Cloud Contraptions
TRAINING & CONSULTING

To discuss this course and customizations:
Call: 434-509-5680 or Email: sales@cloudcontraptions.com

CI/CD with GitHub Actions

Class Duration

14 hours of live training delivered over 2 days.

Student Prerequisites

- Comfortable using Git and GitHub (commits, branches, pull requests)
- Software development experience in any language
- Basic command-line skills
- Familiarity with YAML is helpful but not required
- No prior GitHub Actions or CI/CD experience required

Target Audience

This course is designed for software engineers, DevOps engineers, and team leads who want to automate building, testing, and deploying software with GitHub Actions. It suits teams adopting GitHub Actions for the first time as well as teams with ad hoc workflows who want to consolidate on secure, maintainable, reusable pipelines.

Description

CI/CD with GitHub Actions teaches participants to design, build, and operate continuous integration and continuous delivery pipelines on GitHub's native automation platform. The course begins with workflow syntax, event triggers, and the relationship between workflows, jobs, steps, and runners, then builds up through matrix builds, caching, artifacts, and integrating tests, linters, and container builds into every pull request. Participants learn to eliminate copy-pasted YAML with reusable workflows and composite actions, and to gate production deployments with environments, required reviewers, and deployment protection rules.

The second half of the course focuses on running Actions safely and at scale: managing secrets, authenticating to AWS and Azure with OpenID Connect instead of long-lived credentials, choosing between GitHub-hosted, larger, and self-hosted runners, and hardening pipelines against supply-chain attacks with SHA pinning, least-privilege tokens, and GitHub's immutable releases and immutable actions. The course closes with monorepo strategies, release automation, deploying to cloud targets, and a forward-

To discuss this course and customizations:
Call: 434-509-5680 or Email: sales@cloudcontraptions.com

looking session on AI agents in CI, including the Claude Code GitHub Action and the security considerations that agentic automation introduces.

Learning Outcomes

- Author workflows with correct syntax, expressions, contexts, and event triggers
- Structure pipelines into jobs and steps with appropriate dependencies and concurrency controls
- Run matrix builds across operating systems, language versions, and configurations
- Speed up builds with dependency caching and share results between jobs with artifacts
- Integrate tests, linters, code coverage, and container image builds into pull request checks
- Eliminate duplication with reusable workflows and composite actions shared across repositories
- Protect deployments with environments, required reviewers, and deployment protection rules
- Authenticate to AWS and Azure using OIDC federation with no long-lived cloud keys
- Select and operate the right runner strategy: GitHub-hosted, larger, or self-hosted
- Harden workflows against supply-chain attacks with action pinning, least-privilege GITHUB_TOKEN permissions, and immutable action releases
- Design path-filtered and selective pipelines for monorepos
- Automate versioning and releases with tags, release workflows, and changelog generation
- Evaluate and safely adopt AI agents in CI, including the Claude Code GitHub Action

Training Materials

Comprehensive courseware is distributed online at the start of class. All students receive a downloadable MP4 recording of the training.

Software Requirements

Students will need a free, personal GitHub account with permission to create repositories, Git installed locally, and a code editor (VS Code recommended).

Cloud Contraptions
TRAINING & CONSULTING

To discuss this course and customizations:
Call: 434-509-5680 or Email: sales@cloudcontraptions.com

Docker Desktop or Podman is helpful for the container topics but not required. Cloud deployment demonstrations are run by the instructor; students who want to follow along will need access to an AWS or Azure account.

Training Topics

GitHub Actions Fundamentals

- CI/CD concepts: integration, delivery, deployment
- Where Actions fits in the GitHub platform
- Workflows, jobs, steps, actions, and runners
- The Actions Marketplace and evaluating third-party actions
- Reading workflow logs and debugging failures

Workflow Syntax and Triggers

- Workflow file anatomy and YAML essentials
- Events: push, pull_request, schedule, workflow_dispatch
- Filtering by branch, tag, and path
- Expressions, contexts, and variables
- Conditional execution with if
- Concurrency groups and cancelling stale runs

Jobs, Steps, and Runners

- Job dependencies with needs
- Passing data between steps and jobs with outputs
- GitHub-hosted runner images and tooling
- Job-level and step-level timeouts
- Permissions and the GITHUB_TOKEN

Matrix Builds, Caching, and Artifacts

- Matrix strategies across versions and platforms
- Includes, excludes, and fail-fast behavior
- Dependency caching with actions/cache
- Built-in caching in setup actions
- Uploading and downloading artifacts
- Artifact retention and storage considerations

Integrating Tests, Linters, and Containers

- Running unit and integration tests on every push

To discuss this course and customizations:
Call: 434-509-5680 or Email: sales@cloudcontraptions.com

- Linters and formatters as required checks
- Code coverage reporting in pull requests
- Service containers for databases and dependencies
- Building and pushing container images to GHCR
- Branch protection and required status checks

Reusable Workflows and Composite Actions

- workflow_call and input/secret contracts
- Organization-level shared workflow repositories
- Composite actions for repeated step sequences
- Composite actions vs. reusable workflows: choosing
- Versioning shared automation

Environments and Deployment Protection

- Defining environments: dev, staging, production
- Environment-scoped secrets and variables
- Required reviewers and wait timers
- Deployment protection rules and custom gates
- Deployment history and traceability

Secrets and OIDC Cloud Authentication

- Repository, environment, and organization secrets
- Why long-lived cloud keys in CI are a liability
- OpenID Connect: how token exchange works
- Federating with AWS IAM roles and Azure workload identity
- Scoping trust policies to repos, branches, and environments
- Secret masking, rotation, and leak prevention

Self-Hosted and Larger Runners

- GitHub-hosted vs. self-hosted trade-offs
- Larger runners for compute-heavy builds
- Runner groups, labels, and routing
- Autoscaling self-hosted runners with ARC on Kubernetes
- Security risks of self-hosted runners on public repos

Security Hardening and Supply Chain

- Pinning actions to full commit SHAs
- Immutable releases and immutable actions published as packages

To discuss this course and customizations:
Call: 434-509-5680 or Email: sales@cloudcontraptions.com

- Least-privilege GITHUB_TOKEN permissions per job
- Script injection via untrusted inputs and how to prevent it
- pull_request_target and fork-based attack patterns
- Dependabot for workflow dependencies
- GitHub's Actions security roadmap: what is coming

Monorepo and Release Strategies

- Path filters and selective job execution
- Splitting pipelines per package or service
- Tag-driven release workflows
- Semantic versioning and changelog automation
- Publishing packages and creating GitHub Releases

Deploying to the Cloud

- Deploying containers to cloud container services
- Deploying static sites and serverless functions
- Blue-green and progressive rollout patterns with environments
- Rollbacks and re-running deployments safely

AI Agents in CI/CD

- Where AI agents fit in a pipeline: review, triage, fixes
- The Claude Code GitHub Action: @claude mentions and automation jobs
- Authentication options and permission scoping for agent workflows
- Prompt injection and secret-exposure risks in agentic CI
- Guardrails: least privilege, human approval, and audit trails