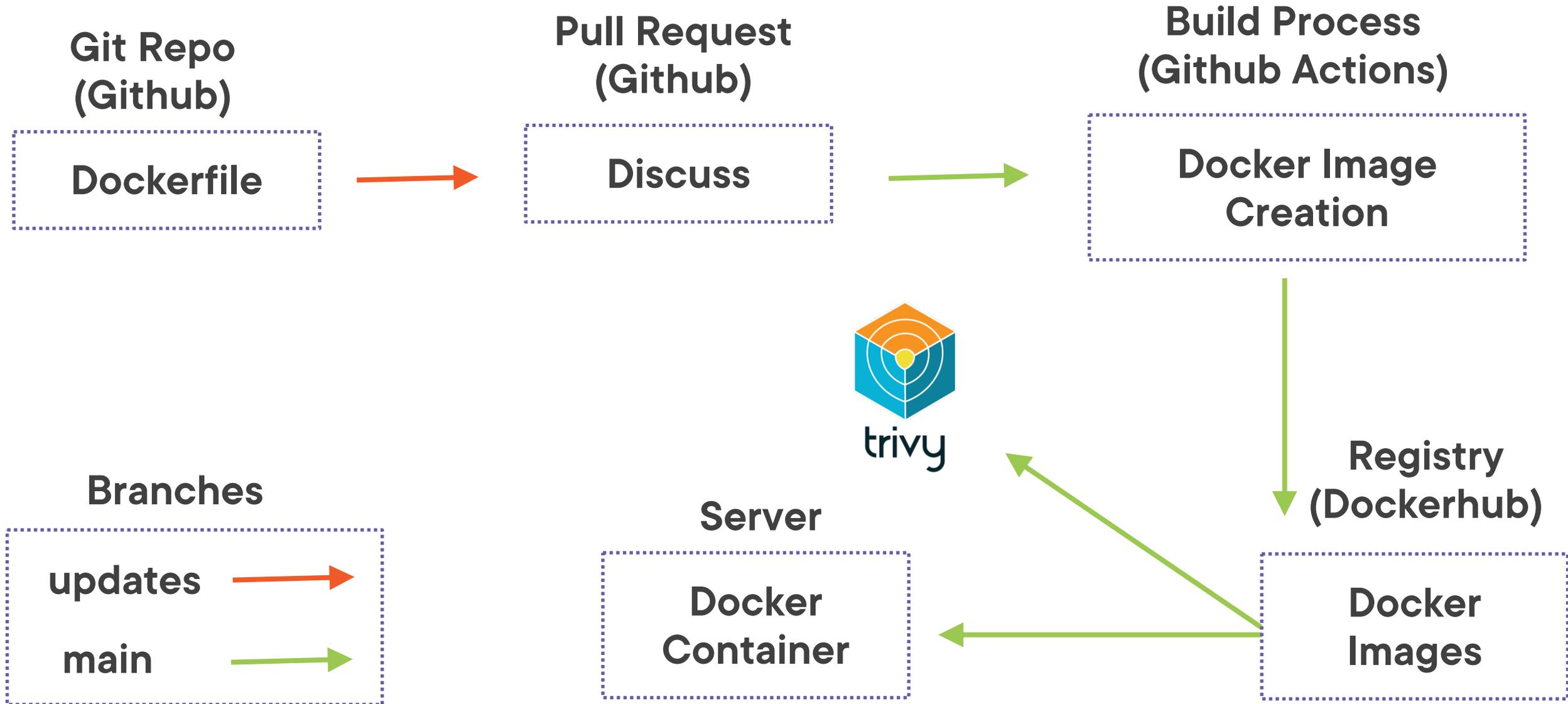
Demo



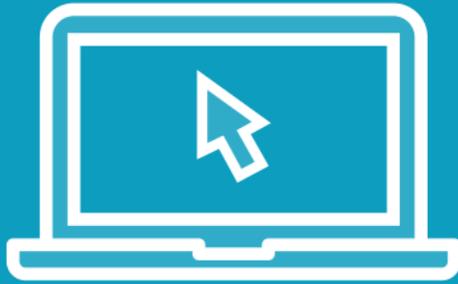
- Review a “reactive” Trivy workflow
- Explore Trivy’s command line flags
- Use Trivy to scan a Docker Image



