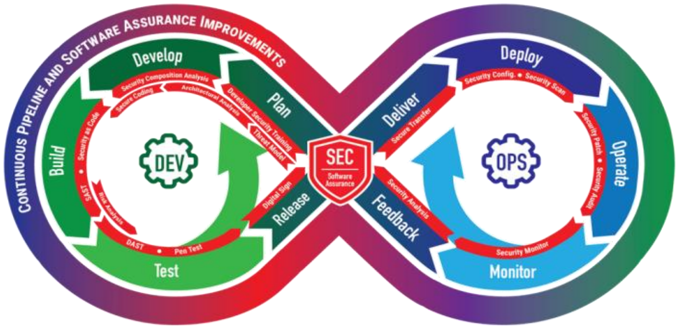
Carnegie Mellon University
Software Engineering Institute

The Platform Independent Model

Systems Engineering Meets DevSecOps for Secure Development

Many enterprises and government programs recognize that adversaries may abuse weaknesses in a DevSecOps pipeline to inject exploitable vulnerabilities into their products and services. Consequently, developers practicing DevSecOps need a way to manage software-intensive development, cybersecurity, and operations activities conducted across distributed systems. To help meet this challenge, the SEI has developed an approach combining model-based systems engineering (MBSE) and the SEI DevSecOps Platform Independent Model (PIM) to facilitate analysis, evaluation, and management of the cybersecurity risks associated with DevSecOps pipelines.



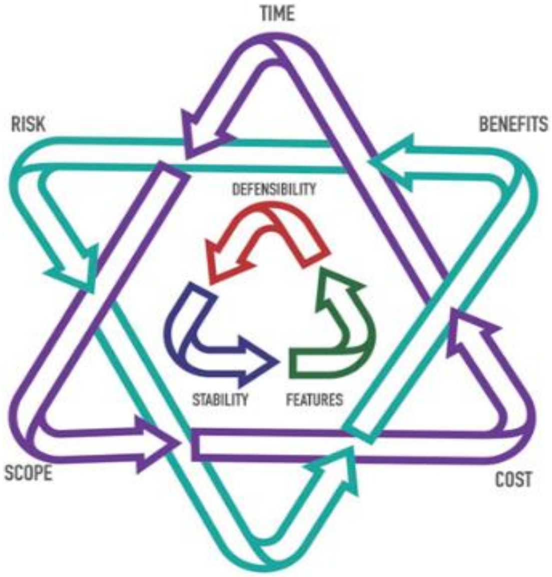
The DevSecOps Infinity Diagram

Our approach focuses on ensuring that the DevSecOps pipeline and its associated products are implemented in a secure, safe, and sustainable way; are sufficiently free from vulnerabilities; and function only as intended. To do so, the PIM provides a reusable reference architecture for DevSecOps pipelines. It explicitly defines the people, tools, processes, and associated interactions (as illustrated in the DevSecOps infinity diagram) needed to construct and operate a DevSecOps pipeline and build a product.

Ultimately, the PIM provides analysts with a minimum set of MBSE tools to help with threat identification, analysis, documentation, and subsequent mitigations.

Using the PIM to Mitigate Cybersecurity Threats

Most threat modelers focus only on the product and miss the pipeline in their analysis. Threat modelers need to focus on the *entire* attack surface. Using the PIM, developers can model and manage cybersecurity threats, modeling DevSecOps as an interaction between people and subsystems within a system. The PIM not only provides state-of-the-art modeling of cybersecurity factors concentrated on supporting risk analysis, safety analysis, and analysis of solutions for cyber-physical systems, but it also provides a universal threat modeling methodology that enables cybersecurity threat analysis at any stage of a system lifecycle. The PIM security view captures all cybersecurity data, including results of threat modeling activities, such as threats and threat scenarios, attack



DevSecOps Equities

types, and relationships with corresponding threat actors.

Organizations must balance risk, quality, and benefits within their time, scope, and cost constraints. The DevSecOps PIM is designed to set the stage by defining what must be considered within a platform-specific DevSecOps pipeline to reflect these properties within reasonable constraints to meet the desired mission objectives and vision.

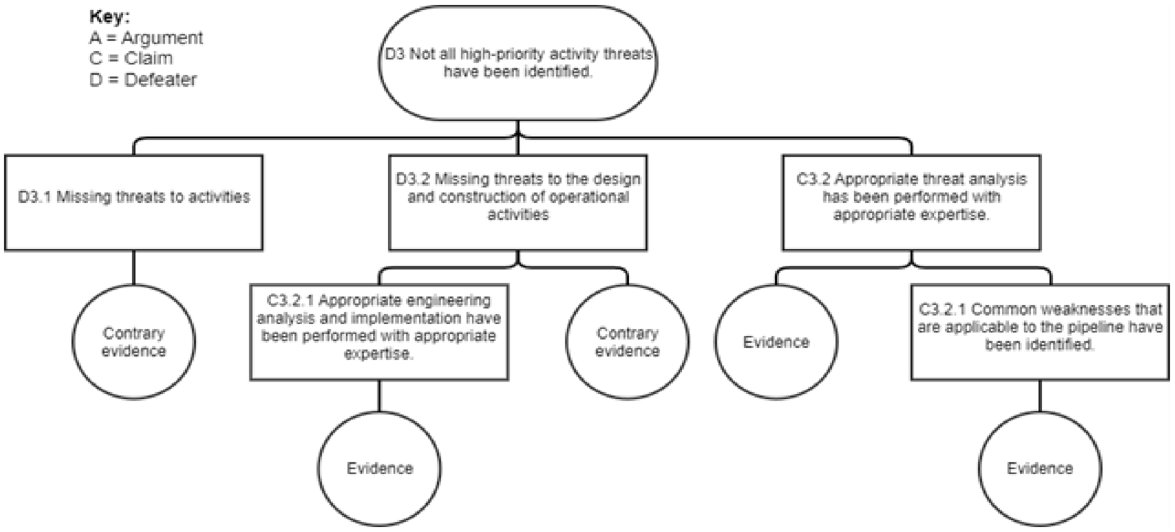
Assuring a DevSecOps Pipeline

Builders and evaluators can use an assurance case to reason about the degree of security for both the pipeline and the product. The DevSecOps PIM can highlight what elements are needed to frame a software assurance case by showing how gathered evidence can be combined into an argument demonstrating that the risks associated with a given pipeline instance have been adequately addressed.

With this information, the organization can make risk-based choices that assure the pipeline functions only as intended while minimizing the risk of adversaries using the pipeline itself to exploit the organization’s products or services. Utilizing MBSE-supported threat modeling methodology in this way also helps organizations impose methodological rigor and formalize assurance activities in the early stages before operational evidence data becomes available.

Pilot Program

We are looking for organizations to work with us to pilot the SEI DevSecOps PIM in a development project as a reference architecture for building an assurance case. We encourage interested parties to contact us at the number and address below.


Key:
A = Argument
C = Claim
D = Defeater
D3 Not all high-priority activity threats have been identified.
D3.1 Missing threats to activities
D3.2 Missing threats to the design and construction of operational activities
C3.2 Appropriate threat analysis has been performed with appropriate expertise.
Contrary evidence
C3.2.1 Appropriate engineering analysis and implementation have been performed with appropriate expertise.
Contrary evidence
Evidence
C3.2.1 Common weaknesses that are applicable to the pipeline have been identified.
Evidence
Evidence

Example Assurance Case Argument Formulated with the PIM

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu