CI/CD Pipeline

Owner: Ayda Zhao
Reviewer:
Contributors:
Date Generated: Sun Jul 14 2024

Executive Summary

High level system description

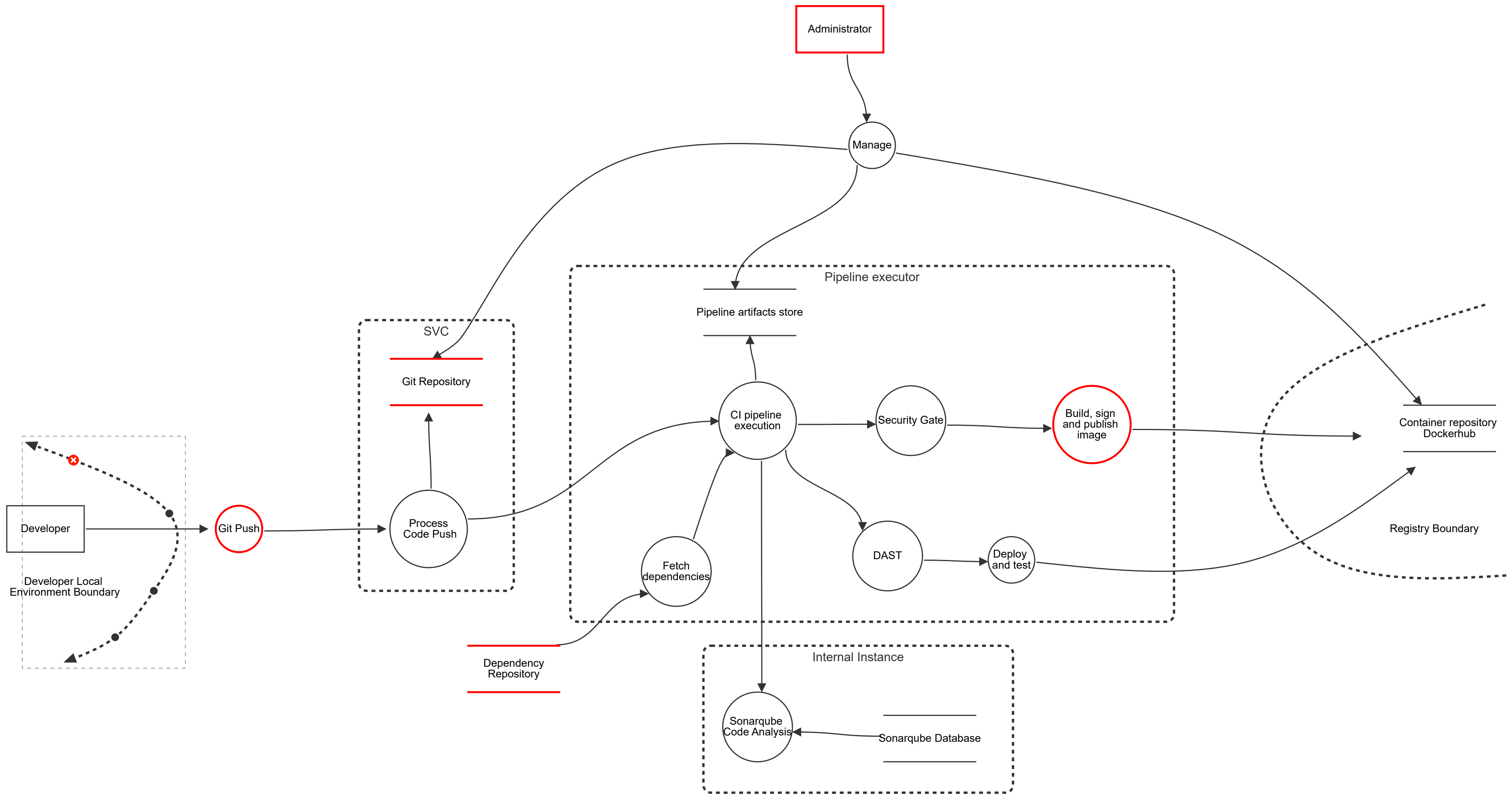
CI/CD pipeline for DevSecOps labs

Summary

Total Threats	5
Total Mitigated	0
Not Mitigated	5
Open / High Priority	0
Open / Medium Priority	5
Open / Low Priority	0
Open / Unknown Priority	0

CI Pipeline

CI Pipeline for DevSecOps lab



CI Pipeline

Developer (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Git Push (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	Employee discloses secrets	Information disclosure	Medium	Open		An employee could expose secrets to a naughty employee by accidentally putting them somewhere in the repository	Use a tool like git-secrets, which can detect secrets and block the changes to the repository

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Git Repository (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
14	Repository gets cloned without permission	Information disclosure	Medium	Open		A naughty developer copies/clones files from the repository without permission, possibly revealing its contents to the outside	Enable audit logging and monitoring of data access, so people can swiftly act. If a developer doesn't need to access certain files, restrict them from accessing those files

Process Code Push (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Pipeline artifacts store (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

CI pipeline execution (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Fetch dependencies (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DAST (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Security Gate (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Manage (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Administrator (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Someone spoofing the administrator	Spoofing	Medium	Open		Someone might spoof and pretend to be the administrator if they find access to the administrator's account	Make the administrator have multifactor authentication to log in, encrypt the laptop/computer in case it ever gets stolen, use credentials that rotate

Dependency Repository (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Malicious dependency	Tampering	Medium	Open		Someone could tamper with the repositories you are getting dependencies from, or make a malicious dependency a developer might choose to use, not knowing it's harmful	Do an automated dependencies analysis, make a company policy that will check for approval of every dependency added

Build, sign and publish image (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	Image with backdoor	Tampering	Medium	Open		A naughty developer pushes an image containing a backdoor somewhere to the container, intending for that image to be pulled and deployed as a production image	Use image signing so only images that have been properly signed can be deployed, don't store development and production images on the same container and restrict access to the production container

Deploy and test (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Sonarqube Database (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Sonarqube

Code Analysis (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Container repository

Dockerhub (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations