DevSecOps for the Enterprise

Luiz Antunes

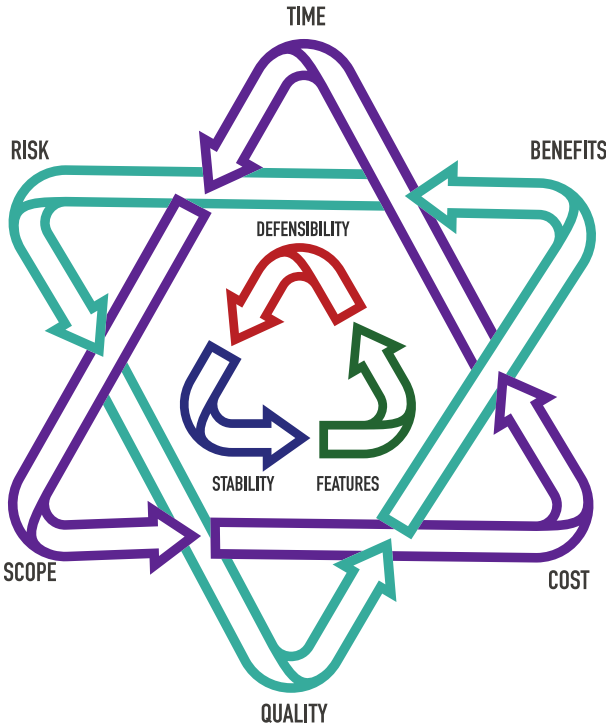
Hasan Yasar

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM22-1078

DevSecOps



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 [1].

A **DevSecOps Pipeline** attempts to seamlessly integrate "three traditional factions that sometimes have opposing interests:

- **development**; which values features;
- **security**, which values defensibility; and
- **operations**, which values stability [2]."

Not only does one need to balance the factions. They must do so in a way that balances **risk**, **quality** and **benefits** within their **time**, **scope**, and **cost** constraints.

[1] DevSecOps Guide: Standard DevSecOps Platform Framework. U.S. General Services Administration. https://tech.gsa.gov/guides/dev_sec_ops_guide. Accessed 17 May 2021
[2] DevSecOps Platform Independent Model, https://cmu-sei.github.io/DevSecOps-Model/

Enterprise-Scale Lean/Agile Delivery Capability

Scaling agility from the software project to the enterprise involves a host of socio-technical challenges

Enterprise Strategy Development - Expand rapid, incremental delivery models up and down the value stream. We deploy agile and lean strategies beyond software development to strategically improve enterprise capabilities:

- Measuring flow and delivery of value
- Simulation-rich CI/CD pipelines
- Systems Engineering discipline applied as intended, to the process and product
- Proactive accumulation of assurance information required for certification

Rapid Engineering Adoption - Implement best-of-breed incremental methods in environments where high levels of engineering discipline are necessary in complex, mission-critical cyber-physical products.

Architecturally-Aware Product & Process - Apply systematic view of enterprise architecture to the design of the product pipeline. Understanding the critical interplay of these systems enables rapid innovation through incremental change and AI, ML, MBSE adoption.

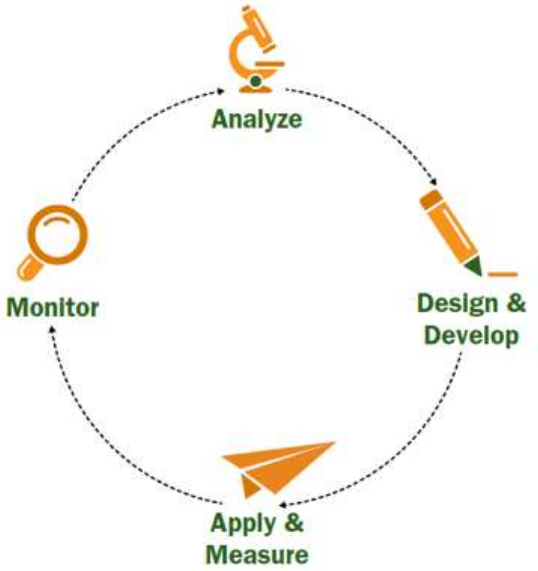
Coaching - We advise leaders and teams through iterative adoption of Lean, Agile methods in complex government/industry collaborations. Shoulder-to-shoulder coaching builds lasting organic capability.

Training - Our experienced instructors provide engaging classroom and virtual workshops for organizational and cultural change. Custom design for alignment with enterprise context uses table top exercises with real challenges instead of toy examples.

Assessment - We assess organizations' breadth of diffusion as well as depth of infusion for Lean/Agile approaches. Building beyond an inventory of practices, we focus on unique readiness and fit for transition of new methods.

Organizational Design and Capability Evolution - We design and support path-finding efforts and pilots for the evolution of the enterprise. Orderly experimentation and enterprise adoption of promising changes support a sustained focus on capability delivery.

DevSecOps Innovations and Solutions



Analyze Analyze an 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 & Develop - Develop a customized strategy and roadmap to improve organizational culture, process, and tools to support business needs and improve software development quality, transparency, and delivery while decreasing risk.

Apply & Measure - Provide tools and methods to enable process measurement capabilities. Apply a process improvement strategy according to the developed roadmap and measure the quantitative impact of DevOps on metrics for collaboration, quality, transparency, and process efficiency.

Monitor - Enable development managers and teams to independently monitor DevOps practices and engage in continuous data-driven improvements to tools and methods according unique organizational needs.

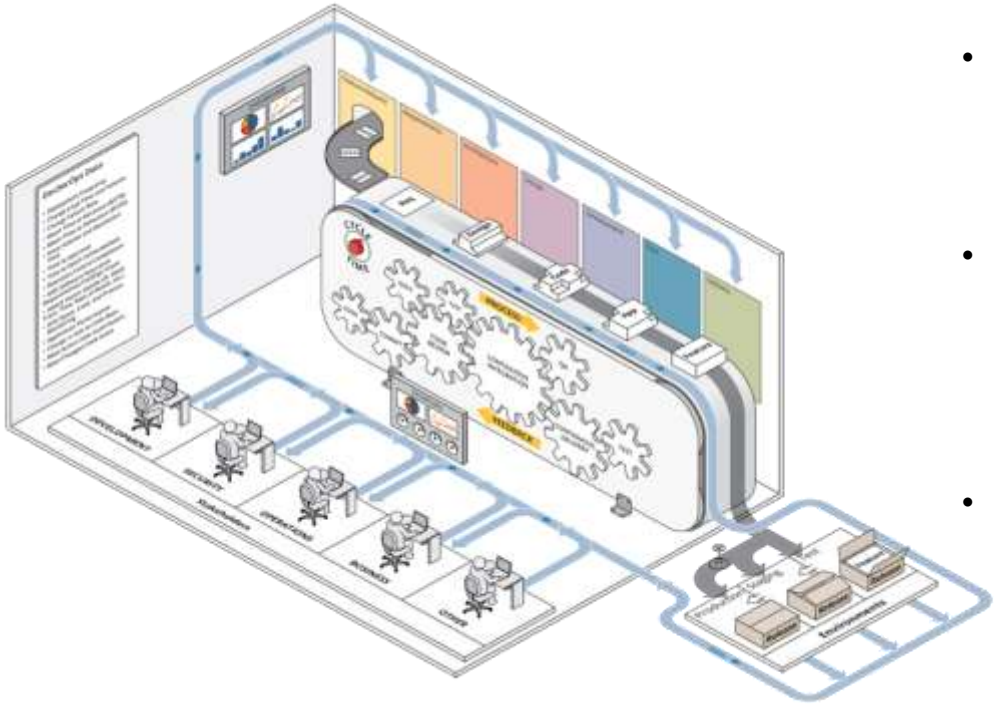
Training - We provide onsite or virtual courses that teach DevOps to managers, technical teams, and other stakeholder groups. We also offer advanced, hands-on DevOps training for development and operational teams that includes processes, tools, and practices.

Workshops - We conduct customized, hands-on workshops that provide comprehensive exercises to deliver practical training in DevOps tools and techniques throughout the SDLC, from inception to production.

Mentoring - By collaborating closely with teams and stakeholders, we facilitate cultural integration and assist in establishing practical guidelines to improve existing DevOps strategies and enhance collaboration among organizational teams.

