Integration of DevSecOps, Model Based Engineering and Cybersecurity

Carol Woody, Ph.D.

Nataliya Shevchenko

December 2020

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-1098

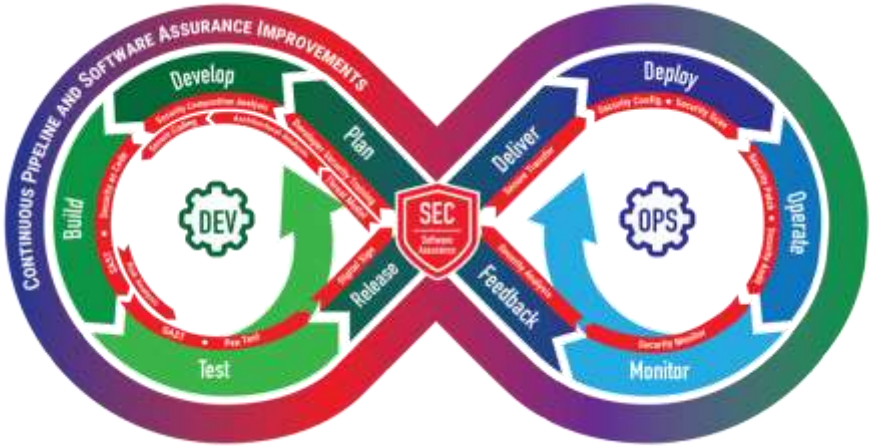
Today, Operations Plays Whac-a-mole Chasing Attacks

Rapid delivery of features is prioritized over defensibility, reliability, and stability.

Operational missions are jeopardized by weak designs that allow attackers to leverage the many vulnerabilities.

Without the ability to perform formal analysis of a system's numerous parameters, the only option is to react and hope for the best.

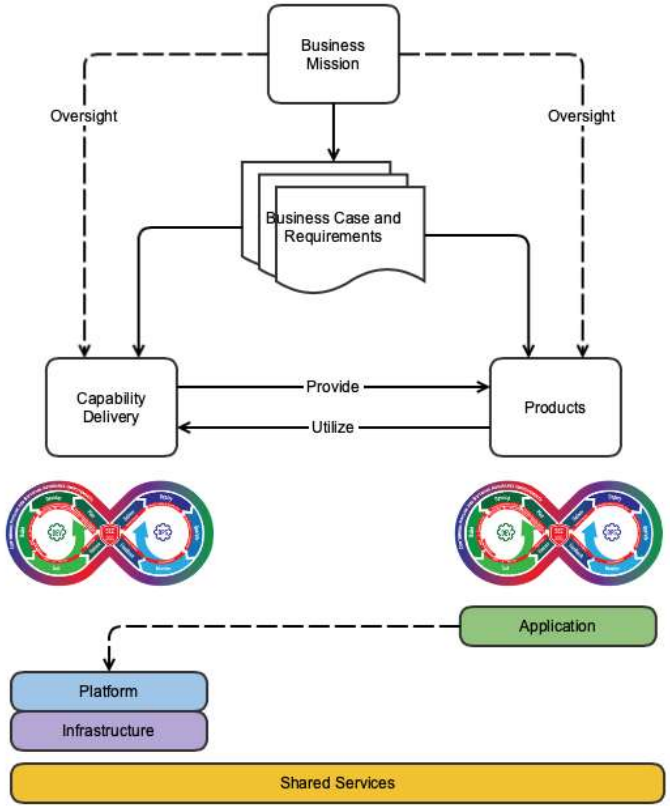
DevSecOps (DSO): integrating automation and development for continuous delivery



DSO is an approach that integrates development (Dev), security (Sec), and delivery/operations (Ops) of software systems to reduce the time required to move from need to capability and provide high software quality.

The pipeline is **not a system to be built or acquired**, it is a personal and organizational **mindset** defining processes for the rapid development, fielding, and operations of software and software-based systems **utilizing automation where feasible** in order to achieve the desired throughput of new features and capabilities.

