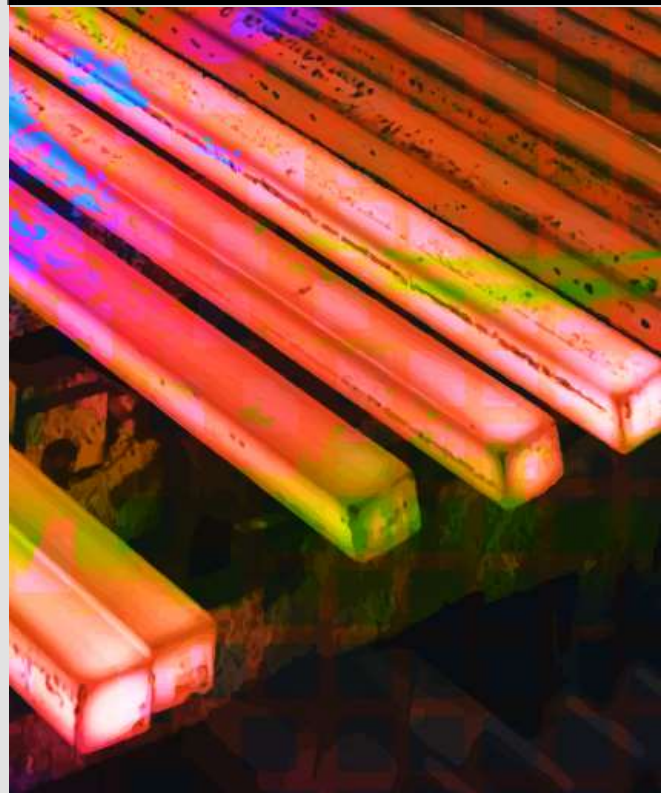
Carnegie Mellon University
Software Engineering Institute