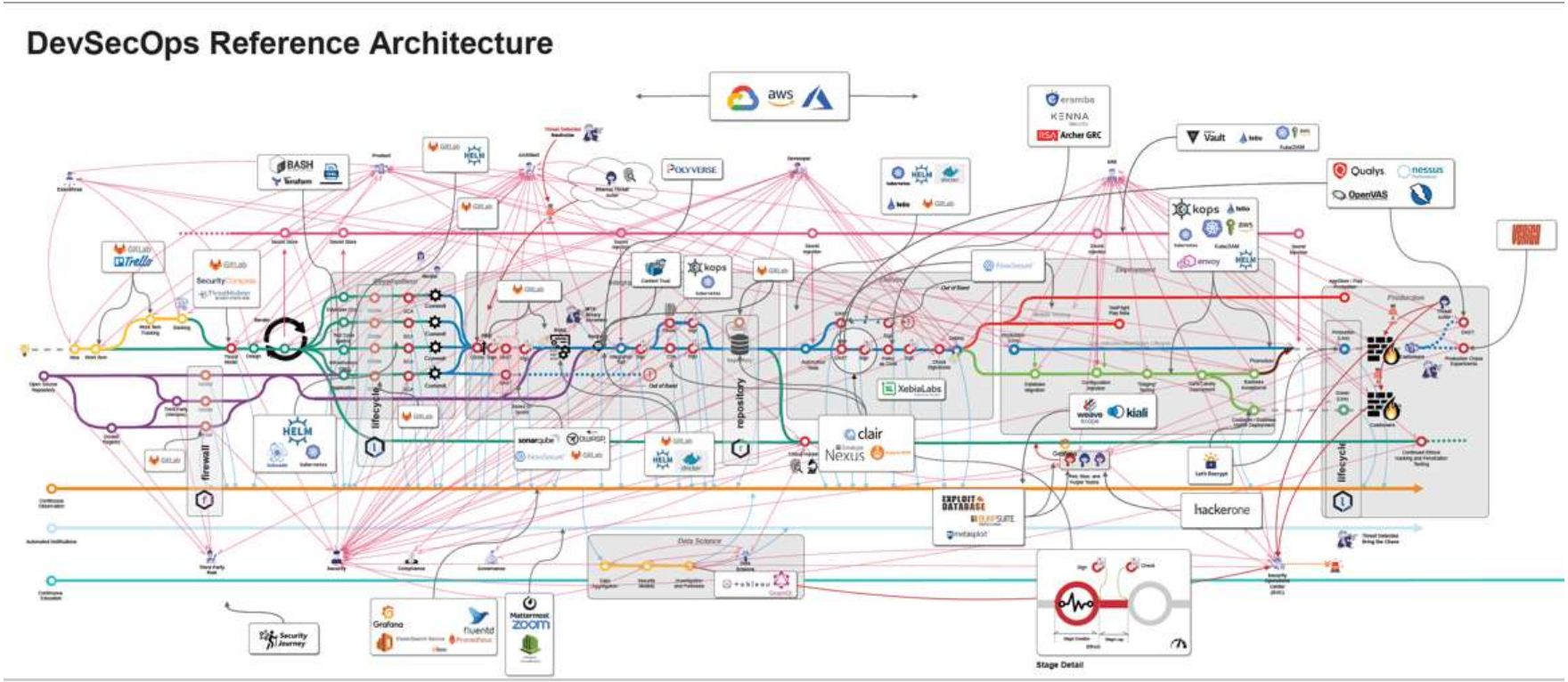
Engineering Support - Our highly experienced engineers assist in the implementation and measurement of DevOps tools and processes.

DevSecOps Platform Independent Model (PIM)



- Is an authoritative reference to fully design and execute an integrated Agile and DevSecOps strategy in which all stakeholder needs are addressed
- Enables organizations to implement DevSecOps in a secure, safe, and sustainable way in order to fully reap the benefits of flexibility and speed available from implementing DevSecOps principles, practices, and tools
- Was developed to outline the activities necessary to consciously and predictably evolve the pipeline, while providing a formal approach and methodology to building a secure pipeline tailored to an organization's specific requirements.

