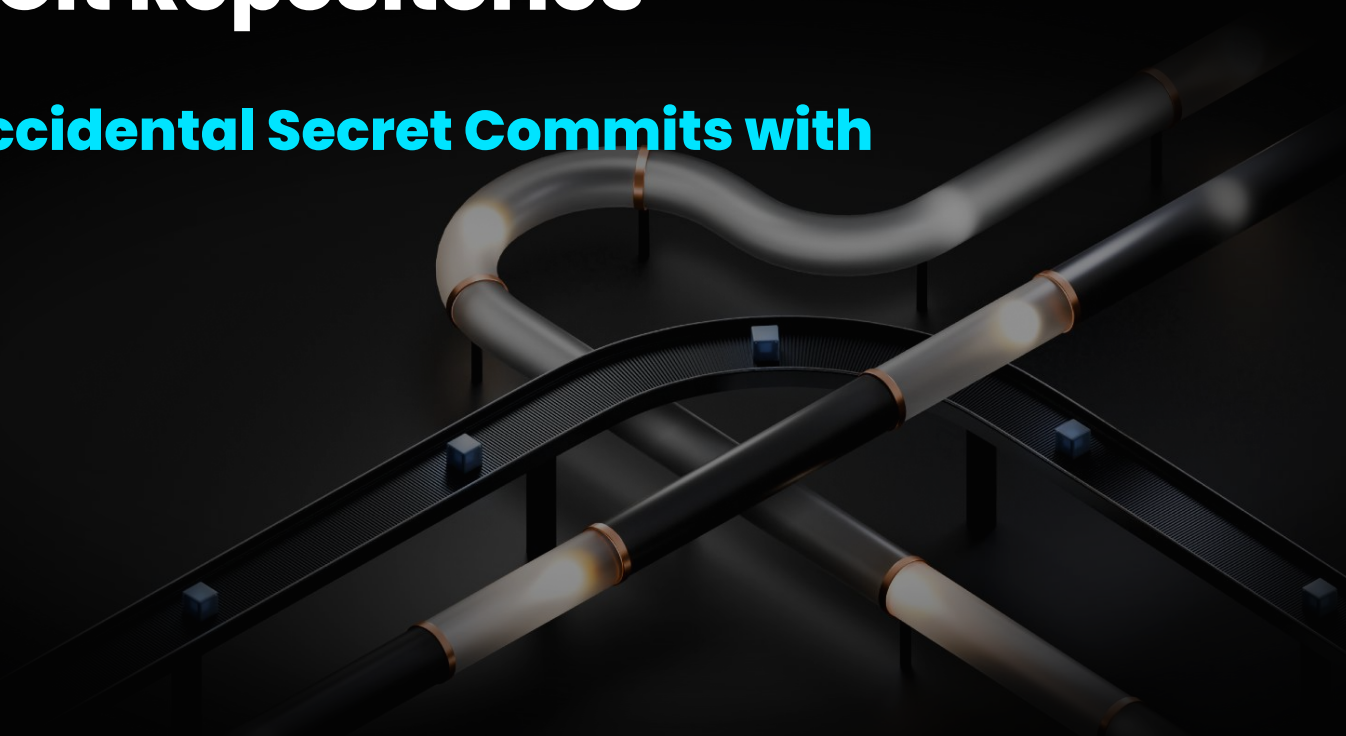# Securing Git Repositories

Preventing Accidental Secret Commits with Gitleaks
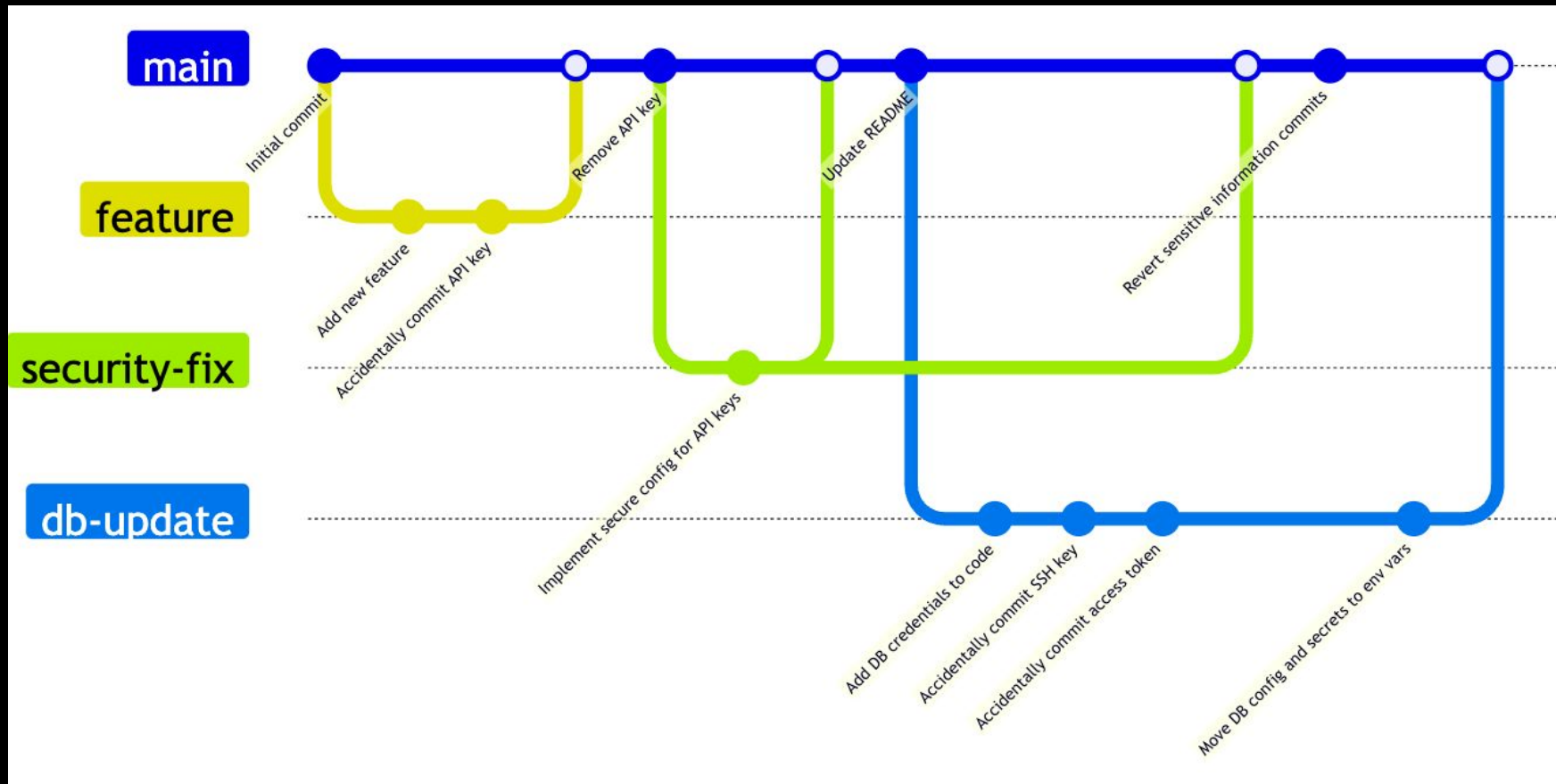
Dewan Ahmed
Principal Developer Advocate

harness

Why Are Git Repositories Vulnerable?

- Collaborative Nature
- Ease of Accidental Commits
- Growing Number of Repositories and Codebases

diahmed

harness

What are Secrets in Code?

Shifting Left on Security

- Catch issues early in the development cycle.
- Benefits:
  - Minimize exposure risk.
  - Reduce time and effort spent fixing issues later.

harness

What is Gitleaks?

- An open-source secret scanner for git repositories, files, and directories.
- Key features:
  - Predefined and customizable secret patterns.
  - Lightweight and fast.
  - CI/CD integration.

harness

Gitleaks rules

```
[[rules]]
id = "harness-api-key"
description = "Identified a Harness Access Token (PAT or SAT), risking unauthorized acces
regex = '''(?:pat|sat)\.[a-zA-Z0-9_-]{22}\.[a-zA-Z0-9]{24}\.[a-zA-Z0-9]{20}'''
keywords = [
    "pat.",
    "sat.",
]
```

harness

How Gitleaks works?

Detection Process:

- Pattern-based scanning.
- Configurable rules.

Modes:

- Local scanning.
- Pre-commit hooks.
- CI/CD pipelines.

diahmed

harness

Repo

Pipelines

Artifact Registry

GitSpaces
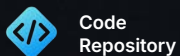
Project

User Management

Secret Management

Harness Open Source

Harness Open Source vs Harness Platform

Harness Open Source

Ideal for individual developers and small teams

- Code Repository
- Continuous Integration
- Continuous Delivery
- Artifact Registry
- Cloud Development Environments

Easy upgrade →

Harness Platform

Ideal for organizations looking for governance and scalability

- Code Repository
- Continuous Integration
- Continuous Delivery & GitOps
- Feature Management & Experimentation
- Service Reliability Management
- Infrastructure as Code Management
- Cloud Development Environments
- Database DevOps
- Chaos Engineering
- Cloud Cost Management
- Software Engineering Insights
- Security Testing Orchestration
- Supply Chain Security
- Internal Developer Portal
- Artifact Registry

Demo: Preventing Accidental Secret Commits

harness

Recap

- Preventing accidental secret commits is critical to repository security.
- Gitleaks is a powerful, open-source tool for detecting secrets.
- Integrating tools like Harness Open Source enhances security and productivity.

diahmed

harness

https://bit.ly/harness-lab

https://bit.ly/harness-opensource

diahmed

harness