Design & Develop to Deploy Securely



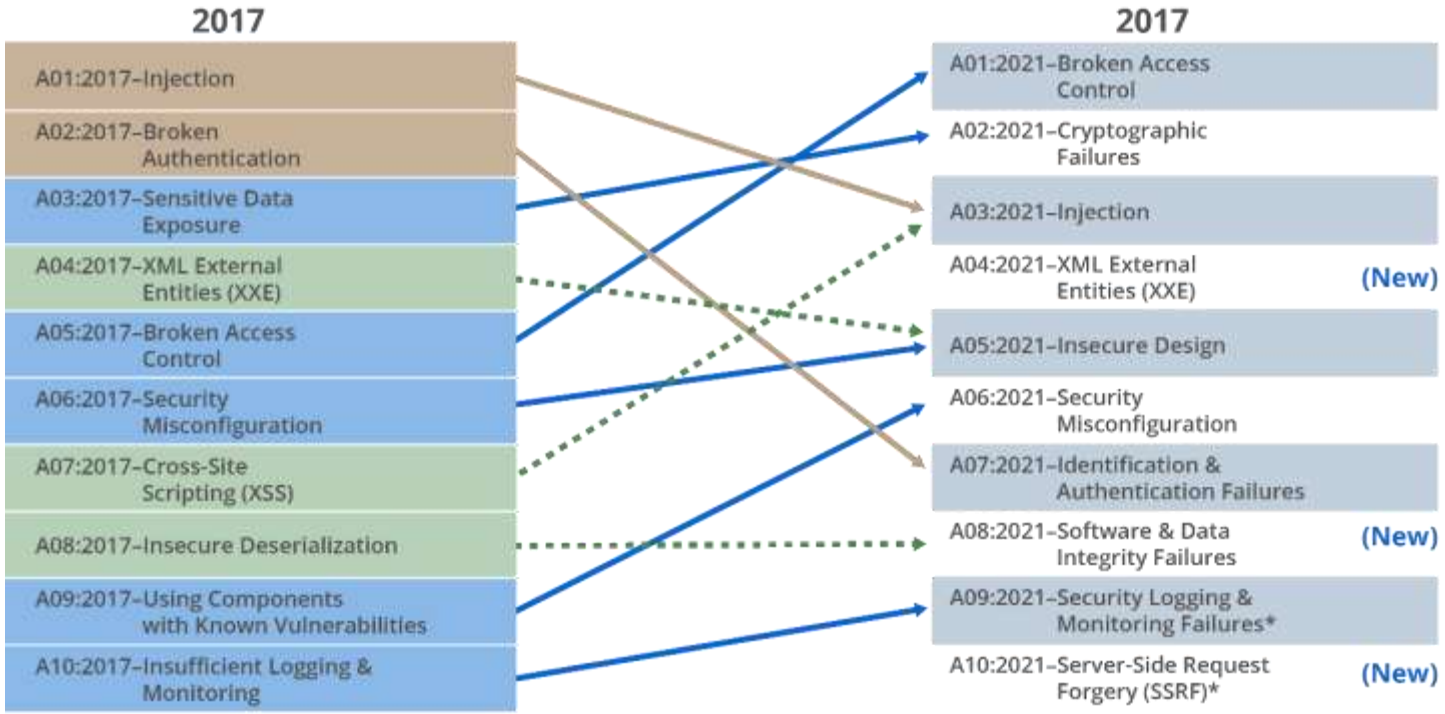
APRIL 25, 2023

Hasan Yasar
Technical Director and Faculty Member

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.