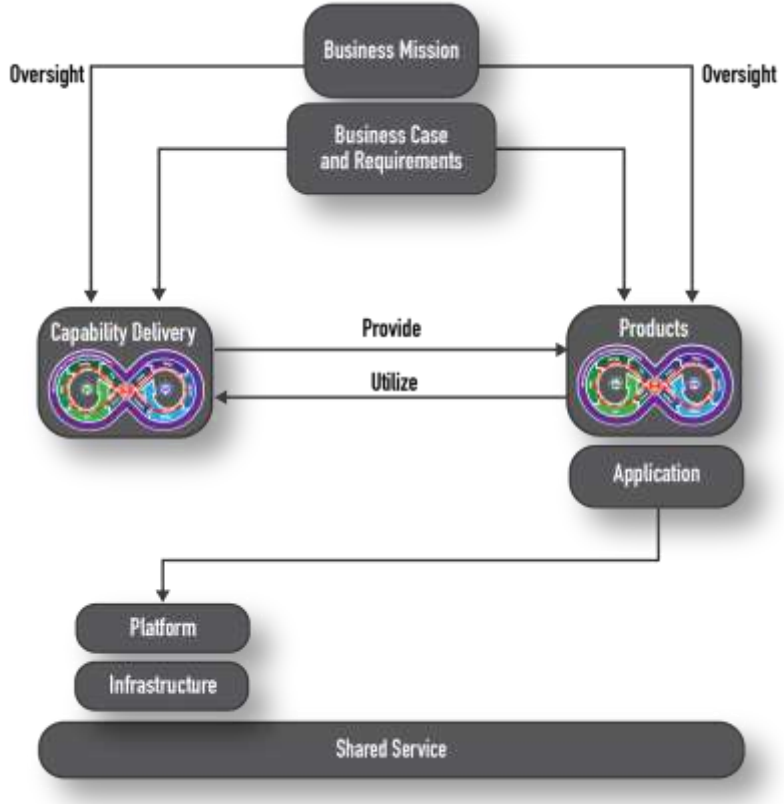
But It's getting really complicated to build



Challenges

- *Emerging technology challenges:* Incorporation of AI/ML models built, trained, tested, and validated within the pipeline
- *Hardware in the Loop challenges:* Application to Large Highly Regulated, Cyberphysical Systems of Systems
- *Governance and collaboration challenges:* Evolution of oversight, evaluation, and collaboration practices for nimble delivery of value
- *Architectural challenges:* Compatible architecture that supports iterative and incremental development