Docker Build Workflow: Reactive



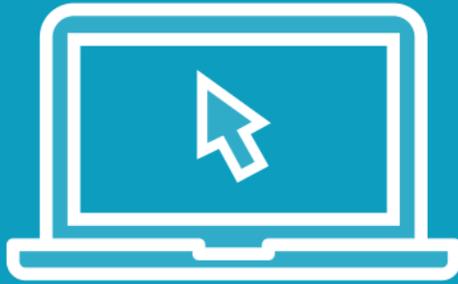
Demo



- Review a “reactive” Trivy workflow
- Explore Trivy’s command line flags
 - severity
 - ignore-unfixed
- Use Trivy to scan a Docker Image
 - Found Heartbleed vulnerability
- Workflow cons
 - Reactive



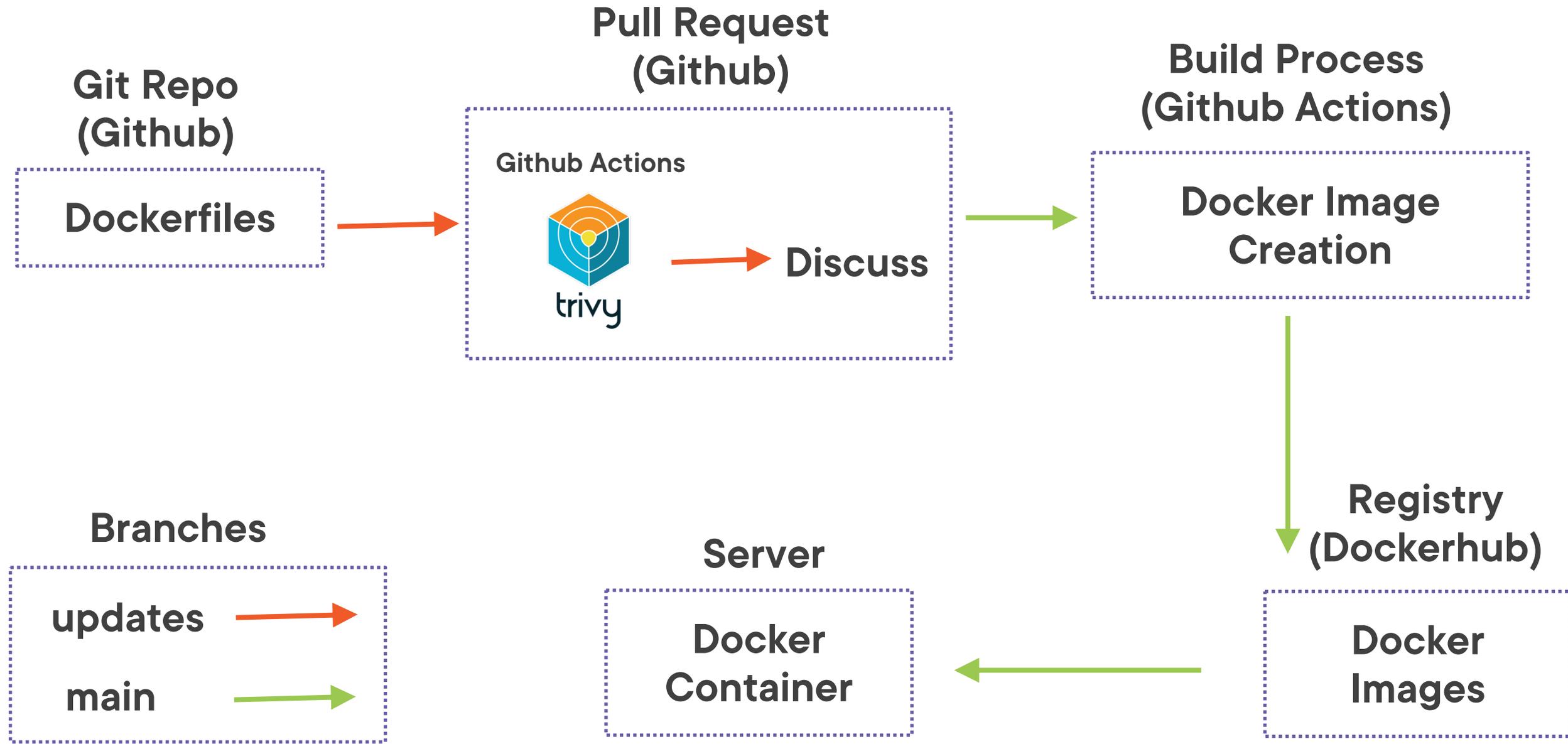
Demo



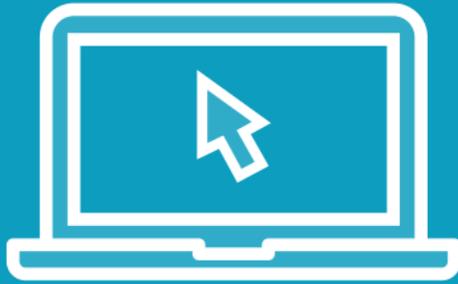
- Review a “proactive” Trivy integration
- Use Github Actions to integrate Trivy into the code review process
 - Consumer view
 - Technical view



Docker Build Workflow: Proactive



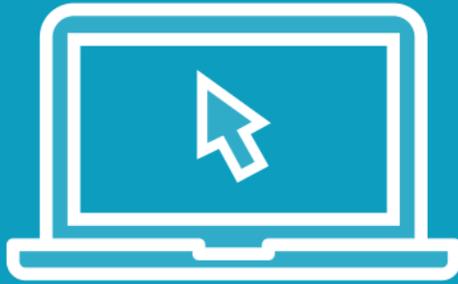
Demo



- Review “proactive” Trivy integration
- Use Github Actions to integrate Trivy into the code review process
- Consumer view
 - Trivy within Pull Request
 - Trivy enforcement settings
- Technical view
 - Github Actions workflow file
 - Docker build and Trivy scan



