CI/CD Pipeline

Owner: Matthew
Reviewer:
Contributors:
Date Generated: Mon Jul 08 2024

Executive Summary

High level system description

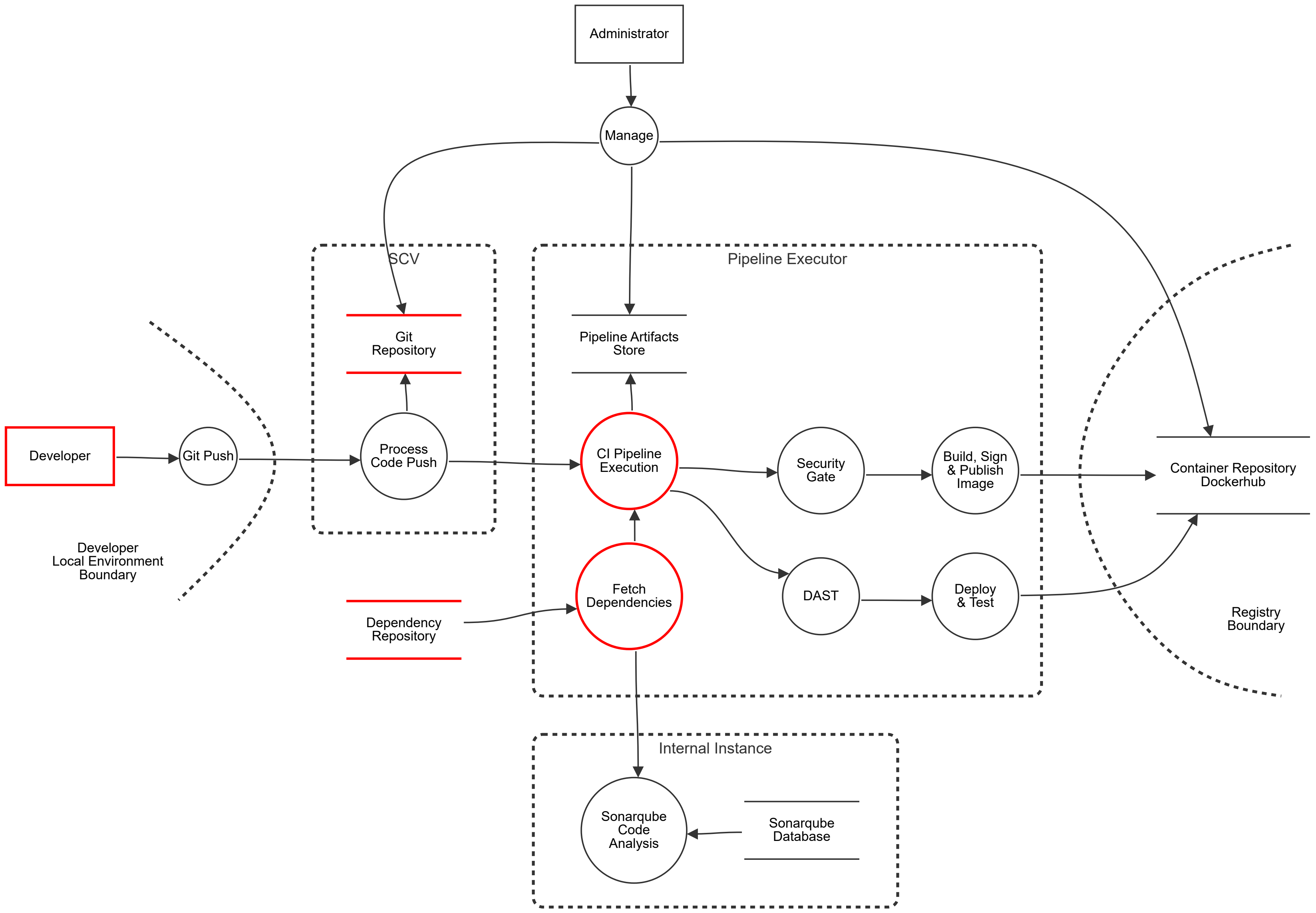
CI/CD Pipeline for DevSecOps labs

Summary

Total Threats	6
Total Mitigated	0
Not Mitigated	6
Open / High Priority	0
Open / Medium Priority	6
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
1	Developer commits secret to Git	Spoofing	Medium	Open		A developer commits secrets to version control either accidentally or on purpose. An angry employee with read access to the repository finds the secrets & proceeds to use them to steal end-user data.	Use git-secrets to watch for any secrets left in code or comments and block them from any merges. Adhere to the principal of "Need to Know" & ensure that production secrets aren't shared with individuals who don't have the need to know. Adhere to the principal of "Least Privilege" & ensure secrets only have the permissions to their use case.
15	Device Stolen	Spoofing	Medium	Open		The developer's working device is stolen or lost. It is unencrypted so that an adversary with tools to bypass security authentication to gain access to all repositories & ssh access points.	Ensure all devices given to employed developers are encrypted. Developer's repository has Least Privilege access applied to only reach what they need. Devices can only run under point end protection/ require a VPN connection, etc.

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 Push (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Process
Code Push (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Git
Repository (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Cloned Git Repository Outside Company	Information disclosure	Medium	Open		A user/adversary outside the organisation is able to pull or clone the git repository, despite that it should not be accessible to them.	Apply network restrictions to not be publicly available. Use temporary tokens instead of long life static tokens Limit the access permissions of each developer, no read/write permissions Provide Audit logging and security monitoring of data access.

Pipeline Artifacts
Store (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

CI Pipeline
Execution (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	Supply Chain Attack	Tampering	Medium	Open		An adversary gains access and control of the CI Pipelines to manipulate the build artifacts, injecting malicious code into the building materials before the build process begins, in hopes the malicious code is included into the build.	Apply Policy as Code to restrict dangerous code. Limit Egress connections via a Proxy or provide IP restrictions. Have an Audit logging of all activities within the CI Pipeline. Add secure monitoring using an IDS/IPS and EDR Have a clean environment on every pipeline run.

Security Gate (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Build, Sign & Publish Image (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DAST (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Deploy & Test (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Fetch Dependencies (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
0	New STRIDE threat	Spoofing	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Dependency Repository (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Malicious Package in Public Repository	Tampering	Medium	Open		An adversary uploads a seemingly benign but malicious package to host on a public repository, in hopes of developers adding this package to become a backdoor into the developer's project.	Make all merge requests require review and approval from other developers and engineers. Build CI pipeline tools for technical control to review package files and to identify non-sanctioned repositories by the company policy.

Administrator (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Manage (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Container Repository Dockerhub (Store)

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