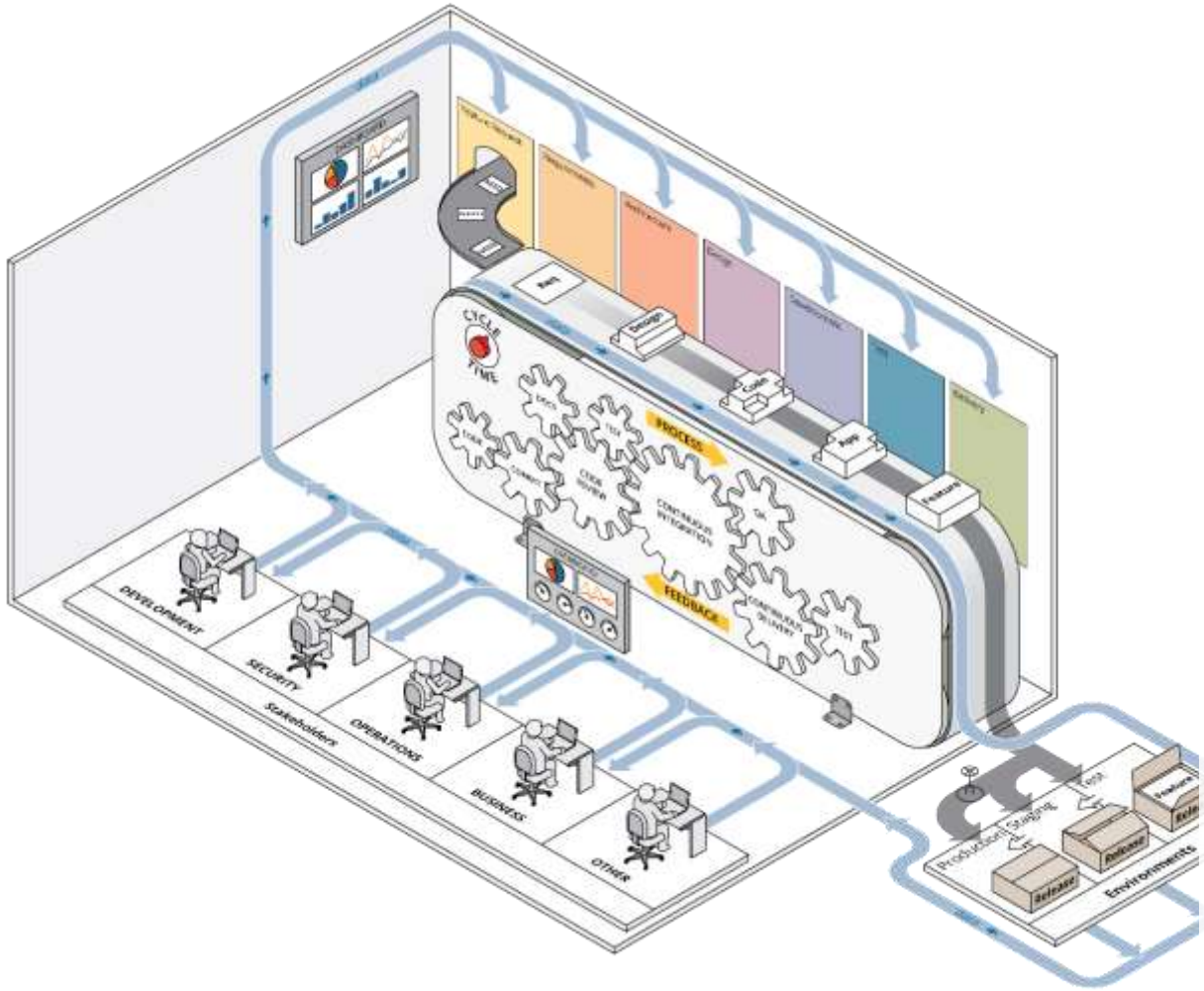
DM23-0402

Smarter software requires safer and more secure **design**, **development**, and **deployment** into **secure** infrastructures.



Is Security All About Tools?

DevSecOps

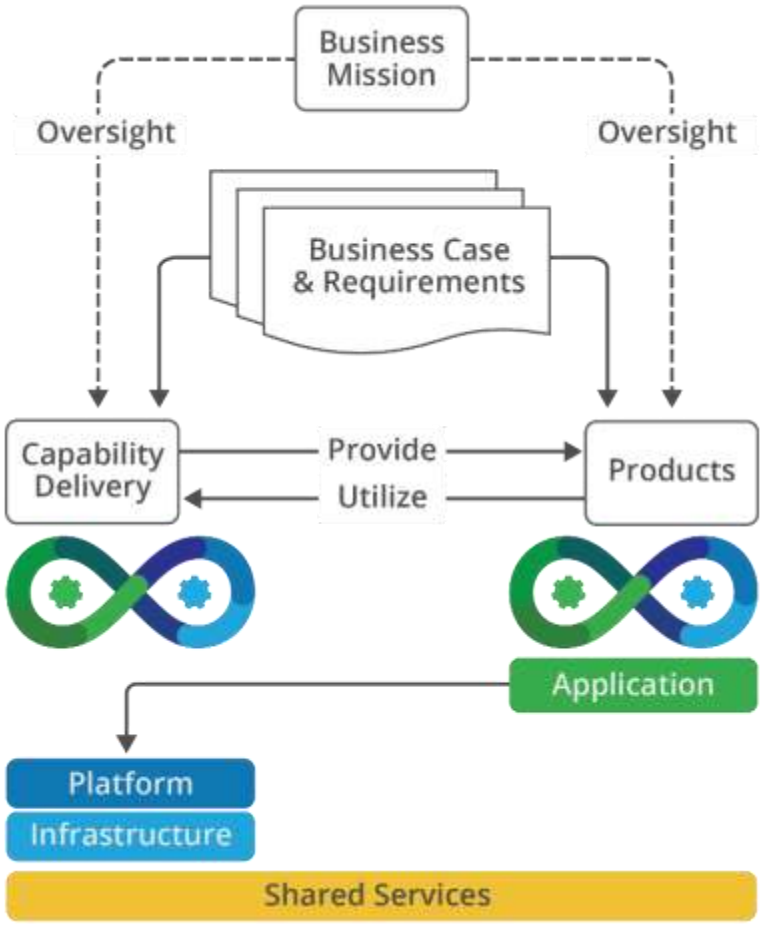


- "DevOps is a set of principles and practices which enable better communication and collaboration between relevant stakeholders for the purpose of specifying, developing, continuously improving, and operating software and systems products and services." [1]

- "DevSecOps is a cultural and engineering practice that breaks down barriers and opens collaboration between development, security, and operations organizations using automation to focus on rapid, frequent delivery of secure infrastructure and software to production. It encompasses intake to release of software and manages those flows predictably, transparently, and with minimal human intervention/effort." [2]

[1] IEEE 2675 *DevOps Standard for Building Reliable and Secure Systems Including Application Build, Package and Deployment*
[2] *DevSecOps Guide: Standard DevSecOps Platform Framework*. U.S. General Services Administration. https://tech.gsa.gov/guides/dev_sec_ops_guide.