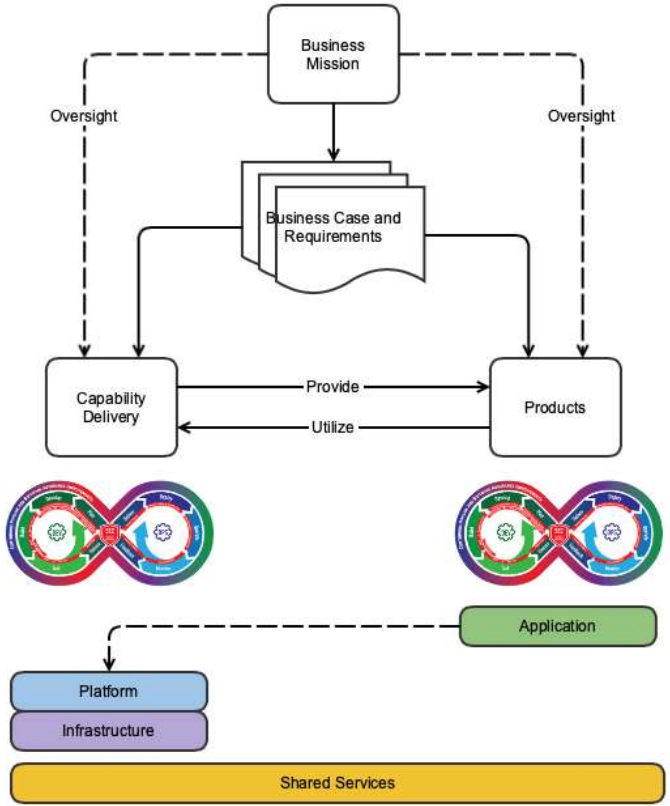
Challenge 1 for DSO: connecting process, practice, & tools



Creation of the DevSecOps (DSO) pipeline for building the product is not static.

- Tools for process automation must work together and connect to the planned infrastructure
- Everything is software and all pieces must be maintained but responsibility will be shared across multiple organizations (Cloud for infrastructure, 3rd parties for tools and services)

Challenge 2 for DSO: cybersecurity of pipeline and product



Managing and monitoring all of the various parts to ensure the product is built with sufficient cybersecurity and the pipeline is maintained to operate with sufficient cybersecurity is complex. Cybersecurity demands effective governance to address:

- What trust relations will be acceptable, and how will they be managed?
- What flow control and monitoring are in place to establish that the pipeline is working properly? Are these sufficient for the level of cybersecurity required?
- What compliance mandates are required? How are they addressed by the pipeline? Is this sufficient?

Our Approach and Why We Think It Will Be Successful

Approach

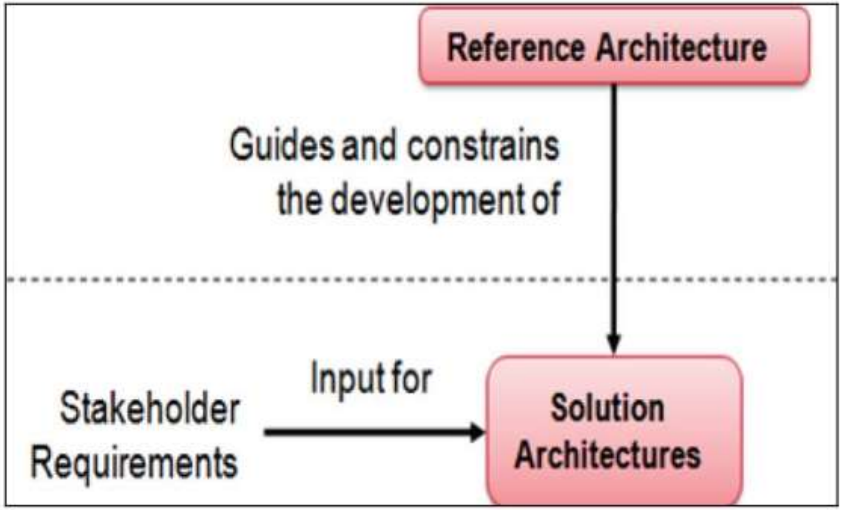
Build a DSO Platform Independent Model (PIM) using a model-based engineering methodology. The model will encode the complex socio-technical system of tools, processes, and human interactions within a DSO pipeline.

