

# CICD

## Security Assessment

### Your Challenge

As developers push the limits of speed and agility, they increasingly rely on Continuous Integration and Continuous Delivery (CI/CD) pipelines. These CI/CD pipelines often require access to your most sensitive assets — your cloud environments, source code, service account credentials, and secrets necessary to deploy production applications.

Sophisticated attackers increasingly recognize CI/CD pipelines as vulnerable links in an organization's supply chain. To stay ahead, you need a security partner leading the charge in CI/CD security — someone who can identify and address vulnerabilities in your pipelines before attackers exploit them.

### Our Solution: Capabilities Overview

To address this challenge, we have harnessed our extensive experience from advanced Red Team assessments, CI/CD vulnerability research, and cloud/application security to emulate attackers performing the highest CI/CD exploitation levels.

Praetorian's CI/CD security experts excel at discovering material risk. They turn seemingly benign vulnerabilities into real-world attack paths, demonstrating how attackers or malicious insiders could execute large-scale internal or external supply chain attacks by exploiting your CI/CD pipelines.

We offer two assessment approaches tailored to meet your specific needs:



#### CI/CD Attack Path Mapping

We collaborate with you to identify the assets in your CI/CD environment that pose the greatest risk to your organization if compromised. From there, we perform hands-on testing across various user roles, revealing pathways attackers could exploit to compromise your critical assets through CI/CD abuse.



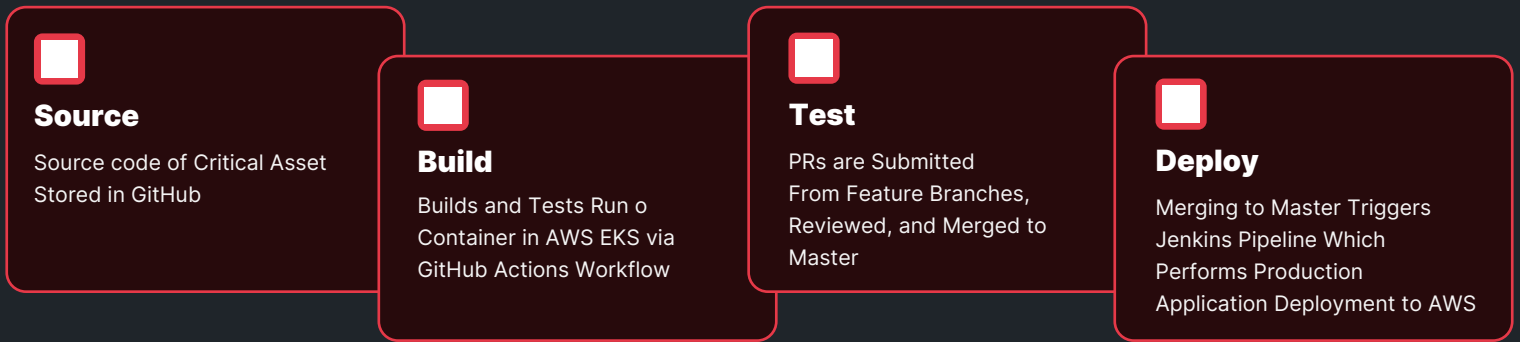
#### Targeted CI/CD Security Assessment

If you are concerned about a specific class of users being able to compromise a certain critical asset, we use a targeted approach to identify risks related to your concerns. Leveraging access as one of the specified user roles, we test whether they can exploit your CI/CD pipelines to compromise your highest-valued assets.

*We will work as a strategic partner during the scoping process to determine which approach is right for you.*

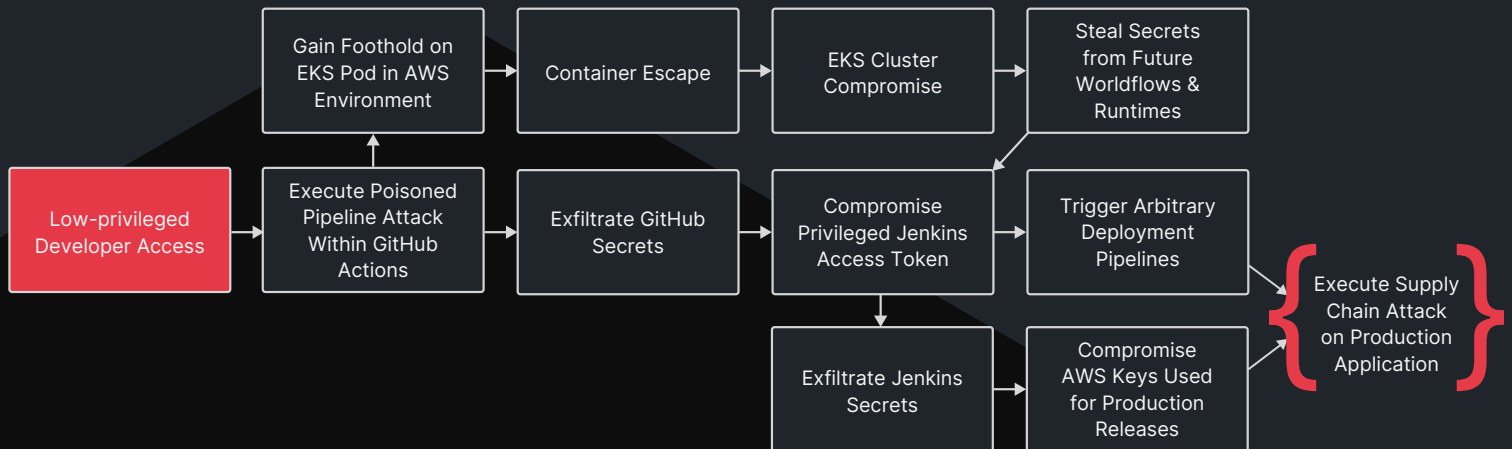
Both approaches are objective-driven. A simplified example CI/CD environment and attack path is depicted below.  
([Lucid link](#))