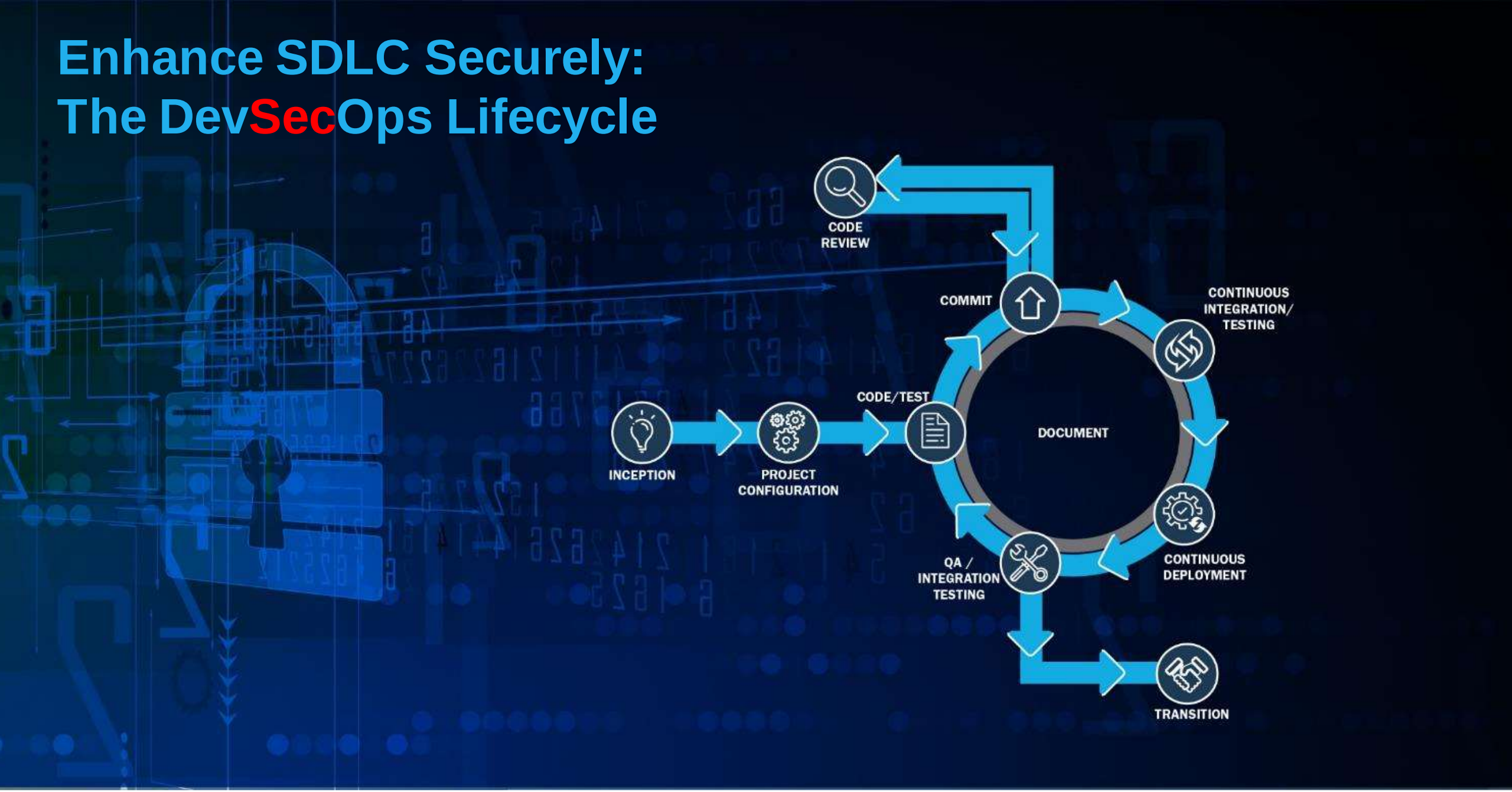
DevSecOps Goal



DevSecOps-oriented enterprises are driven by three concerns:

- *Business Mission* captures stakeholder needs and channels the whole enterprise to meet those needs. It answers the questions: *Why does the enterprise exist?* and *For Whom does the enterprise exist?*
- *Capability to Deliver Value* covers the people, processes, and technology necessary to build, deploy, and operate the enterprise's products.
- *Products* are the units of value delivered by the organization. Products utilize the capabilities delivered by the software factory and operational environments.

