Carnegie Mellon University
Software Engineering Institute

Executing DevSecOps

with the Software Engineering Institute

How We Can Help

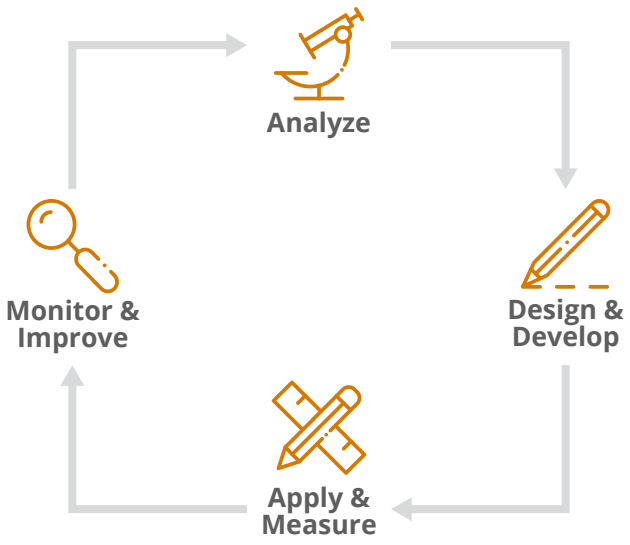
When you work with us, we help you establish robust DevSecOps capabilities by following a process that includes these four elements:

1. 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.

2. 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.

3. 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.

4. 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.



Features and Benefits of DevSecOps

Develop software systems with consistently higher quality and accuracy of project budgeting and estimation.

Increase the visibility of development to stakeholders and get their input about features for the next release as it is being developed.

Engage stakeholders early and consistently throughout the SDLC, leading to fewer defects and more accurate requirements.

Build trust among software developers and IT staff, enabling organic process improvement and risk mitigation.

Maximize the business value of software development by enabling technical staff to adapt to changing requirements or environmental factors.

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

For more information about SEI DevSecOps, visit our website at **sei.cmu.edu/our-work/devsecops**.

Find out about our prototypes, tools, methods, curricula, and more at **sei.cmu.edu/education-outreach**.

Find Us on GitHub at **github.com/cmu-sei**.

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

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