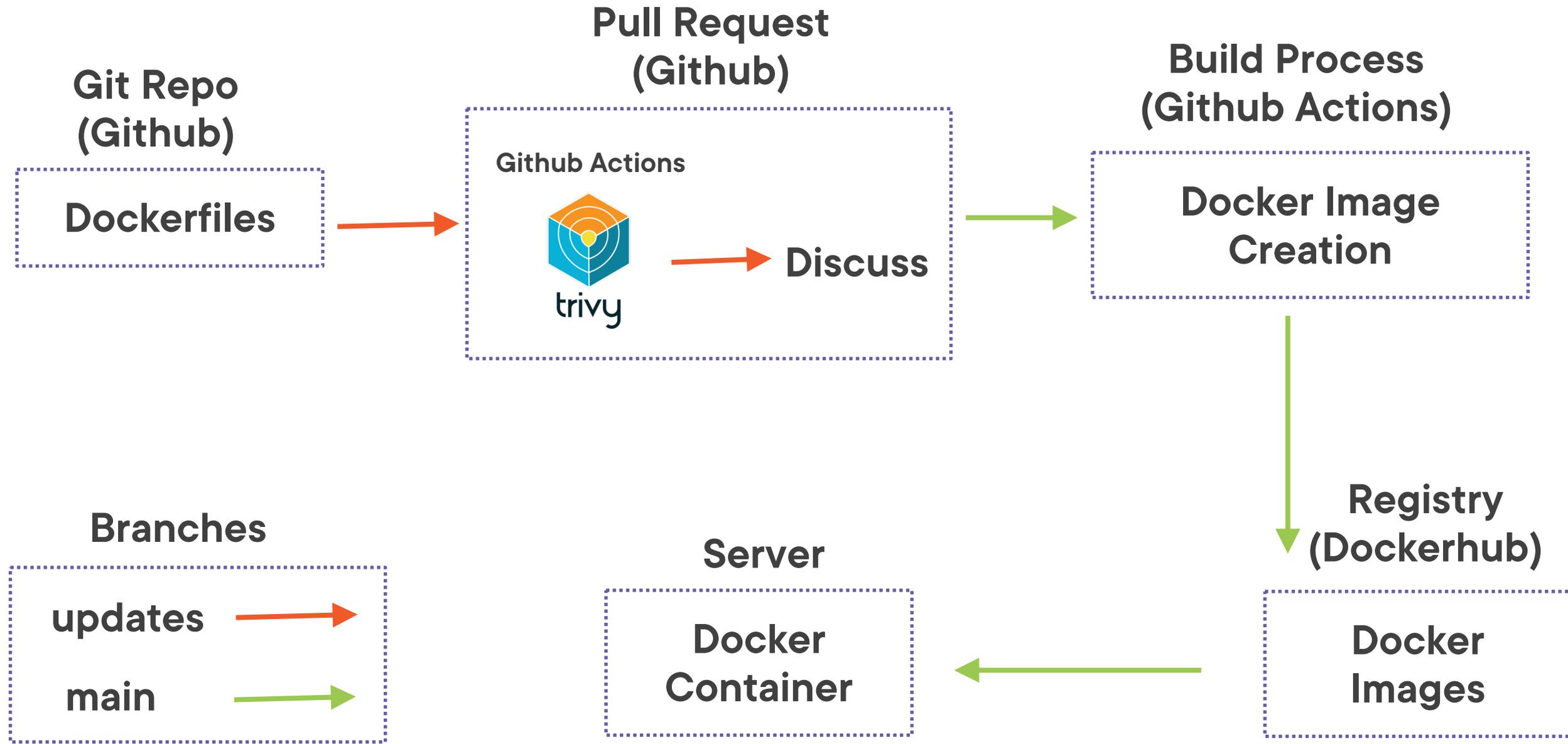
Demo



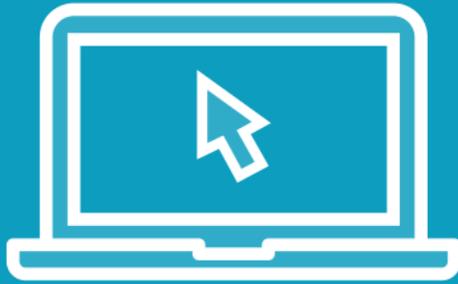
- Use Github Actions to upload Docker Images to the Docker Registry
- Rebuild Docker Images on a schedule to reduce vulnerabilities
- Circumvent Trivy
 - Docker Registry Tampering
 - Unscannable Vulnerabilities



Docker Build Workflow: Proactive



Demo



- Used Github Actions to upload a Docker Image to the Docker Registry
- Witnessed how Docker Images can be rebuilt on a schedule to reduce vulnerabilities
- Used Github Actions to expose Docker Registry tampering
- Analyzed a “tampered” Docker Image with
 - Trivy
 - container-diff



Additional Resources

Capabilities

[Trivy Github README](#)

[Trivy Visual Studio Code Extension](#)

[Handling Container Vulnerabilities with Open Policy Agent](#)

[Harbor Scanner Adapter for Trivy](#)

Related Information

[Infrastructure Analysis with kube-hunter](#)

[container-diff](#)

[Docker Image History Modification](#)

[Github Actions Overview](#)

[Open Policy Agent](#)

