

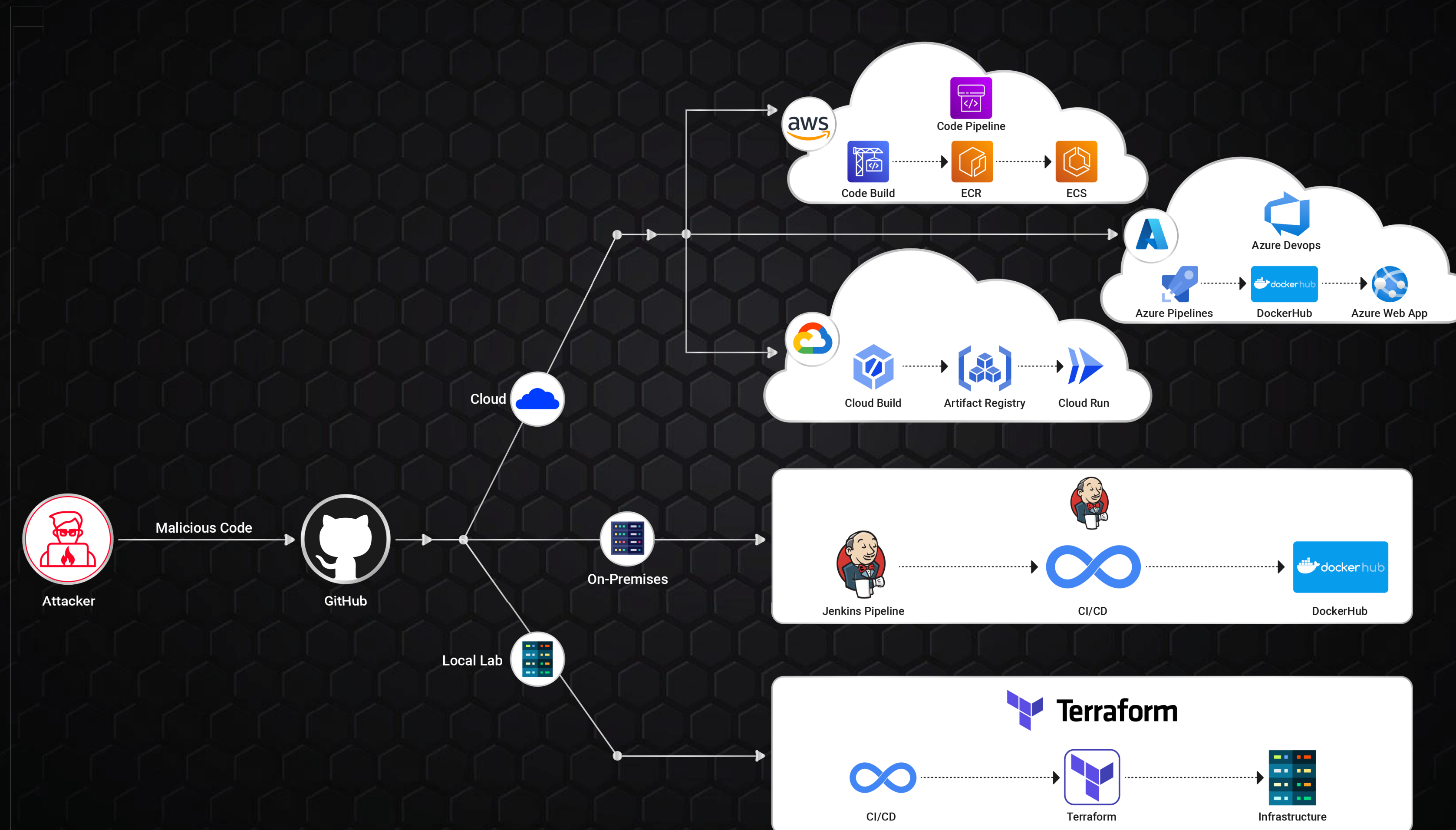


Certified Dev-Ops Red Team Analyst (DO-RTA)



@CyberWarFare Labs

Certified Dev-Ops Red Team Analyst (DO-RTA) Architecture



I. Software Development

- 1.1 Software Development 101
- 1.2 Software Development Life Cycle (SDLC) Model
- 1.3 Software Testing Life Cycle (STLC) Model
- 1.4 CIA Triad
- 1.5 Software Development Models

II. DevOps 101

- 2.1 Introduction to DevOps
- 2.2 Tools of Interest
- 2.3 DevOps in Cloud
 - 2.3.1 Introduction
 - 2.3.2 AWS CodePipeline
 - 2.3.3 Azure DevOps
 - 2.3.4 GCP DevOps
- 2.4 DevOps On-Premises
 - 2.4.1 Introduction
 - 2.4.2 Jenkins

III. Source Code Phase

- 3.1 Source Code Phase
- 3.2 GitHub 101
- 3.3 Demo 01: GitHub Enumeration
- 3.4 Backdoors
- 3.5 Malicious IDE Extension
- 3.6 Dockerfile Backdoor
- 3.7 Malicious GitHub Actions
- 3.8 Malicious Webhook

IV. Attacking DevOps

4.1 AWS CodePipeline

4.1.1 Introduction

4.1.2 Environment Variables Exfiltration

4.1.3 ECR Enumeration & Exploitation

4.1.4 CodeBuild Exploitation & Exploitation

4.1.5 Production App Token Exfiltration

IV. Attacking DevOps

4.2 Azure DevOps

4.2.1 Introduction

4.2.2 Environment Variables Exfiltration

4.2.3 Azure DevOps Enumeration & Exploitation

4.2.4 Docker Hub Enumeration

4.2.5 Production App Token Exfiltration

IV. Attacking DevOps

4.3 GCP DevOps

4.3.1 Introduction

4.3.2 Service Account Token Exfiltration

4.3.3 GCP Project Enumeration

4.3.4 Cloud Run Enumeration & Exploitation

IV. Attacking DevOps

4.4 Jenkins

4.4.1 Introduction

4.4.2 Credential Exfiltration via Misconfigured Jenkins GUI

4.4.3 Credential Exfiltration via Webhook

4.4.4 Pipeline Access via leaked API Token

4.4.5 Reverse Shell via Jenkins Build Modification

4.4.6 Docker Image Poisoning

IV. Attacking DevOps

4.5 Terraform

- 4.5.1 Introduction
- 4.5.2 Terraform RCE w/ Custom Provider
- 4.5.3 Terraform RCE w/Data Source
- 4.5.4 Terraform RCE w/ Provisioner
- 4.5.5 Terraform Data Exfil
- 4.5.6 Terraform CI/CD Attacks

V. DevSecOps

- 5.1 Introduction
- 5.2 Phases
- 5.3 Pre-Commit
- 5.4 Post-Commit
- 5.5 Secrets Management
- 5.6 Continuous Testing
- 5.7 Artifact Storage
- 5.8 DAST Testing
- 5.9 Monitoring



Thank You

Cyberwarfare.live

