



How Hackers Use Tokens To Break Into Google Cloud Pipelines

ABOUT CYBERWARFARE LABS :

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform



INFINITE LEARNING EXPERIENCE

ABOUT SPEAKER

SUBASHINI K B

Security Consultant

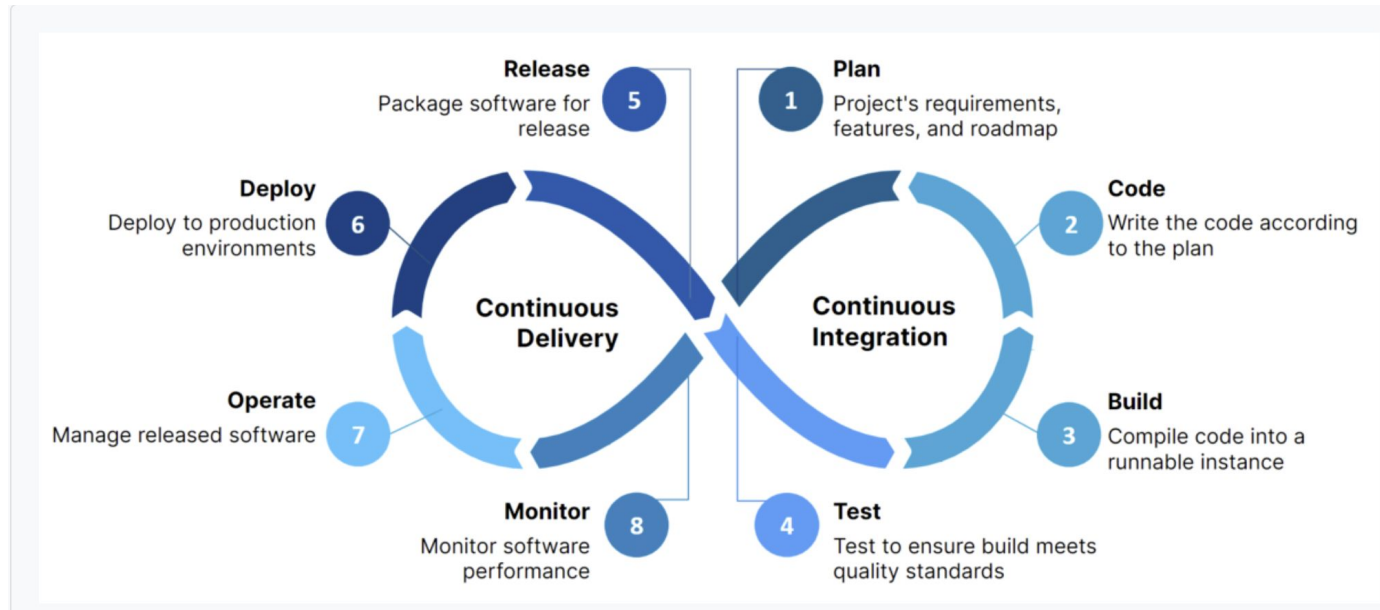
Subashini Balaji is a Security Consultant at **CyberWarFare Labs**, specializing in **Red Teaming and APT simulations** in enterprise environments. She also writes **technical blogs and articles** focused on real-world cyber attack techniques and defenses.

What is CI/CD?

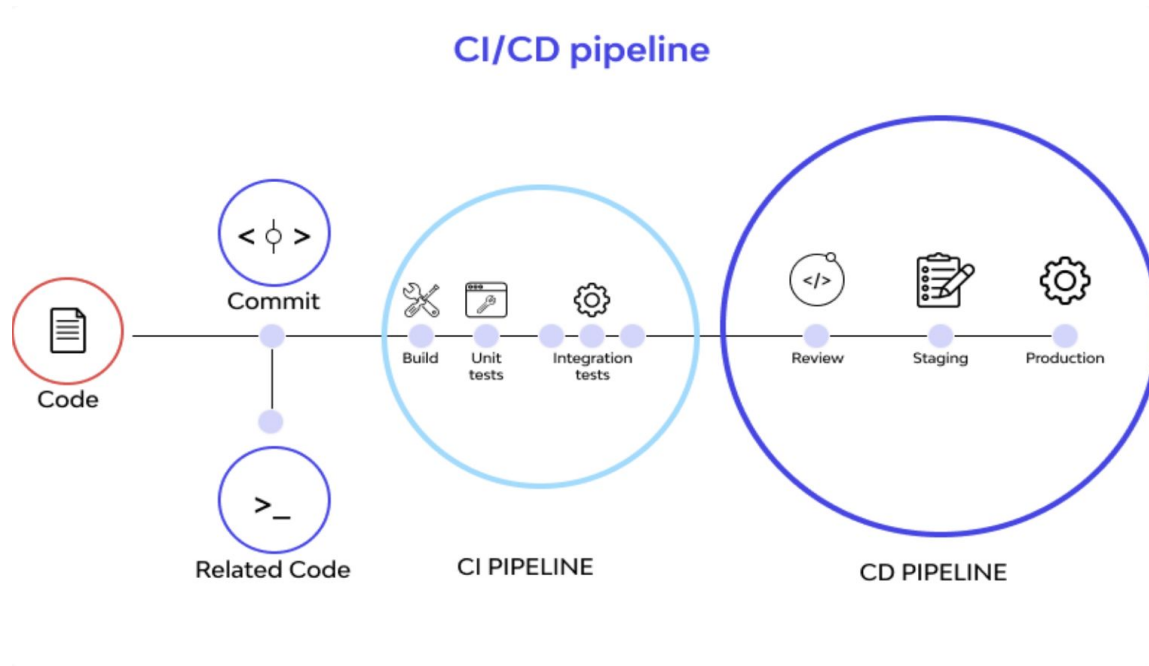
CI/CD (Continuous Integration and Continuous Delivery/Deployment) is a modern software development practice that automates the process of building, testing and releasing applications.