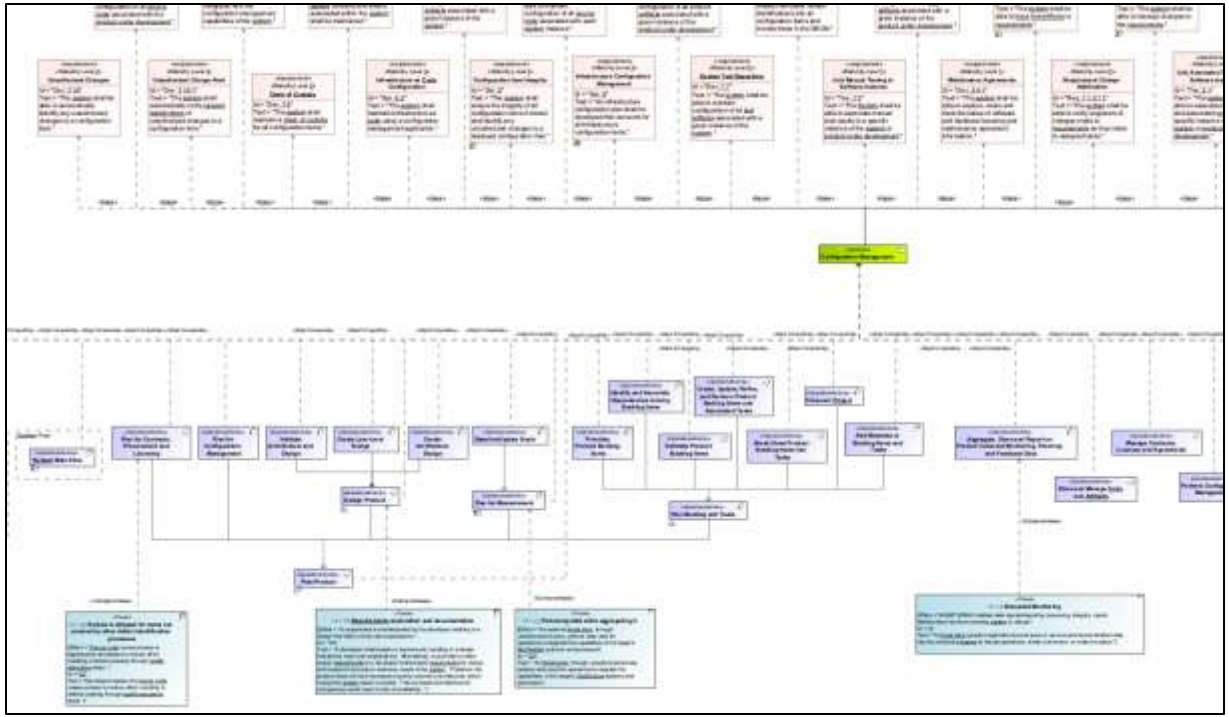
An Enterprise View of DevSecOps



A successful Enterprise DevSecOps strategy is driven by three aspects:

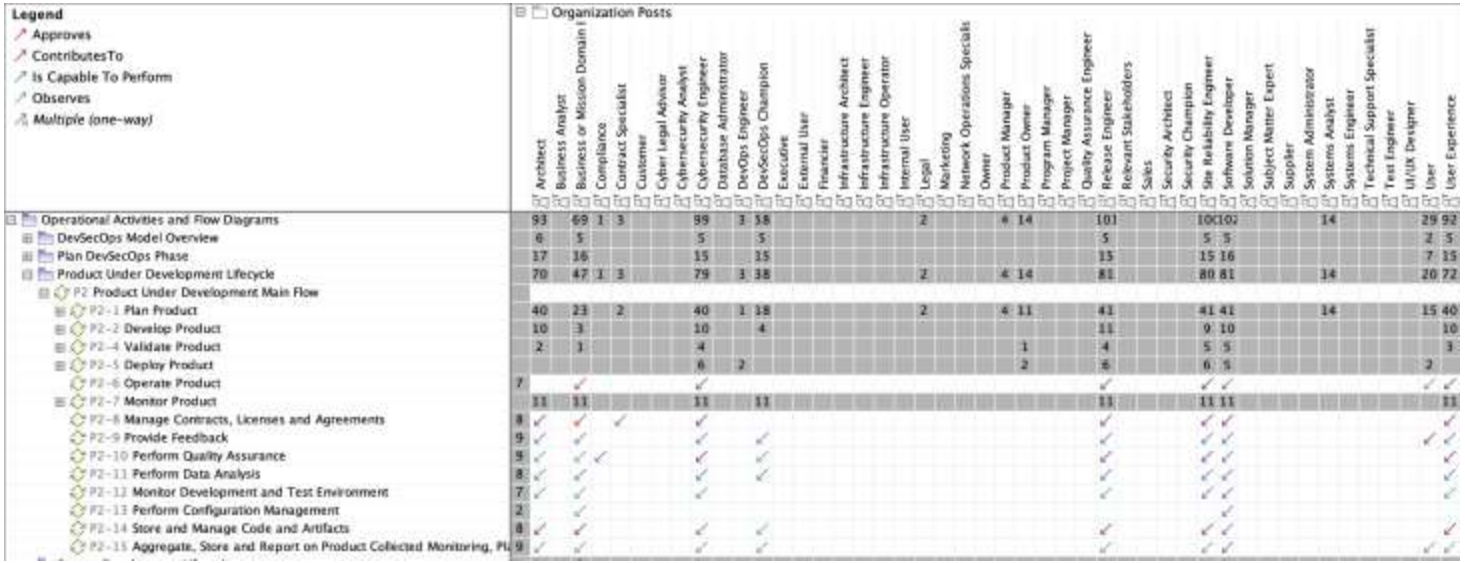
- **Business Mission** - Captures stakeholder needs and channels the whole enterprise in meeting those needs. It answer the questions *Why* and *For Whom* the enterprise exists
- **Capability to Deliver Value** - Covers the people, processes, and technology necessary to build, deploy, and operate the 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.