Enhance SDLC Securely: The DevSecOps Lifecycle

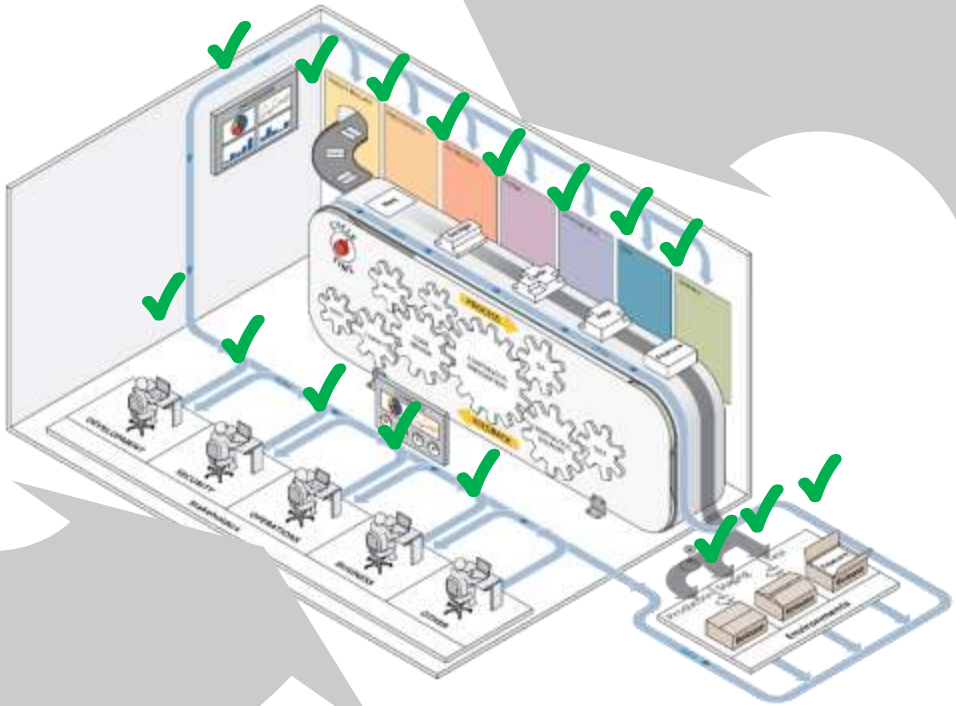


Understand How to Test, Validate, and Recognize as Secure Across DevSecOps

Think **Security** from Inception to Deployment, and improve every delivery by gathering *all metrics.*

Data…

- Attack Vector Details (e.g., IP, Stack Trace, Time, Rate of Attack)
- Server Disk Space, Load and Process Monitoring
- Application Performance
- Maximize Monitoring
- Change in Size to Code Base
- Most Active Code Contributors
- Most Changed Code Areas



