Cloud Contraptions
TRAINING & CONSULTING

To discuss this course and customizations:
Call: +1 434-509-6890 or Email: sales@cloudcontraptions.com

Secure Coding Practices and DevSecOps

Class Duration

21 hours over 3 full days, or 6 half-days, to accommodate flexible scheduling needs

Student Prerequisites

- Programming experience in at least one modern language (Java, C#, Python, JavaScript, or similar)
- Basic understanding of software development lifecycle
- Familiarity with version control systems (Git)
- Basic knowledge of web applications and APIs

Target Audience

This course is designed for software developers, DevOps engineers, security professionals, and technical leads who need to implement secure coding practices and integrate security into their development workflows. It's particularly valuable for teams transitioning to DevSecOps methodologies and organizations looking to enhance their application security posture through proactive development practices. Teams standardizing on GitHub can pair this with GitHub Advanced Security in Action.

Description

This comprehensive course provides hands-on training in secure coding practices and the integration of security throughout the software development lifecycle. Participants will master the identification and mitigation of common vulnerabilities, learn to implement robust threat modeling processes, and gain practical experience with security testing tools and techniques. The course emphasizes the DevSecOps philosophy of shifting security left, enabling teams to build security into their development pipelines rather than treating it as an afterthought. Students will work with real-world scenarios and tools to understand how to conduct secure design reviews, implement automated security testing, and respond to security incidents effectively. The curriculum can be customized to focus on specific programming languages and technology stacks based on organizational needs. Optional modules on AI-assisted security tools provide cutting-edge

Copyright 2026 Cloud Contraptions LLC – All Rights Reserved

insights into leveraging artificial intelligence for vulnerability detection and code review processes.

Learning Outcomes

- Apply secure coding principles and best practices across multiple programming languages and frameworks.
- Conduct comprehensive threat modeling using STRIDE methodology and risk assessment techniques.
- Identify, assess, and mitigate vulnerabilities from the OWASP Top 10 and beyond.
- Design and implement secure application architectures with defense-in-depth strategies.
- Integrate static application security testing (SAST) and software composition analysis (SCA) into development workflows, and perform effective secure code reviews using both manual and automated techniques.
- Build and secure CI/CD pipelines with embedded security testing and automated remediation, and implement dynamic application security testing (DAST) in staging and production environments.
- Establish monitoring, logging, and incident response capabilities for application security.
- Ensure compliance with regulatory frameworks through automated auditing and documentation practices.

Training Materials

- Comprehensive course handbook with secure coding checklists and reference materials
- Hands-on lab exercises with vulnerable code samples and remediation examples
- Security testing tool evaluation guides and configuration templates
- DevSecOps pipeline templates and implementation blueprints
- Incident response playbooks and compliance frameworks
- Access to online security testing tools and platforms during training

Software Requirements

- Development environment for chosen programming language (IDE/editor)
- Git version control system

Copyright 2026 Cloud Contraptions LLC – All Rights Reserved

- Docker Desktop for containerization exercises
- Access to cloud-based security scanning tools (provided during training)
- Web browser for DAST tool interfaces
- Optional: Kubernetes cluster access for advanced container security topics

Training Topics

Security Foundations and Principles

- Modern software security landscape and threat environment
- CIA triad and defense-in-depth strategies
- Principle of least privilege and secure defaults
- Shift-left practices and collaborative security culture

Threat Modeling and Risk Assessment

- Asset identification and attack surface analysis
- STRIDE model implementation and DREAD scoring
- Data flow diagram construction and review
- Risk prioritization and mitigation strategies

OWASP Top 10 Vulnerabilities

- Injection attacks (SQL, command, LDAP) and prevention
- Broken authentication and session management
- Cross-site scripting (XSS) and cross-site request forgery (CSRF)
- Security misconfigurations and insecure direct object references

Secure Design and Architecture

- Security requirements gathering and documentation
- Secure component design and interface specifications
- Peer review processes and security checklists
- Architectural threat modeling and security patterns

Static and Composition Analysis

- Static application security testing (SAST) tool integration
- IDE-based security analysis and real-time feedback
- Software composition analysis (SCA) for dependency management
- False positive management and rule customization

Copyright 2026 Cloud Contraptions LLC – All Rights Reserved

To discuss this course and customizations:
Call: +1 434-509-6890 or Email: sales@cloudcontraptions.com

Secure Code Review Techniques

- Manual code review methodologies and checklists
- Pair programming and collaborative security practices
- Automated code review with AI-assisted tools
- Security finding tracking and remediation workflows

Container and Infrastructure Security

- Docker image security scanning and hardening
- Kubernetes workload security best practices
- Infrastructure as Code (IaC) security validation
- Container registry security and access controls

DevSecOps Implementation

- Security integration in CI/CD pipelines
- Automated security testing orchestration
- Security gate implementation and failure handling
- Cross-functional team collaboration strategies

Dynamic Security Testing

- Dynamic application security testing (DAST) implementation
- Automated vulnerability scanning in staging environments
- Production security monitoring and testing
- Result interpretation and automated remediation

Secrets and Configuration Management

- Secure secrets management with vault solutions
- Configuration security and environment management
- API key rotation and credential lifecycle management
- Secure deployment practices and environment isolation

Monitoring and Incident Response

- Application security monitoring and telemetry
- Centralized logging and security event correlation
- Security incident detection and response procedures
- Tabletop exercises and response plan validation

Compliance and Governance

- Regulatory framework compliance (GDPR, HIPAA, PCI DSS)
- Automated compliance checking and audit trails

Copyright 2026 Cloud Contraptions LLC – All Rights Reserved

To discuss this course and customizations:
Call: +1 434-509-6890 or Email: sales@cloudcontraptions.com

- Security metrics and KPI development
- Documentation and reporting best practices

Advanced Topics and AI Integration

- AI-assisted vulnerability detection and code analysis
- Machine learning for security pattern recognition
- Automated security testing with intelligent feedback
- Future trends in application security and DevSecOps

Copyright 2026 Cloud Contraptions LLC – All Rights Reserved