## Example CI/CD Process

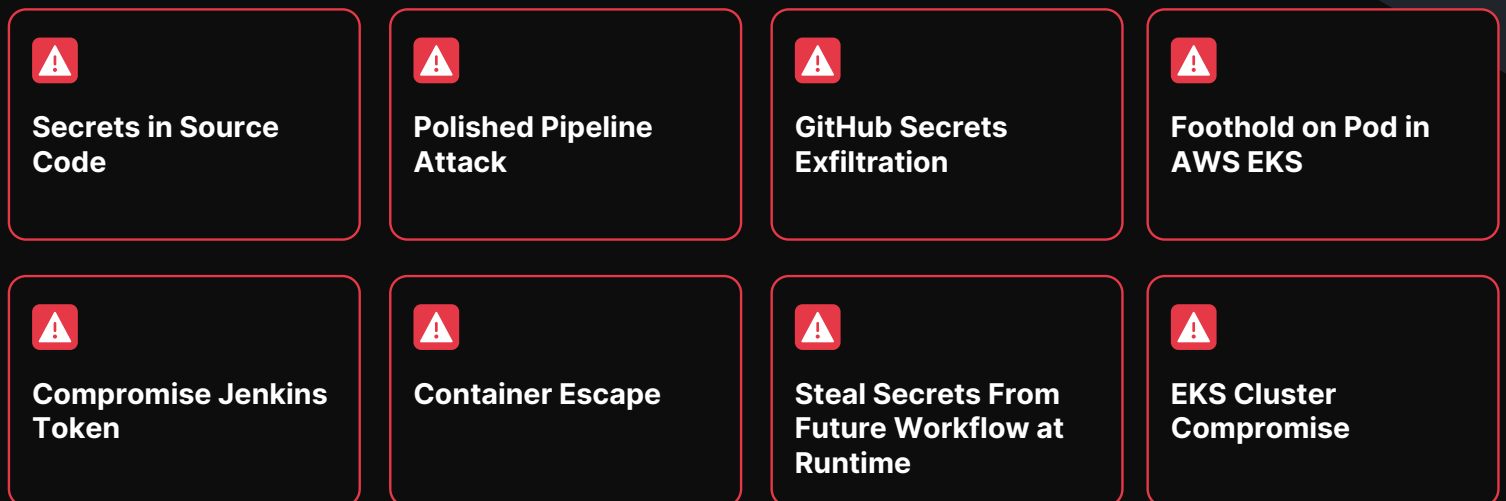


## Example Attack Path (Simplified)

**Client Objective:** As a low-privileged developer, demonstrate paths to execute a supply chain attack on our public-facing production application



## Potential Areas of Exposure



Other examples of past objectives include:

## Risk-Informed



Identify potential pathways to initiate a supply chain attack targeting core, public-facing applications.



Exploit CI/CD pipelines to compromise privileged cloud environments or Active Directory domains.

## Customer-Informed



With write access to a specific repository, escalate privileges to platform administrator to compromise the main infrastructure-as-code repository.



Leverage developer access to a repository in the staging DevOps environment to infiltrate the production environment.

## Why Praetorian

Praetorian brings over a decade of experience conducting offensive security engagements, and the resulting adversarial perspective underpins everything we do. Our highly technical CI/CD security engineers stem from our Advanced Red Team practice and have a background in multiple security aspects, which is essential to understanding the complex ecosystem of an organization's CI/CD environment. Armed with this understanding, these engineers analyze discrete components of the supply chain to determine which attack vectors an advanced attacker could realistically exploit.

Our engineers understand the specific business risks each of our clients faces and explore the business risk potential of every vulnerability they find. By combining unique vectors we identify from CI/CD pipelines with traditional offensive security, we can thoroughly test the entire CI/CD lifecycle.

Our CI/CD services are set apart from fully automated or commercial tool-dependent competitors. We focus on our clients' specific needs and critical assets to help them achieve their goals and securely realize the benefits of CI/CD at scale. We test your organization's security assumptions and provide factual information regarding the current security posture. We want your developers to maintain their speed and agility without exposing your organization to compromise.

## Key Benefits



**Learn** about cutting-edge TTPs sophisticated threat actors use and where they can impact your



**Identify** and **demonstrate** key sources of risk in the supply chain to inform future security investment and planning.



**Understand** the root causes of vulnerabilities and provide recommendations tailored to your business needs.

## Who Needs This Service



**Organizations** concerned about their critical applications being targeted by supply chain attacks.



**Enterprises** seeking to learn about CI/CD security, identify gaps in their CI/CD security posture, and uncover the associated risks.



**Security teams** looking for a demonstration of material risk to justify new security initiatives, budget cycles, or recent security investments.



**Mature organizations** who have locked down traditional attack surfaces and are seeking to protect their organization from sophisticated attackers.

## Deliverables

### Executive Summary

Concise explanation of engagement goals, significant findings, business impacts, and strategic recommendations  
Upon request, a letter of attestation

### Engagement Outbrief Presentation

Similar to the executive summary, presented to the audience of your choosing

### Technical Findings Report

Detailed description of issues and the methodology used to identify them, as well as an impact assessment for each