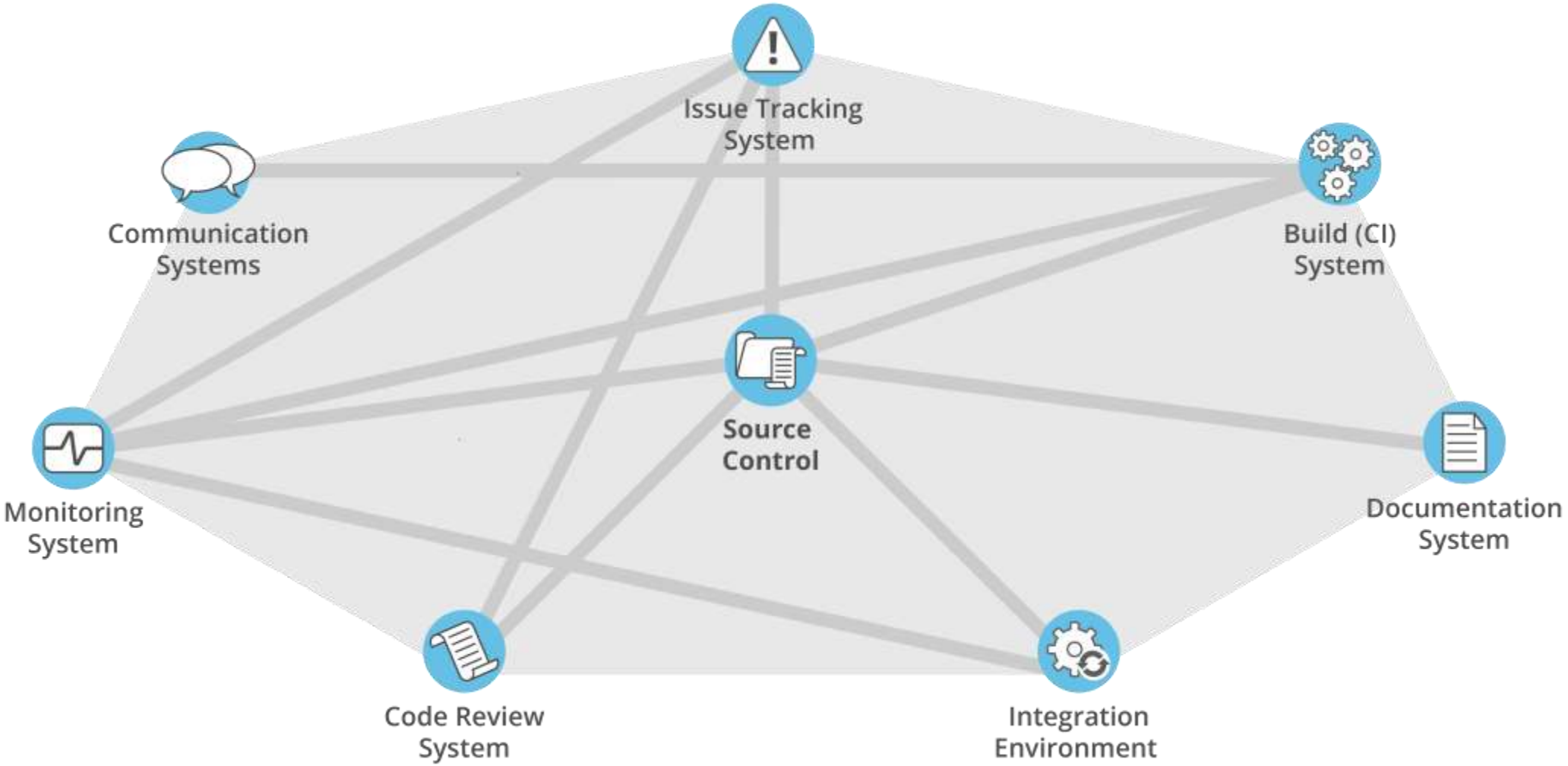
Data…

- Deployment Frequency
- Change Lead Time and Volume
- Change Failure Rate
- Mean Time To Recovery (MTTR)
- Mean Time to Detection (MTTD)
- Issue Volume and Resolution Time
- Time to Approval
- Time to Patch Vulnerabilities
- Development and Application Logging Availability
- Retention Control Compliance
- SAR Findings

