# DevSecOps Software and Infrastructure Development

## Securing Your Software Immediately to Reduce Risk and Mitigate Threats

Concurrent Technologies Corporation (CTC) has embraced the Development, Security, and Operations (DevSecOps) model of rapid development for software and infrastructure solutions. DevSecOps incorporates security throughout the entire IT lifecycle.

Complementing our other services, DevSecOps provides the ability for CTC to deliver a secure, rapid, and repeatable solution that can be deployed to a system in minutes. Our solutions save valuable time by implementing elements of Zero Trust (where a person, application, or entity connecting to a system must prove their identity and authenticate successfully, based on a least-privilege access policy) and a "shift-left" philosophy of cybersecurity that empowers and requires our developers to build in security at the earliest parts of the development pipeline.

Our DevSecOps software developers are experts at mitigating threats, neutralizing malware, and identifying bad actors attempting to disrupt critical systems such as:

- Cloud-based web applications
- Network-connected Edge nodes running local software
- Interconnected cloud-to-Edge
- Standalone isolated systems

Our developers meet security challenges early and continuously—and with frequent scanning of code for vulnerabilities and feedback from running systems. They use their knowledge of security controls and consult with other CTC engineers with extensive experience in Risk Management Frameworks (RMF) for Assessment & Authorization (A&A).

*It's not a matter of **IF** you should adopt DevSecOps, it's a matter of **WHEN**.*

CTC® *Concurrent Technologies Corporation*

www.ctc.com

continued

## Our Software Developers and Solutions Architects Practice These DevSecOps Principles

- Agile Development with Micro-Sprints
- Cloud-Native Solutions / Cloud Service Provider (CSP) Native Solutions
- Continuous Authorization to Operate (c-ATO) Principles
- Continuous Monitoring with Feedback Loops
- Defensive Cyber Operations
- Design to Support Failure Then Mitigate Rapidly
- Documentation as Code (DaC)
- Dynamic Application Security Testing (DAST)
- Continuous Integration / Continuous Delivery (CI/CD)
- Edge-Node Solutions
- Hybrid-Cloud Integration (Cloud-to-Edge, Cloud-to-On-Premise)
- Immutable, Hardened Containerized Solutions
- Infrastructure as Code (IaC)
- Integration Testing
- Linting of Software Code
- Microservice-Based Architectures and Orchestrators
- Minimum Viable Product (MVP) Concept (rapid delivery of a 60% solution)
- Multi-CSP Simultaneous Integration (e.g., Amazon Web Service, Google Cloud, Microsoft Azure)
- Open-Source Software
- Real-Time Monitoring Dashboards
- Software Factories
- Static Application Security Testing (SAST)
- Trusted Software Repositories
- Unit Testing
- Zero Trust

## DevSecOps is a Foundational Enabler

| | |
|---|---|
| AI/ML | Artificial Intelligence/ Machine Learning |
| AR/VR | Augmented Reality/ Virtual Reality |
| CDS | Cross Domain Solutions |
| CI/CD | Continuous Integration/ Continuous Delivery |
| CSSP | Cybersecurity Service Provider |
| DCO | Defensive Cyber Operations |
| IaaS | Infrastructure as a Service |
| OCONUS | Outside Continental United States |
| PaaS | Platform as a Service |
| SaaS | Software as a Service |


**Contact**
Digital Mission Solutions
(814) 269-6880
Digital-Mission@ctc.com


© 2026. Concurrent Technologies Corporation. All Rights Reserved.