DevSecOps is a complex interconnected system



https://cmu-sei.github.io/DevSecOps-Model/

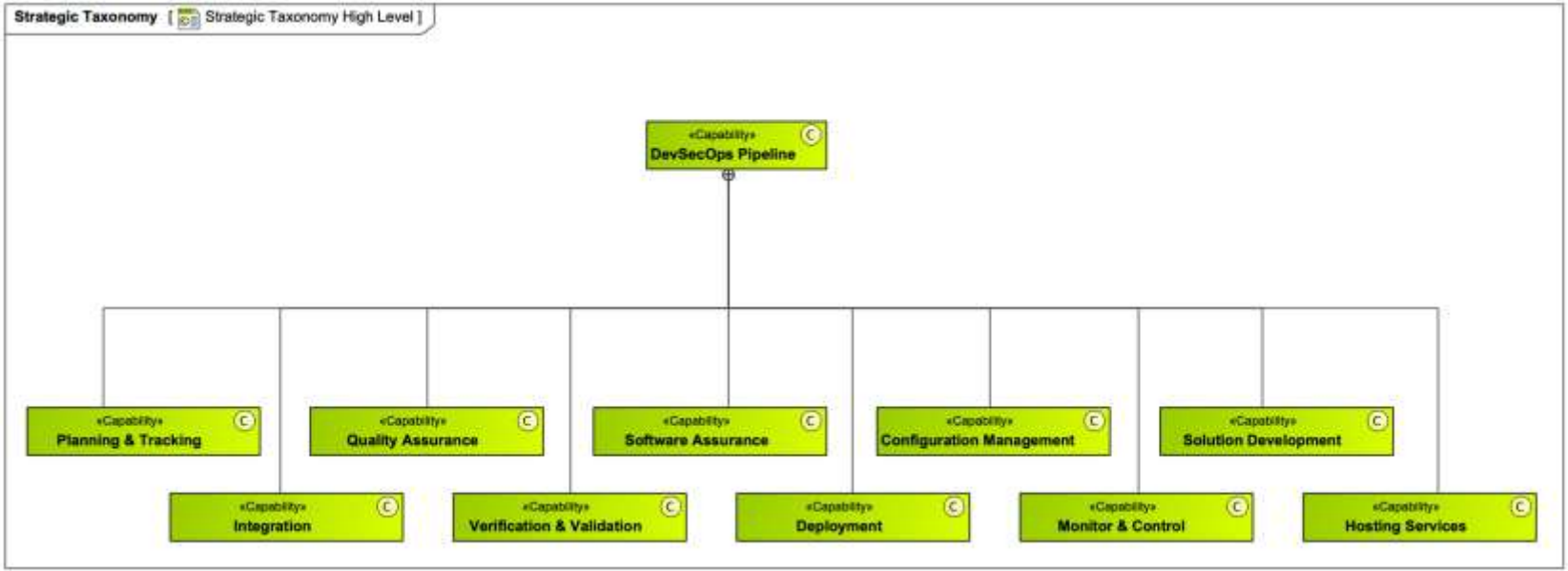
Everyone Plays a Role in DevSecOps



Legend	Organization Posts	Architect	Business Analyst	Business or Mission Domain	Compliance	Contract Specialist	Customer	Cyber Legal Advisor	Cybersecurity Analyst	Cybersecurity Engineer	Database Administrator	DevOps Engineer	DevSecOps Champion	Executive	External User	Financier	Infrastructure Architect	Infrastructure Engineer	Infrastructure Operator	Internal User	Legal	Marketing	Network Operations Specialis	Owner	Product Manager	Product Owner	Program Manager	Project Manager	Quality Assurance Engineer	Release Engineer	Relevant Stakeholders	Sales	Security Architect	Security Champion	Site Reliability Engineer	Software Developer	Solution Manager	Subject Matter Expert	Supplier	System Administrator	Systems Analyst	Systems Engineer	Technical Support Specialist	Test Engineer	UI/UX Designer	User	User Experience
Approves	Operational Activities and Flow Diagrams	93	69	1	3				99		3	38								2				4	14			101					100	102					14					29	92
ContributesTo	DevSecOps Model Overview	6	5						5			5																5					5	5										2	5
Is Capable To Perform	Plan DevSecOps Phase	17	16						15			15																15					15	16										7	15
Observes	Product Under Development Lifecycle	70	47	1	3				79		3	38								2				4	14			81					80	81					14					20	72
Multiple (one-way)	P2 Product Under Development Main Flow																																												
	P2-1 Plan Product	40	23		2				40		1	18								2				4	11			41					41	41					14					15	40
	P2-2 Develop Product	10	3						10			4																11					9	10											10
	P2-4 Validate Product	2	1						4																1			4					5	5											3
	P2-5 Deploy Product								6		2														2			6					6	5										2	
	P2-6 Operate Product	7		✓					✓																			✓					✓	✓										✓	✓
	P2-7 Monitor Product		11	11					11			11																11					11	11											11
	P2-8 Manage Contracts, Licenses and Agreements	8	✓	✓		✓			✓																			✓					✓	✓											✓
	P2-9 Provide Feedback	9	✓	✓					✓			✓																✓					✓	✓										✓	✓
	P2-10 Perform Quality Assurance	9	✓	✓	✓				✓			✓																✓					✓	✓											✓
	P2-11 Perform Data Analysis	8	✓	✓					✓			✓																✓					✓	✓											✓
	P2-12 Monitor Development and Test Environment	7	✓	✓					✓																			✓					✓	✓											✓
	P2-13 Perform Configuration Management	2		✓																														✓											
	P2-14 Store and Manage Code and Artifacts	8	✓	✓					✓			✓																✓					✓	✓											✓
	P2-15 Aggregate, Store and Report on Product Collected Monitoring, Pl	9	✓	✓					✓			✓																✓					✓	✓										✓	✓

Critical Roles mapped to Operational Activities

As a DevSecOps system matures, so will its capabilities



https://cmu-sei.github.io/DevSecOps-Model/

DevSecOps Maturity Levels

Term	Documentation