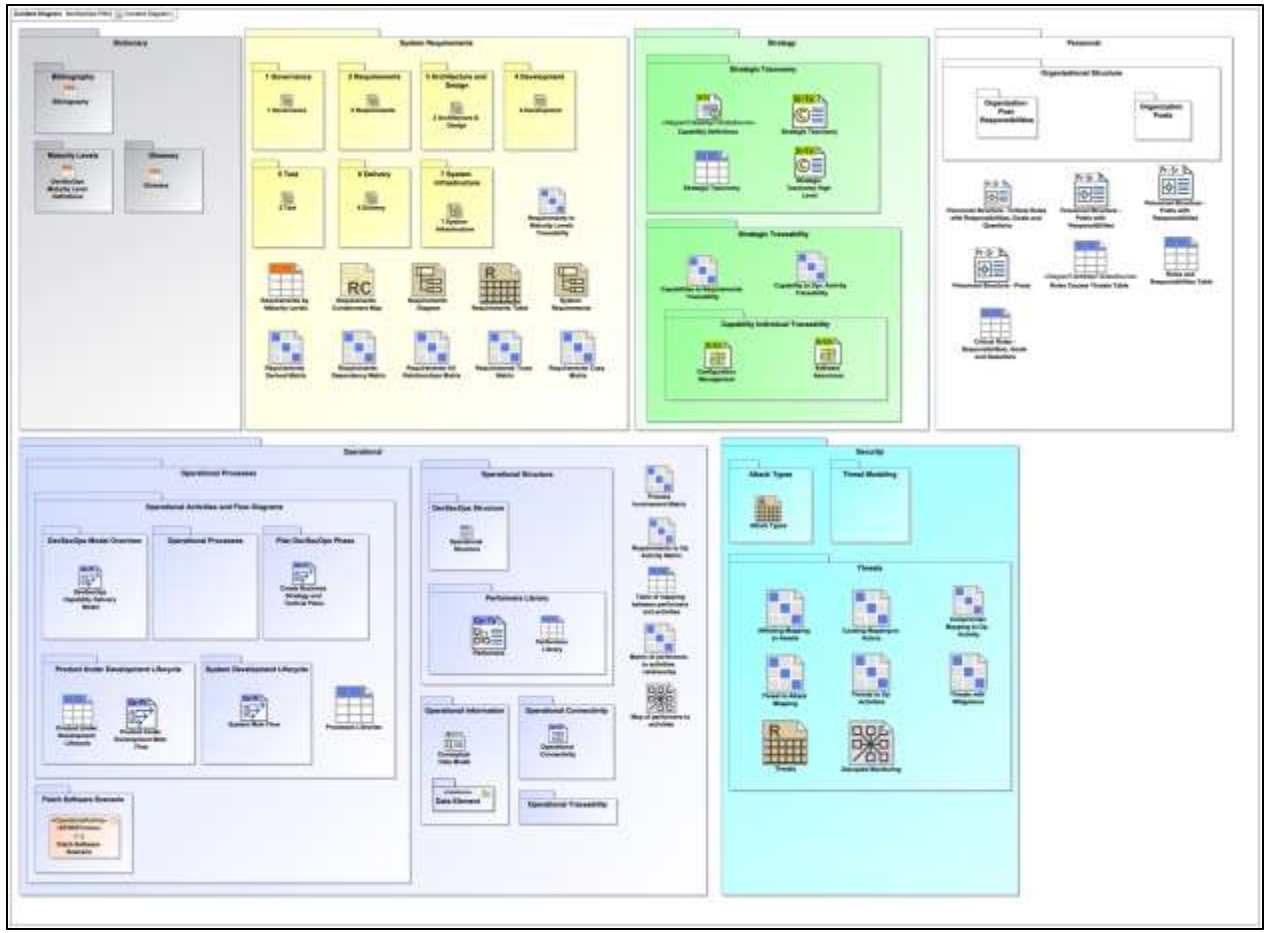
But How to Start?

Carnegie Mellon University
Software Engineering Institute

Don’t Let Tools Bend Your Security Posture; Start to Build a Secure Infrastructure



What Is the DevSecOps Platform Independent Model (PIM)?



- The PIM is an authoritative reference to fully design and execute an integrated Agile and DevSecOps strategy in which all stakeholder needs are addressed.
- It enables organizations to implement DevSecOps in a secure, safe, and sustainable way to fully reap the benefits of flexibility and speed available from implementing DevSecOps principles, practices, and tools.
- The PIM was developed to outline the activities necessary to consciously and predictably evolve the pipeline while providing a formal approach and methodology for building a secure pipeline tailored to an organization's specific requirements.
  https://cmu-sei.github.io/DevSecOps-Model/

What Does the DevSecOps PIM Provide?

