DevSecOps

Building Secure Applications

The DevSecOps Ecosystem

DevSecOps is a 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. DevSecOps 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), DevSecOps affects the people, processes, and technology of an organization. DevSecOps also requires adopting and implementing cutting-edge practices based on the primary tenets of collaborative culture; automation; data-driven processes; infrastructure as code; and ubiquitous, real-time system monitoring.

The features and benefits of DevSecOps 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
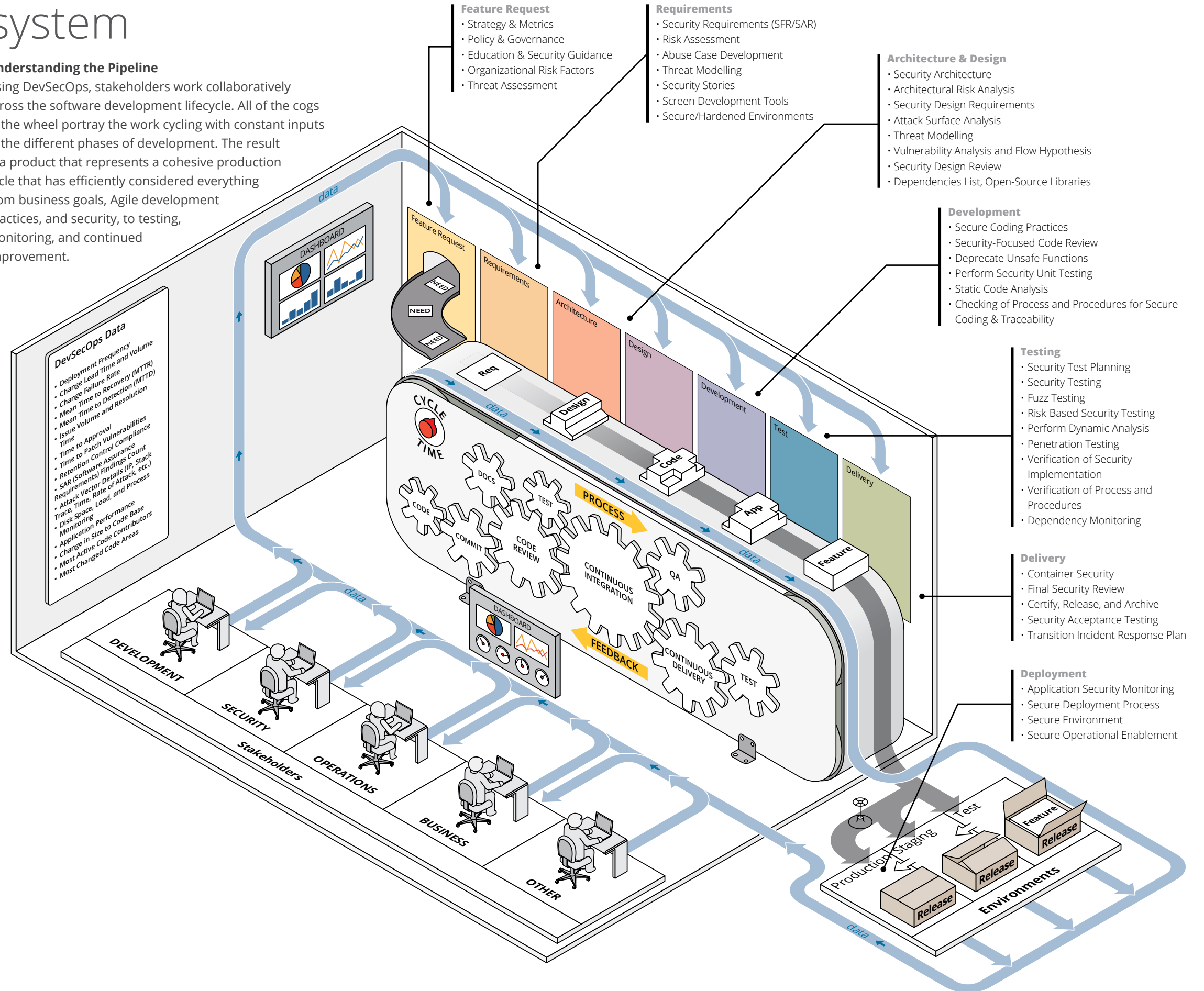
Building trust between software development and IT, enabling organic process improvement and risk mitigation

Maximizing business value by enabling technical staff to adapt to changing requirements or environmental factors

Understanding the Pipeline

Using DevSecOps, stakeholders work collaboratively across the software development lifecycle. All of the cogs in the wheel portray the work cycling with constant inputs in the different phases of development. The 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

Deployment
· Application Security Monitoring
· Secure Deployment Process
· Secure Environment
· Secure Operational Enablement

DevSecOps Data
· Deployment Frequency
· Change Lead Time and Volume
· Change Failure Rate
· Change Time to Recovery (MTTR)
· Mean Time to Detection (MTTD)
· Mean Time and Resolution
· Issue Volume and Resolution Time
· Time to Approval
· Time to Patch Vulnerabilities
· Retention Control Compliance
· SAR (Software Assurance Requirements) Findings Count
· Attack Vector Details (IP, Stack Trace, Time, Rate of Attack, etc.)
· Disk Space, Load, and Process
· Monitoring
· Application Performance
· Change in Size to Code Base
· Most Active Code Contributors
· Most Changed Code Areas

DASHBOARD

Feature Request

Requirements

Architecture

Design

Development

Test

Delivery

CYCLE TIME

PROCESS

FEEDBACK

Req

Design

Code

App

Feature

DOCS

TEST

CODE

COMMIT

CODE REVIEW

CONTINUOUS INTEGRATION

QA

CONTINUOUS DELIVERY

TEST

DASHBOARD

DEVELOPMENT

SECURITY

OPERATIONS

BUSINESS

OTHER

Stakeholders

data

Production Staging

Test

Feature

Release

Release

Release

Release

Environments

NEED

data

How We Can Help

We help you establish robust DevSecOps 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 DevSecOps on metrics for collaboration, quality, transparency, and process efficiency.

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

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

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

Workshops
We conduct customized, hands-on workshops that provide comprehensive practical training, including exercises using DevSecOps 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 DevSecOps strategies and enhance collaboration among organizational teams.

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

Learn More in the SEI Digital Library
See the collection of DevSecOps resources insights.sei.cmu.edu/library/finding-your-way-in-devops/.

For our blog series on DevSecOps, visit insights.sei.cmu.edu/blog/topics/devsecops/.

About the SEI

The Software Engineering Institute is a federally funded research and development center (FFRDC) that works with defense and government organizations, industry, and academia to advance the state of the art in software engineering and cybersecurity to benefit the public interest. Part of Carnegie Mellon University, the SEI is a national resource in pioneering emerging technologies, cybersecurity, software acquisition, and software lifecycle assurance.

Contact Us