- **Continuous Integration (CI):** Developers keep adding their code into a common place and every time new code is added, it is automatically built and tested to catch problems early.
- **Continuous Delivery/Deployment (CD):** Once the code passes tests, it is automatically sent to staging or production, so new features and fixes reach users quickly and safely.

Architecture



CI/CD Pipeline Components

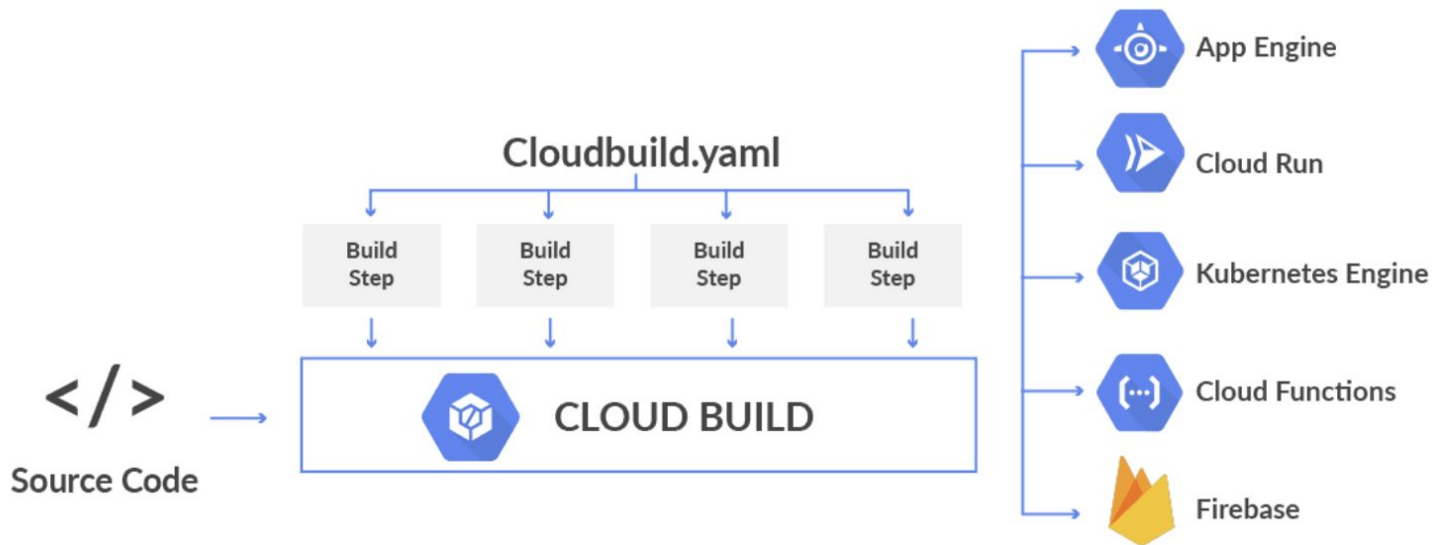


What is Cloud Build?

A fully managed CI/CD service that lets you build, test, and deploy applications on Google Cloud.

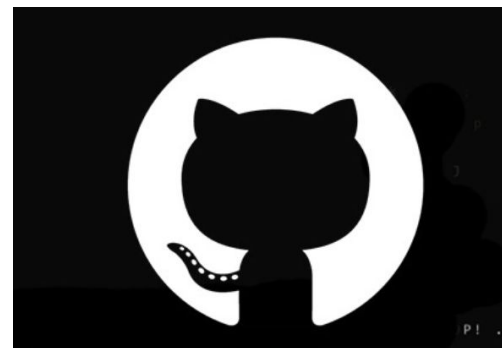
- ❖ Automates builds from source code.
- ❖ Supports containers, VMs and serverless deployments.
- ❖ Scales automatically, so you don't need to manage servers.
- ❖ Works with GitHub, GitLab, Bitbucket and Cloud Source Repositories.

Architecture



Scenario Overview


- ❖ Hijacking a CI/CD pipeline on GCP via GitHub
- ❖ Leveraging a GitHub token (PAT) for repo access
- ❖ Injecting a malicious build step in cloudbuild.yaml
- ❖ Executing a script to steal GCP service account tokens
- ❖ Exfiltrating tokens to an attacker-controlled server
- ❖ Using the stolen token to query Google APIs
- ❖ Flag: Reveal the service account email running the build



Solving Challenge

GCP CI-CD-02: Token Tactics

As part of Secure Corp's penetration testing team, your mission should you choose to accept it, is to enumerate their GCP DevOps setup and exfiltrate the value of GCP service account used for running the builds.

 Medium Free 20 Not Completed



NEW CHALLENGES RELEASED

ACROSS 3 CORE DOMAINS



**ON-PREMISE
SECURITY**



**CLOUD
SECURITY**



**KUBERNETES
SECURITY**

TRY NOW

infinity.cyberwarfare.live



Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :

support@cyberwarfare.live

To know more about our offerings, please visit: **<https://cyberwarfare.live>**