Maturity Level 1	Performed Basic Practices: This represents the minimum set of engineering, security, and operational practices that is required to begin supporting a product under development, even if only performed in an ad-hoc manner with minimal automation, documentation, or process maturity. This level is focused on minimal development, security, and operational hygiene.
Maturity Level 2	Documented/Automated Intermediate Practices: Practices are completed in addition to meeting the level 1 practices. This level represents the transition from manual, ad-hoc practices to the automated and consistent execution of defined processes. This set of practices represents the next evolution of the maturity of the product under development's pipeline by providing the capability needed to automate the practices that are most often executed or produce the most unpredictable results. These practices include defining processes that enable individuals to perform activities in a repeatable manner.
Maturity Level 3	Managed Pipeline Execution: Practices are completed in addition to meeting the level 1 and 2 practices. This level focuses on consistently meeting the information needs of all relevant stakeholders associated with the product under development so that they can make informed decisions as work items progress through a defined process.
Maturity Level 4	Proactive Reviewing and Optimizing DevSecOps: Practices are completed in addition to meeting the level 1-3 practices. This level is focused on reviewing the effectiveness of the system so that corrective actions are taken when necessary, as well as quantitively improving the system's performance as it relates to the consistent development and operation of the product under development.

Selecting the Appropriate Techniques

- Three Fundamental Factors
  1. Identifying **the ability of the organization** to adopt new techniques
     - Successful adoption requires the absorption of associated costs, as well as expending the required time and effort.
  2. Determining **the suitability of Agile and DevSecOps practices in the development** of a given product or system
     - Development and product characteristics play a large role in determining the suitability of a particular agile technique.
     - The desired product qualities also play a role in determining appropriate agile technique
  3. Determining **the suitability of Agile and DevSecOps practices for the organization** developing the product or system.

Adapted from Sidky, Ahmed; James Arther, *Determining the Applicability of Agile Practices to Mission and Life-critical Systems,* Proceedings of the 31st IEEE Software Engineering Workshop (SEW 2007). pp 3-12.

Areas of Focus

Lifecycle:

- Governance
- Requirements
- Architecture & Design
- Development
- Test
- Delivery
- System Infrastructure

Capabilities:

- Configuration Management
- Deployment
- Hosting Services
- Integration
- Monitor & Control
- Planning & Tracking
- Quality Assurance
- Software Assurance
- Solution Development
- Verification & Validation

Thank You

Luiz Antunes
Member of the Technical Staff / DevOps Engineer
Continuous Deployment of Capability
lantunes@sei.cmu.edu