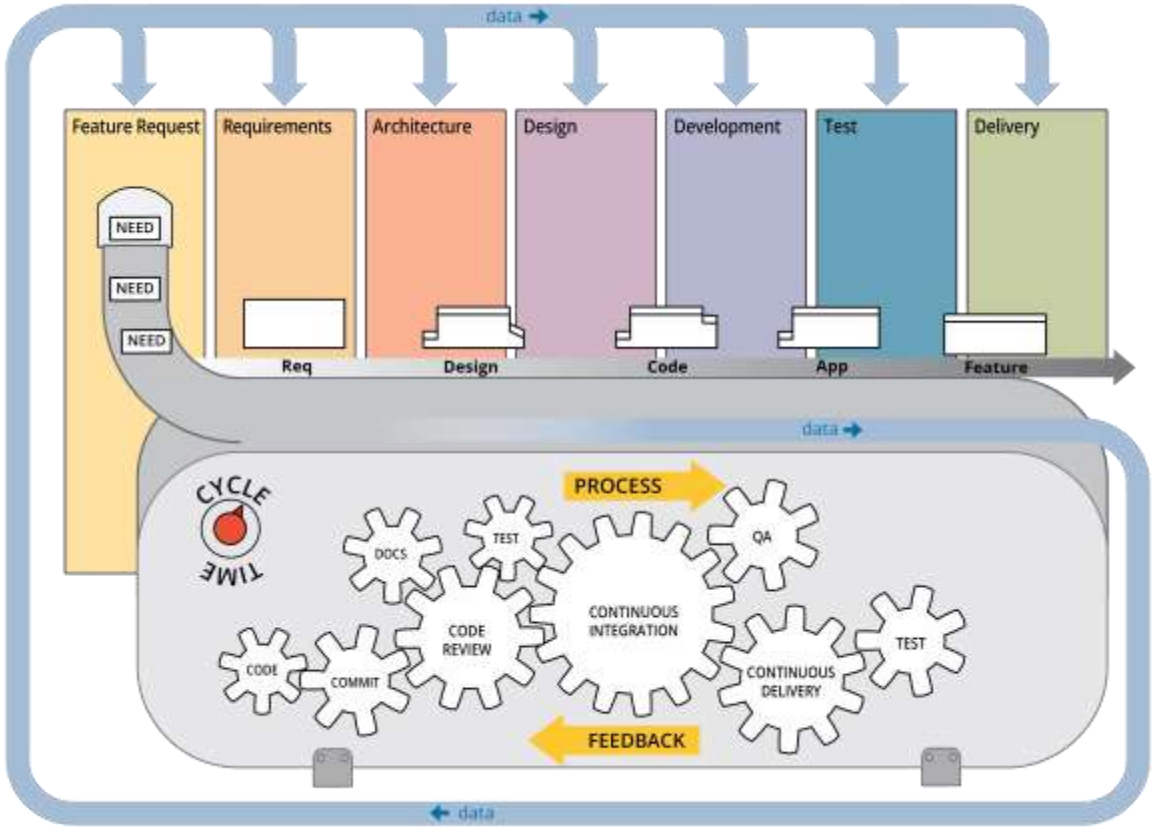
Consistent guidance and a modeling capability that ensure all proper layers and development concerns relevant to the needs of the organization, project, and team are captured

The basis for creating a DevSecOps platform-specific model (PSM) that can be incorporated into the product's model-based engineering approach as the DevSecOps master model is included in the product's model (This allows **proper modeling of DevSecOps design trades within a project's Analysis of Alternatives (AoA) processes**, resulting in less costly and more secure products.)

The **basis for metrics and documentation of tradeoffs** to be captured and analyzed through the model-based engineering approach (The model provides dynamic matrices that show whether or not those points were addressed, how they were addressed, and how well the module that corresponds to those points is covered.)

The **basis for performing risk modeling** against decisions and DevSecOps model-based engineering to ensure security controls and processes are properly selected and deployed

Security Is Not Just About Tools!
What Is Next?



Bring the security community into development early:

- The ideal time is during backlog grooming; the security operations center (SOC) team can develop security stories.
- This is particularly true for Scaled Agile Framework (SAFe) features and capabilities; use behavior-driven development (BDD) to define acceptance.

Aim for no surprises:

- There should be no hidden vulnerabilities; provide security to developers as soon as you have it.
- Remember that independence does not mean isolation.

Integrate. **Integrate. INTEGRATE!**

Automate as much as possible.

Deliver security with the design and code.

Carnegie Mellon University Software Engineering Institute

For More Information

DevSecOps: https://www.sei.cmu.edu/go/devops
DevOps Blog: https://insights.sei.cmu.edu/devops
Webinar Series: https://www.sei.cmu.edu/publications/webinars/
Podcast Series: https://www.sei.cmu.edu/publications/podcasts/

Contact Information

Hasan Yasar
Technical Director, Adjunct Faculty Member
Continuous Deployment of Capability,
Software Engineering Institute | Carnegie Mellon University
hyasar@cmu.edu