Reason for Success

- A DSO PIM will bridge the gap between multiple high-level system and infrastructure concept/views and actual instantiations.
- A DSO PIM will provide a single source of truth in which multiple perspectives (system stakeholders, cybersecurity, system operations) and views can be analyzed.

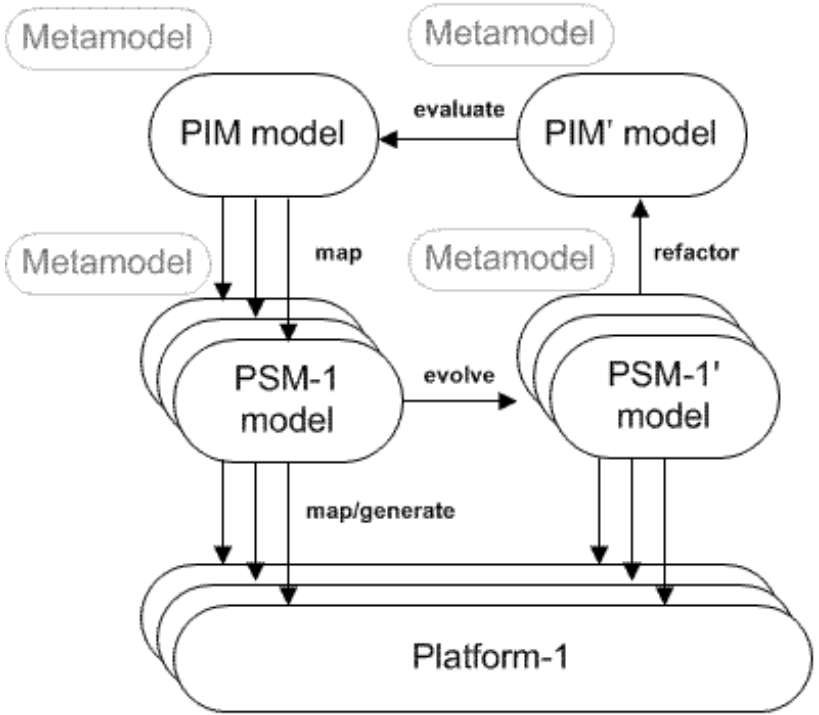
Reference Architecture/Platform Independent Model (PIM)

A **Reference Architecture** is an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.



A PIM is a general and reusable model of a solution to a commonly occurring problem in software engineering within a given context, and is independent of the specific technological platform used to implement it.

PIM Provides a Blueprint for the Platform-Specific Model (PSM)



This approach will enhance an organizations ability to:

- Specify the DSO requirements to the lead system integrators who need to develop a PSM that integrates organizational needs into both the system and pipeline
- Assess and analyze alternative pipeline functionality and feature changes as the system evolves
- Apply DSO methods to complex systems that do not follow well-established software architectural patterns commonly used in industry
- Provide a basis for threat and attack surface analysis to build a cyber assurance case

Future Operations Play a New Game - Topple

PIM will explicitly identify points (e.g. requirements, constraints, and conditions) that should be addressed or mitigated as well as mechanisms to manage coverage of these points. PSMs will present solutions that address these mandated points.

Through proper balance all participants (development, cybersecurity, operations, and governance) can play Topple indefinitely.

Contact Information

Carol Woody, Ph.D.

cwoody@cert.org

Nataliya Shevchenko

san@cert.org

Web Resources
https://sei.cmu.edu/