Carnegie Mellon University
Software Engineering Institute

CERT® DevSecOps Model

Building Secure Applications

The DevOps Factory

DevOps is a modern software development approach that strives to bring development and operations teams together along with other stakeholders to improve efficiency and outcomes by focusing on shared business goals. DevOps follows and expands on key principles of the Agile software development and Lean engineering movements and represents a fundamental shift in how large, distributed enterprise organizations develop and deliver software.

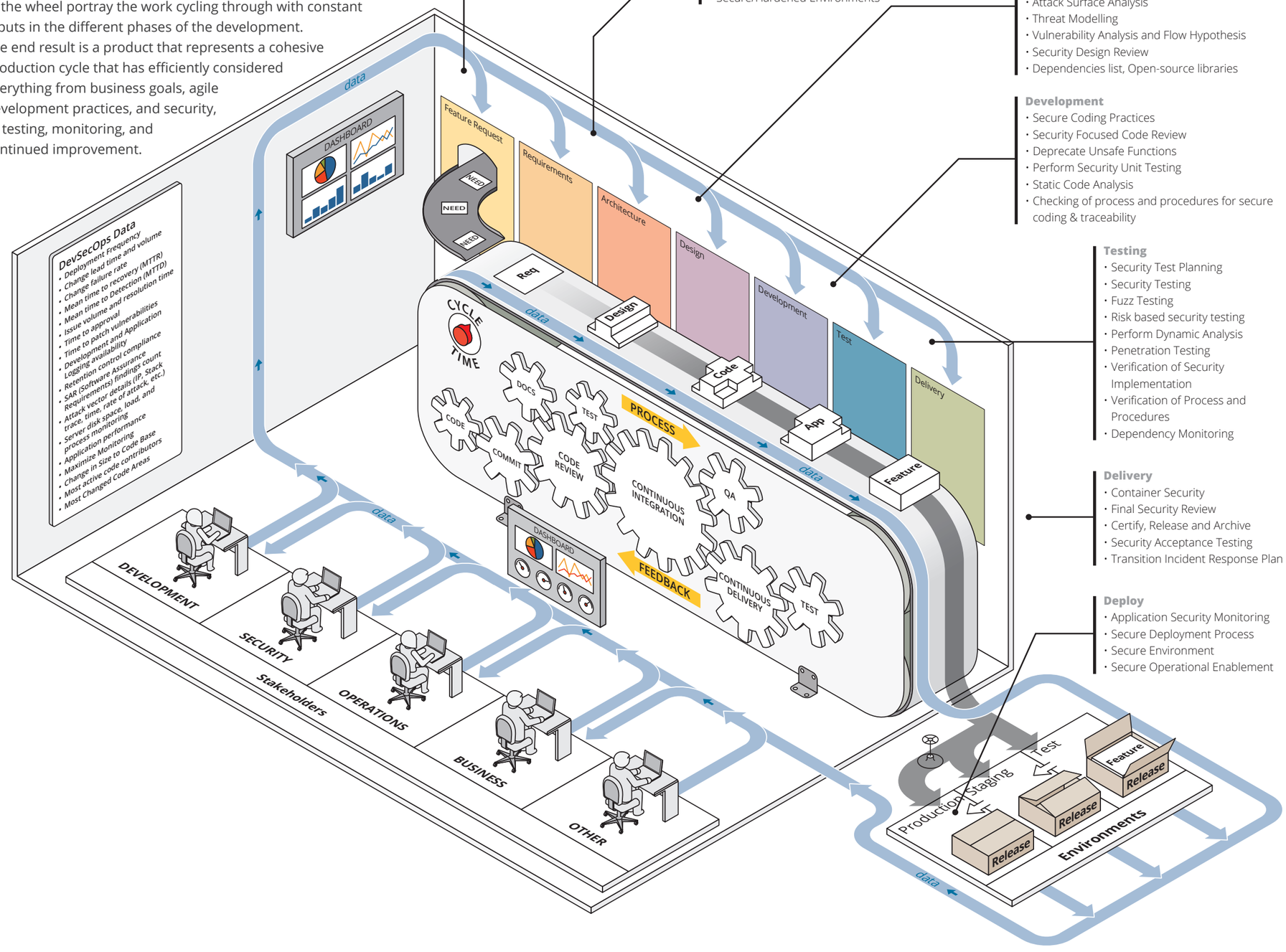
By cultivating cross-functional collective engagement in software development projects throughout the software development lifecycle (SDLC), DevOps affects the people, processes, and technology of an organization. DevOps also requires adopting and implementing cutting-edge practices based on the primary tenants of collaborative culture, automation, data-driven processes, infrastructure as code, and ubiquitous, real-time system monitoring.

The features and benefits of DevOps include

- **Consistently developing** software systems with higher quality and accuracy of project budgeting and estimation
- **Increased visibility** and stakeholder input into features for the next release as it is being developed
- **Engaging stakeholders** early and consistently throughout the SDLC, leading to fewer defects and incorrect requirements
- **Building trust** between software development and IT, enabling organic process improvement and risk mitigation
- **Maximizing business value** by enabling technical staff to adapt to changing requirements or environmental factors

Understanding the Factory

In the DevOps factory, stakeholders work collaboratively across the software development lifecycle. All of the cogs in the wheel portray the work cycling through with constant inputs in the different phases of the development. The end result is a product that represents a cohesive production cycle that has efficiently considered everything from business goals, agile development practices, and security, to testing, monitoring, and continued improvement.



Feature Request
- Strategy & Metrics
- Policy & Governance
- Education & Security Guidance
- Organizational Risk Factors
- Threat Assessment

Requirements
- Security Requirements (SFR/SAR)
- Risk Assessment
- Abuse Case Development
- Threat Modelling
- Security Stories
- Screen Development Tools
- Secure/Hardened Environments

Architecture & Design
- Security Architecture
- Architectural Risk Analysis
- Security Design Requirements
- Attack Surface Analysis
- Threat Modelling
- Vulnerability Analysis and Flow Hypothesis
- Security Design Review
- Dependencies list, Open-source libraries

Development
- Secure Coding Practices
- Security Focused Code Review
- Deprecate Unsafe Functions
- Perform Security Unit Testing
- Static Code Analysis
- Checking of process and procedures for secure coding & traceability

Testing
- Security Test Planning
- Security Testing
- Fuzz Testing
- Risk based security testing
- Perform Dynamic Analysis
- Penetration Testing
- Verification of Security Implementation
- Verification of Process and Procedures
- Dependency Monitoring

Delivery
- Container Security
- Final Security Review
- Certify, Release and Archive
- Security Acceptance Testing
- Transition Incident Response Plan

Deploy
- Application Security Monitoring
- Secure Deployment Process
- Secure Environment
- Secure Operational Enablement

How We Can Help

We help you establish robust DevOps capabilities by following a process in which we do the following.

Analyze—Analyze your organization's business goals, processes, and development/operational challenges to assess the status quo, bottlenecks, and areas that could get maximum impact from process improvement efforts.

Design and Develop—Develop a customized strategy and roadmap to improve your organization's culture, processes, and tools to support its business needs and improve its software development quality, transparency, and delivery while decreasing its risk.

Apply and Measure—Provide tools and methods for your organization to enable its process measurement capabilities. Apply a process improvement strategy according to the developed roadmap and measure the quantitative impact of DevOps on metrics for collaboration, quality, transparency, and process efficiency.

Monitor—Enable your organization's development managers and teams to independently monitor DevOps practices and engage in continuous data-driven improvements to tools and methods according to your organization's unique needs.

DevOps Solutions

We offer the following solutions to help you develop a robust DevOps capability in your organization.

Training

We provide onsite or virtual courses that teach DevOps to managers, technical teams, and other stakeholder groups. We also offer advanced, hands-on DevOps training for development and operational teams.

Workshops

We conduct customized, hands-on workshops that provide comprehensive practical training, including exercises using DevOps tools and techniques throughout the SDLC, from inception to production.

Mentoring

By collaborating closely with teams and stakeholders, we assist in establishing practical guidelines to improve existing DevOps strategies and enhance collaboration among organizational teams.

Engineering Support

Our highly experienced engineers help you implement and measure your organization's DevOps tools and processes.

Learn More in the SEI Digital Library

Visit resources.sei.cmu.edu/library and search for the phrase Finding your way in DevOps.

For our blog series on Devops, visit https://insights.sei.cmu.edu/category/devops.

About the CERT Division

The CERT® Division of Carnegie Mellon University's Software Engineering Institute studies and solves problems with widespread cybersecurity implications, researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu