

Using MBSE to Secure your DevSecOps Pipeline

**Carnegie
Mellon
University**
Software
Engineering
Institute

Timothy A. Chick
CERT Applied Systems Group Technical Manager, CMU-Software Engineering Institute
Adjunct Faculty Member, CMU-Software and Societal Systems Department (S3D)

Document Markings

Copyright 2023 Carnegie Mellon University.

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. The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM23-0208

Agenda

About DevSecOps

Challenges associated with DevSecOps

- **Challenge 1: Connecting process, practice, and tools**
- **Challenge 2: Cybersecurity of pipeline and product**

Addressing the Cybersecurity challenges with MBSE

About DevSecOps

Today: Program Office Whac-A-Mole

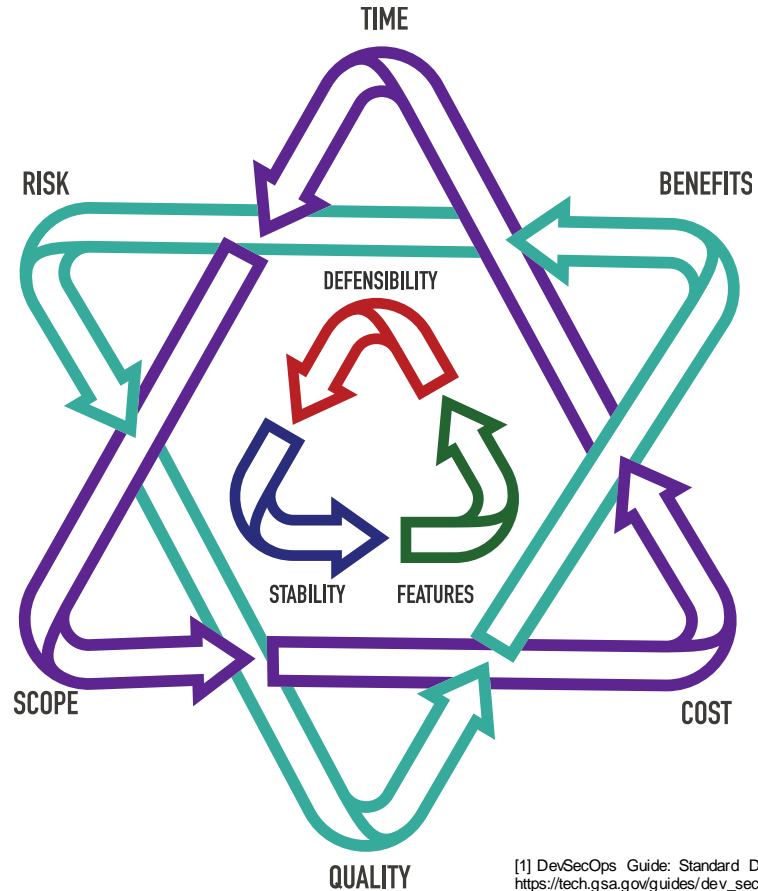


**Winning in Features and Effectiveness, but
Losing in Defensibility and Stability**

In June of 2020 a generally successful DoD program completed an **8 week “Hardening the Software Factory” effort** in order to address **accumulated technical debt** and to address **insufficient security and operations practices due to the narrow focus on speed of delivery**. These things occur, even in small relatively successful programs, when technical debt and insufficient security and operational practices are in place **due to lack of knowledge, experience, and reference material to fully design and execute an integrated DevSecOps strategy in which all stakeholder needs, including cybersecurity, are addressed**.

While playing Whac-A-Mole is inevitable, instead of missing the holes, or constantly hitting the same hole, the key is to fill in the holes.

DevSecOps: Modern Software Engineering Practices and Tools that Encompass the Full Software Lifecycle



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:

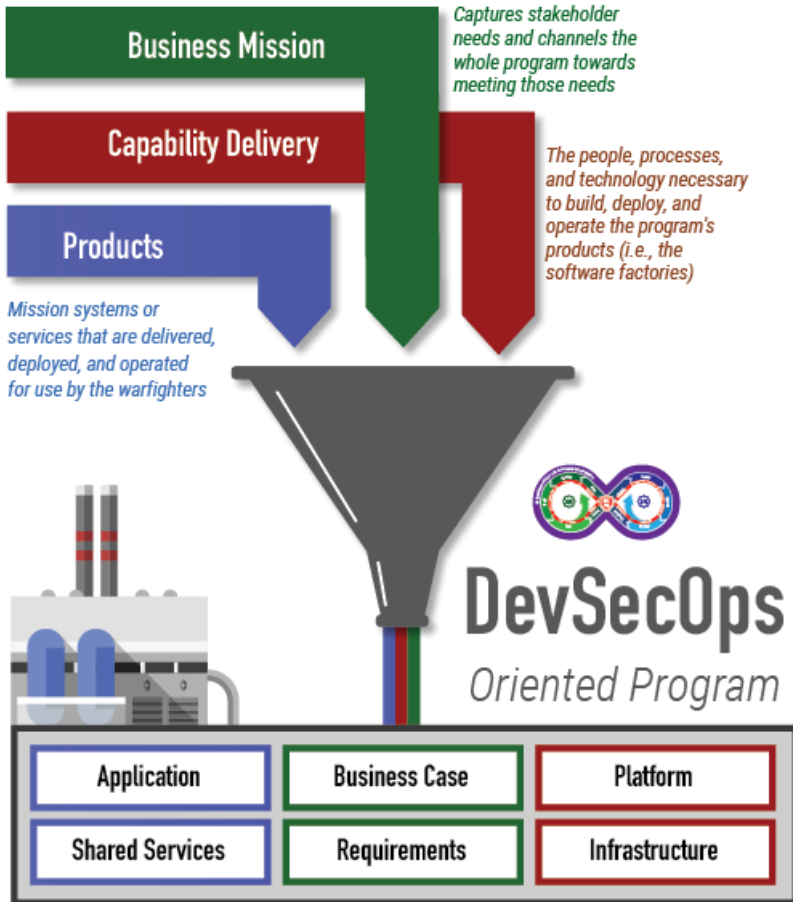
- **development**; which values features;
- **security**, which values defensibility; and
- **operations**, which values stability [2].”

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/>

A Program View

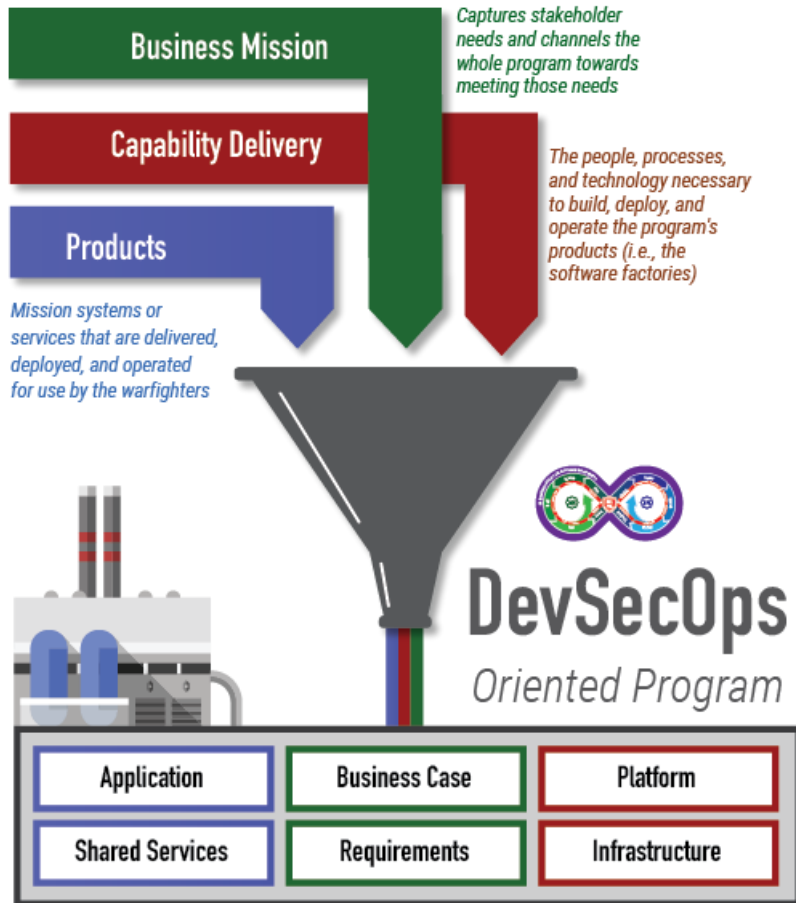


All software oriented programs are driven by three concerns:

- **Business Mission** – captures stakeholder needs and channels the whole program in meeting those needs. It answer the questions *Why* and *For Whom* the program exists
- **Capability to Deliver Value** – covers the people, processes, and technology necessary to build, deploy, and operate the program's products
- **Products** – the units of value delivered by the program. Products utilize the capabilities delivered by the software factory and operational environments.

Challenges Associated with DevSecOps

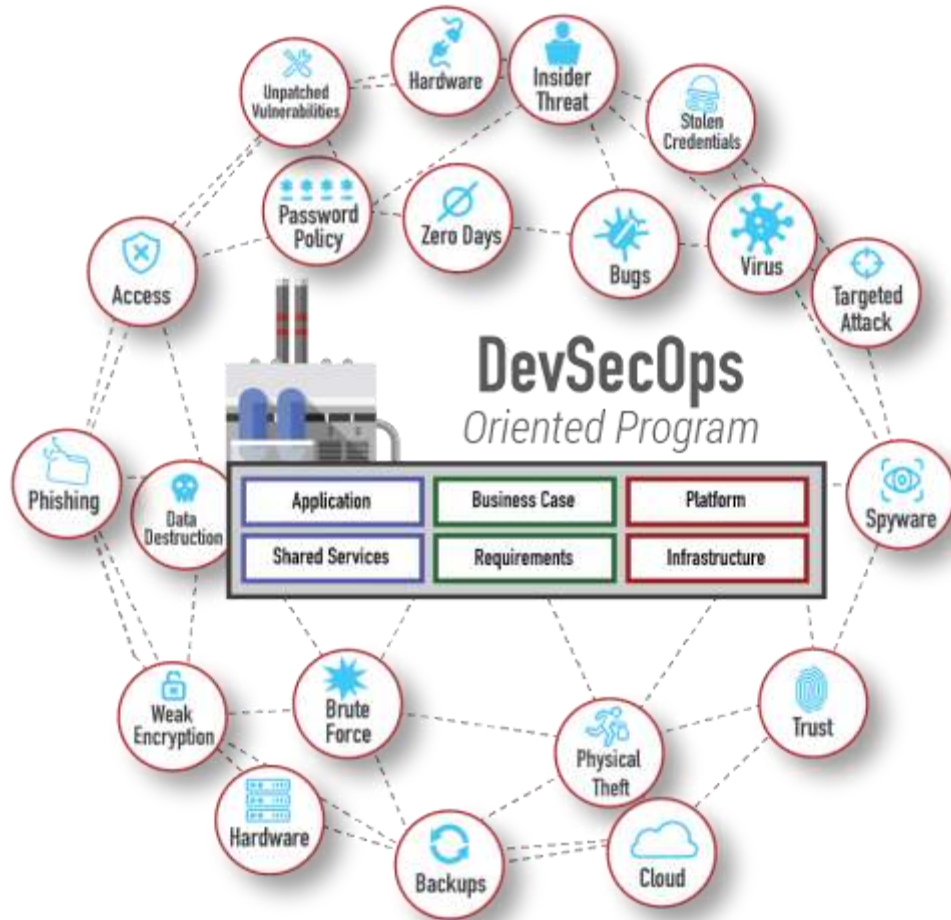
Challenge 1: connecting process, practice, and tools



Capabilities and Products are not static.

- Infrastructure and shared services are often maintained across multiple organizations
- Processes, practices, and tools must evolve to meet the needs of the products being built and operated
- Products must evolve to meet changing needs, defects found, and changes to other systems.

Challenge 2: Addressing Threats to both Pipeline and Product



The tight integration of Business Mission, Capability Delivery, and Products, using integrated processes, tools, and people, increases the attack surface of the product under development.

Managing and monitoring all the various parts to ensure the product is built with sufficient cybersecurity and the pipeline is maintained to operate with sufficient cybersecurity is complex.

How do you focus attention to areas of greatest concern for security risks and identify the attack opportunities that could require additional mitigations?

Using a capability service to attack a product isn't new



<https://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html>

“Steelworks compromise causes massive damage to furnace.

One of the most concerning was a targeted APT attack on a German steelworks which ended in the attackers gaining access to the business systems and through them to the production network (including SCADA). The effect was that the attackers gained control of a steel furnace and this caused massive damages to the plant.”

Software Assurance (SwA)

DoD definition:

“the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the **software functions in the intended manner.**”

[CNSS Instruction No. 4009; DoDi 5200.44 p.12]

SwA Curriculum Model definition:

Application of technologies and processes to achieve a required level of confidence that **software systems and services function in the intended manner**, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures.

[Mead, Nancy; Allen, Julia; Ardis, Mark; Hilburn, Thomas; Kornecki, Andrew; Linger, Richard; & McDonald, James. *Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum*. CMU/SEI-2010-TR-005. Software Engineering Institute, Carnegie Mellon University. 2010. <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9415>]

Risk

The perception of risk drives assurance decisions

- Assurance implementation choices (policies, practices, tools, restrictions) are based on the perception of threat and the expected impact should that threat be realized
- Perceptions are primarily based on knowledge about successful attacks
 - the current state of assurance is largely reactive
 - successful organizations learn from attacks and figure out how to react and recover faster and be vigilant in anticipating and detecting attacks
- Misperceptions are failures to recognize threats and impacts – “how could it happen to us?” or “it could not happen here!”

Attacker

There are no perfect protections against attacks.

There exists a broad community of attackers with growing technology capabilities able to compromise the confidentiality, integrity, and availability of any and all of your technology assets, and the attacker profile is constantly changing.

- The attacker uses technology, processes, standards, and practices to craft a compromise (socio-technical responses).
- Attacks are crafted to take advantage of the ways we normally use technology or designed to contrive exceptional situations where defenses are circumvented.

Mitigating Risk with Assurance Cases

Understanding risk is hard!

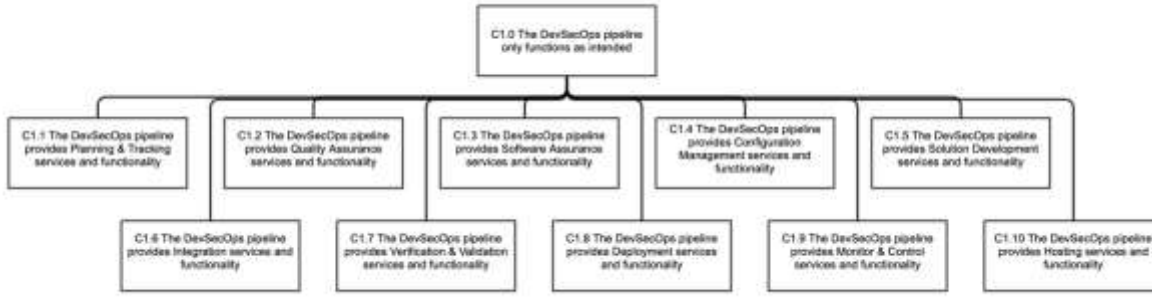
Without being able to quantify, or reason around, the cybersecurity risks associated with your product and DevSecOps pipeline, you will not be able to:

- properly balance between features, defensibility, and stability
- make necessary trade-off choices to achieve your organization's mission and vision in a cost-effective way

An assurance case can be used to reason about the adequacy for both the pipeline and the product.

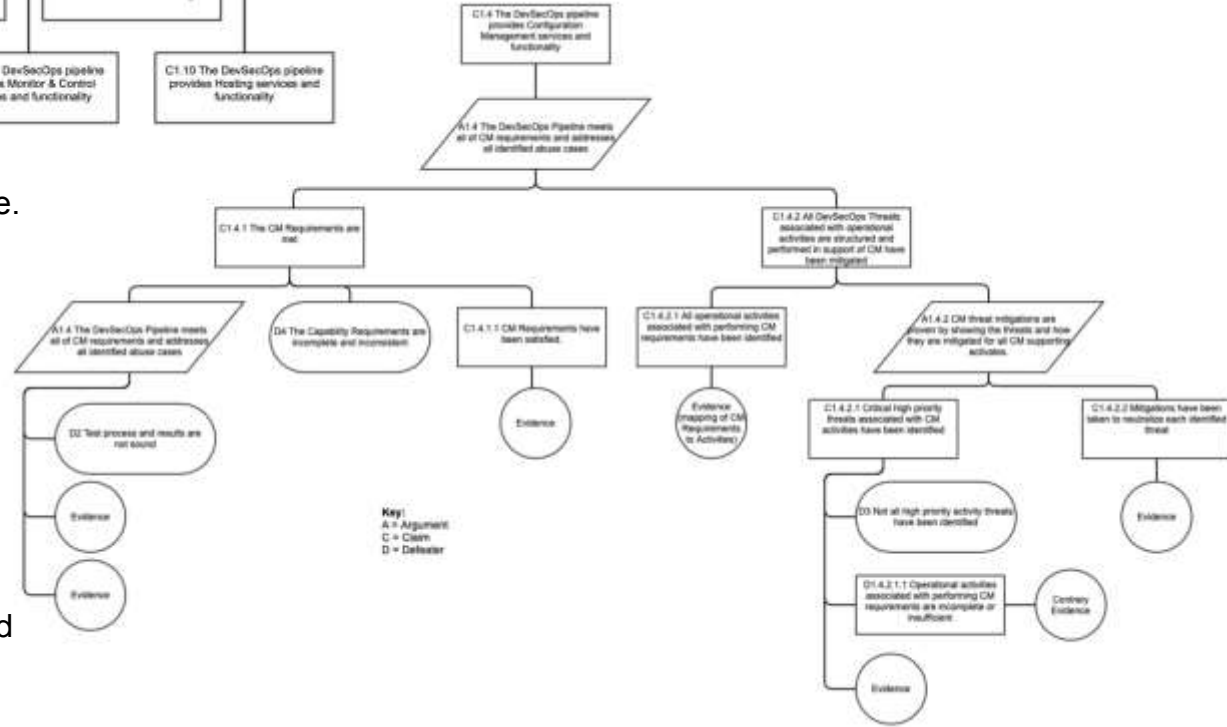
- It is a structured approach used to argue that available evidence supports a given claim
- It provides the organization with the basis for making risk-based choices tied to assuring that the pipeline only functions as intended.
- It provides requirements for automated systems testing, or other evidence collection techniques.
- Actual test results provide the evidence needed to support the assurance claims.

Assuring that your Program only Functions as Intended



Assurance cases are composed of the following elements:

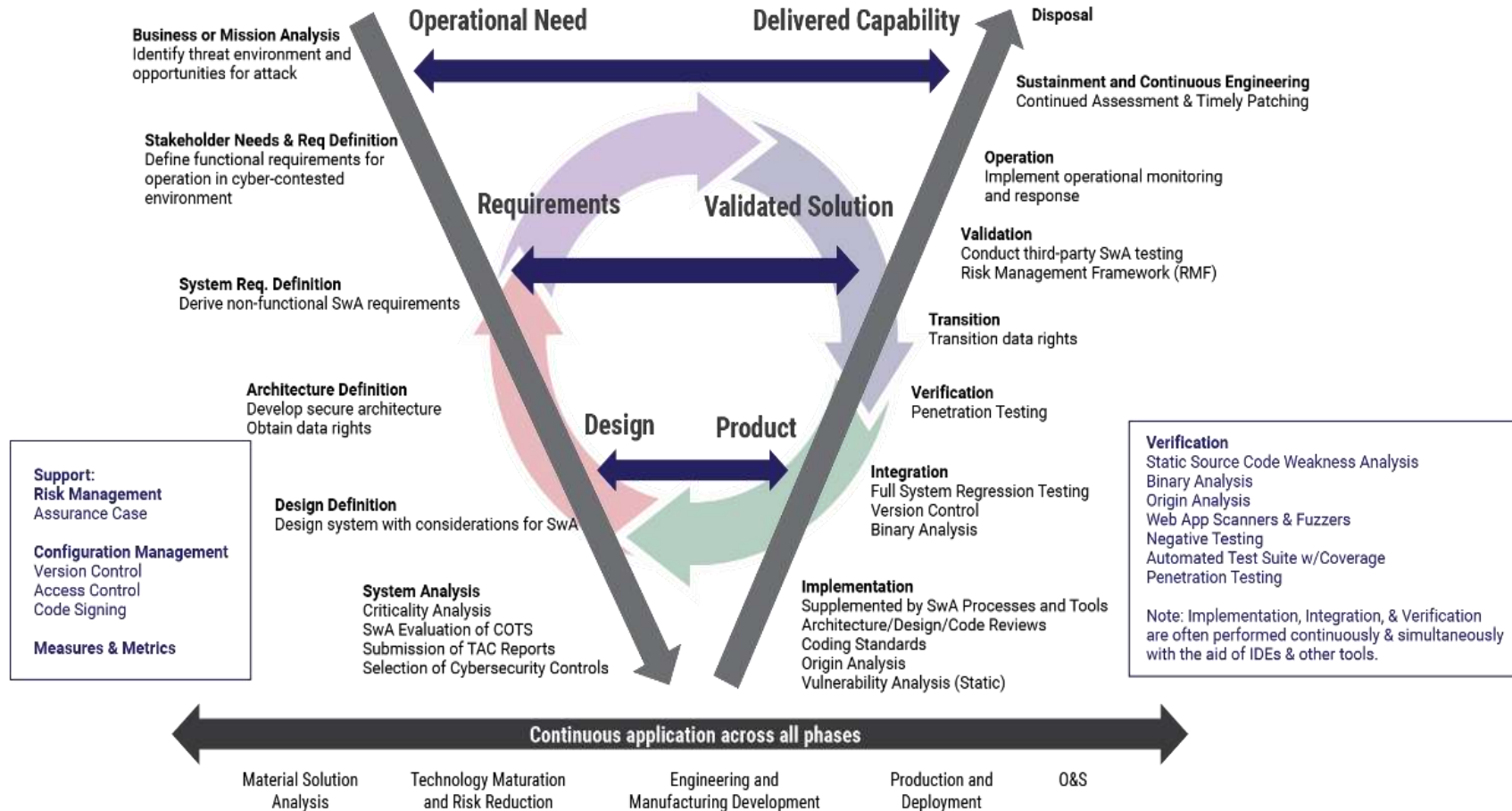
- Claims— “assertions put forward for general acceptance. They are typically statements about a property of the system or some subsystem. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called subclaims [1].”
- Arguments – “link the evidence to the claim [1]” by stating the assumption(s) on which the claim and the evidence are built upon.
- Evidence – “Evidence that is used as the basis of the justification of the claim. Sources of evidence may include the design, the development process, prior field experience, testing, source code analysis or formal analysis [1].”
- Defeaters – “possible reasons for doubting the truth of a claim [2].”



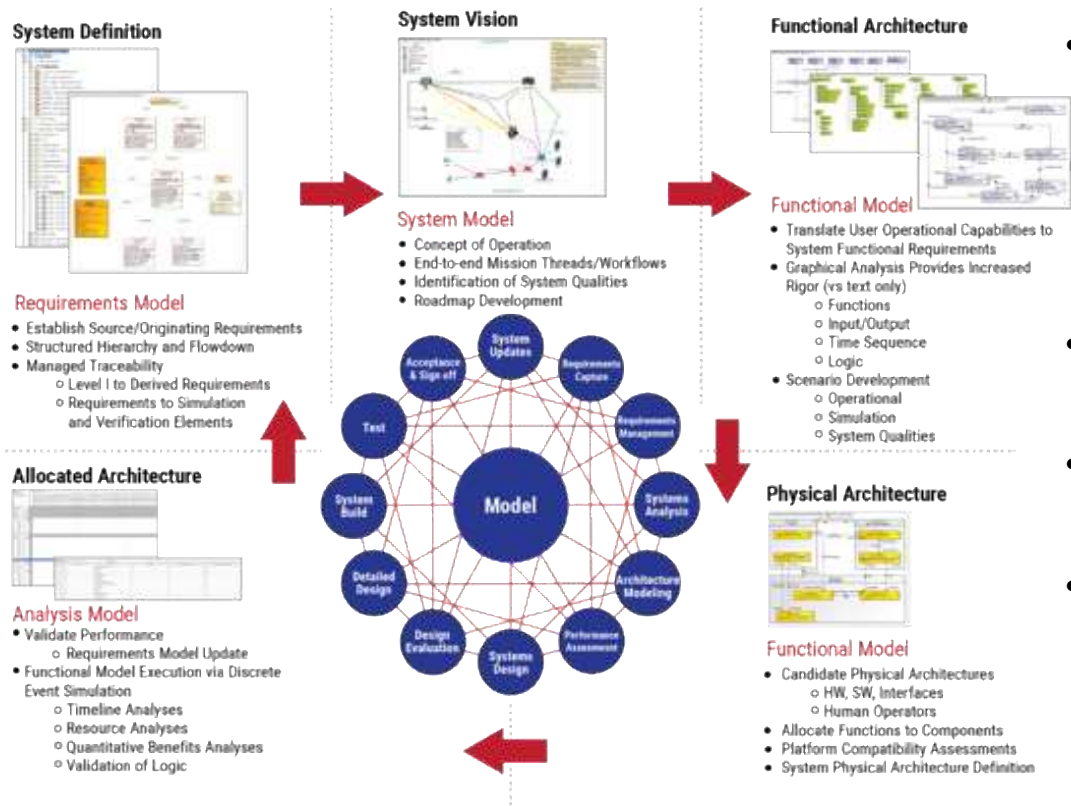
[1] Bloomfield, R. E. and Netkachova, K. Building Blocks for Assurance Cases. Paper presented at the International Symposium on Software Reliability Engineering (ISSRE), 03-11-2014- 06-11-2014, Naples, Italy.
[2] Goodenough, John B., Charles B. Weinstock, Ari Z. Klein. Toward a Theory of Assurance Case Confidence, CMU/SEI-2012-TR-002 September 2012.

Addressing the Cybersecurity Challenge with MBSE

Just like Quality, Security is a lifecycle challenge



Model Based Systems Engineering



- **Not yesterday's Document-Centric Systems Engineering!**
- MBSE uses a Digital System Model* to facilitate common system understanding and decision-making.
- The Digital System Model* is the single authoritative source of truth
- System and Components can be integrated at various levels of abstraction and fidelity
- Model Views are chosen to best communicate information to a variety of stakeholders via the dynamic creation of multiple, consistent, accurate views
- Impacts of changes are more easily analyzed and evaluated

*The Digital System Model contains the most current requirements, key mission/business operations, architecture, design details, implementation details, test and evaluation details, and supporting documentation.

Security Requirements Challenges

Typical problems with security requirements

- Stated as specific security solutions (practices) and not real requirements
 - Ex: Only authorized users shall access personal healthcare information
- Too narrowly focused on security in a particular application
 - Ex: use SSL for Web communication
- Compliance mandates are substituted for security requirements
 - Ex: An audit log must be maintained of every access to the patient's healthcare information
- Focused on selection of controls after designs are complete
- Ignored in requirements elicitation because no stakeholders are knowledgeable enough about security impacts to state their security requirements

Merely Specifying Security Features is Insufficient

One needs to

- anticipate ways in which a system can be misused by adversaries
- perform systematic, rigorous, and customized threat analysis
- associate attack methods with the likely identified threats
- define and document mitigation strategies aimed at thwarting the attacks
- Write appropriately specific security requirements

“Early specification of security requirements positively impacts fundamental architectural decisions that enable security concerns to be addressed from the ground up, rather than added as late-in-the-day patches in an attempt to remediate security vulnerabilities.”

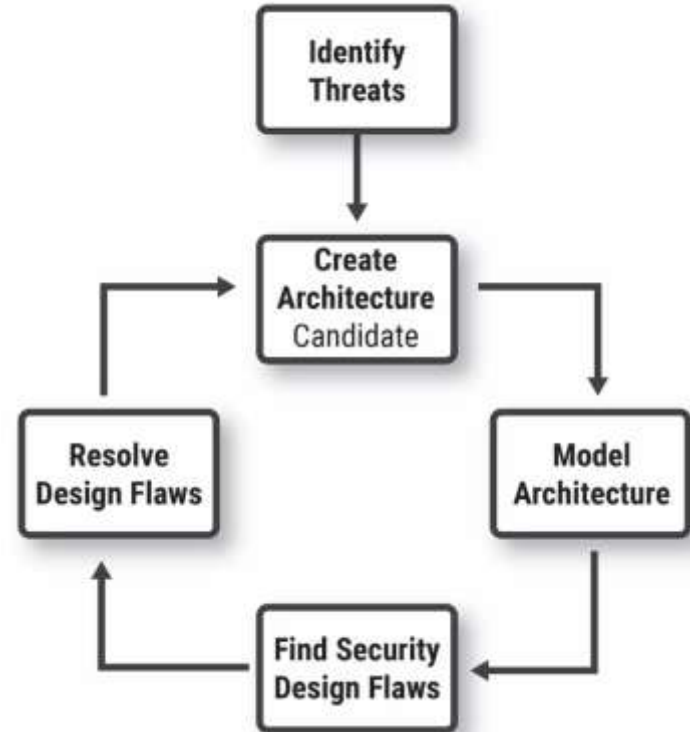
https://resources.sei.cmu.edu/asset_files/TechnicalNote/2018_004_001_516627.pdf

Value of Modeling Security

Crucial security decisions to address risks are made in the architecture.

Analyzing an architecture is a huge opportunity for improving security.

Threat Modeling methods can be combined with MBSE to create a more robust and well-rounded view of potential threats.

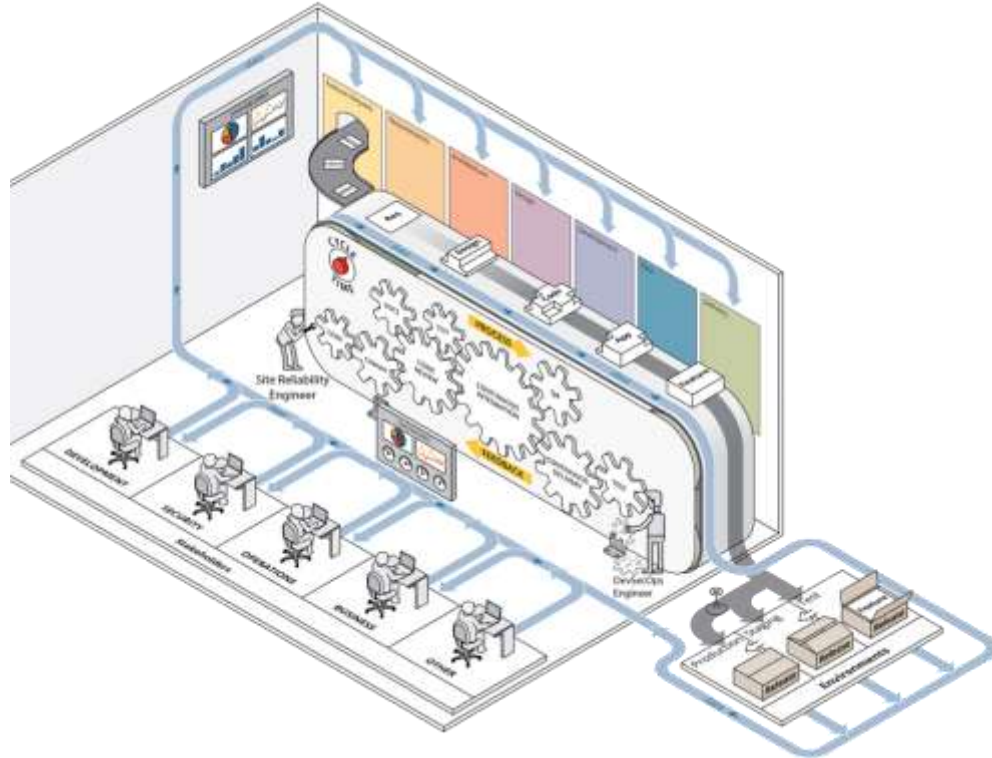


Threat Modeling

- **Threat Modeling** is the process of creating an abstraction of a system, aimed at identifying attackers' abilities and goals, and using that abstraction to generate and catalog possible threats that the system must mitigate.
- While security can be analyzed at the networking and code levels to prevent buffer overflows, SQL injection attacks, etc. there is value in **creating a mindset of defensive thinking** early in the requirements and architecture phases.
- **Defensive thinking** means that for every new feature, one must think about how it could be abused or defeated by adversaries.
- The defensive thinking mindset **underlies the approach to threat modeling**

<https://insights.sei.cmu.edu/blog/the-hybrid-threat-modeling-method/>

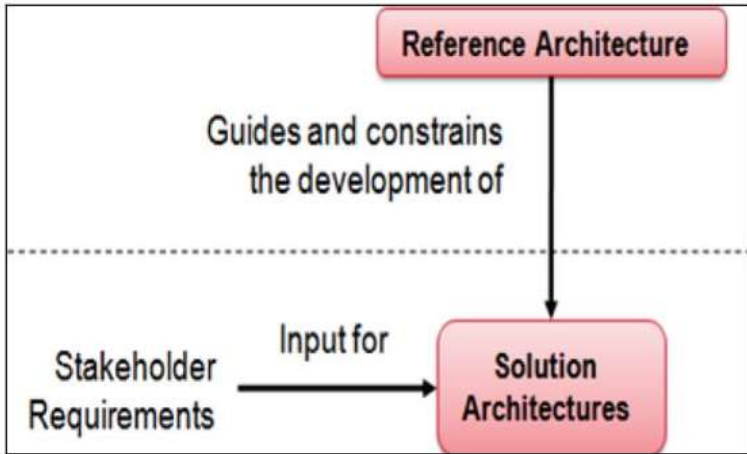
DevSecOps Platform Independent Model (PIM)



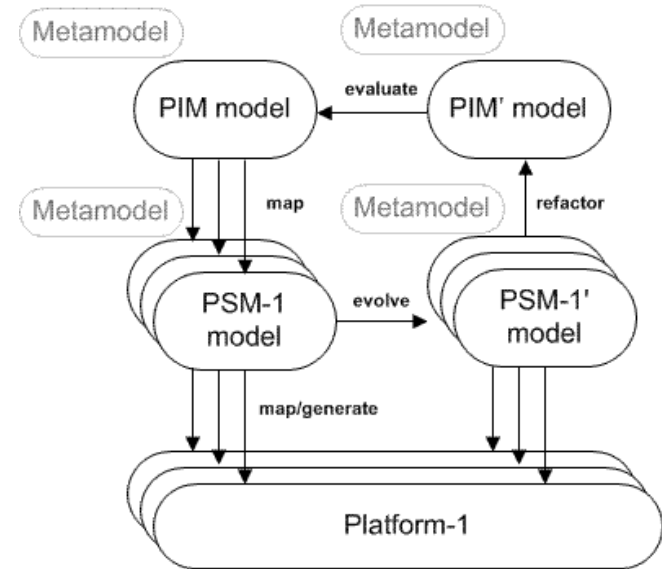
- is an authoritative reference to fully design and execute an integrated Agile and DevSecOps strategy in which all stakeholder needs are addressed
- enables organizations to implement DevSecOps in a secure, safe, and sustainable way in order to fully reap the benefits of flexibility and speed available 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

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 [1].



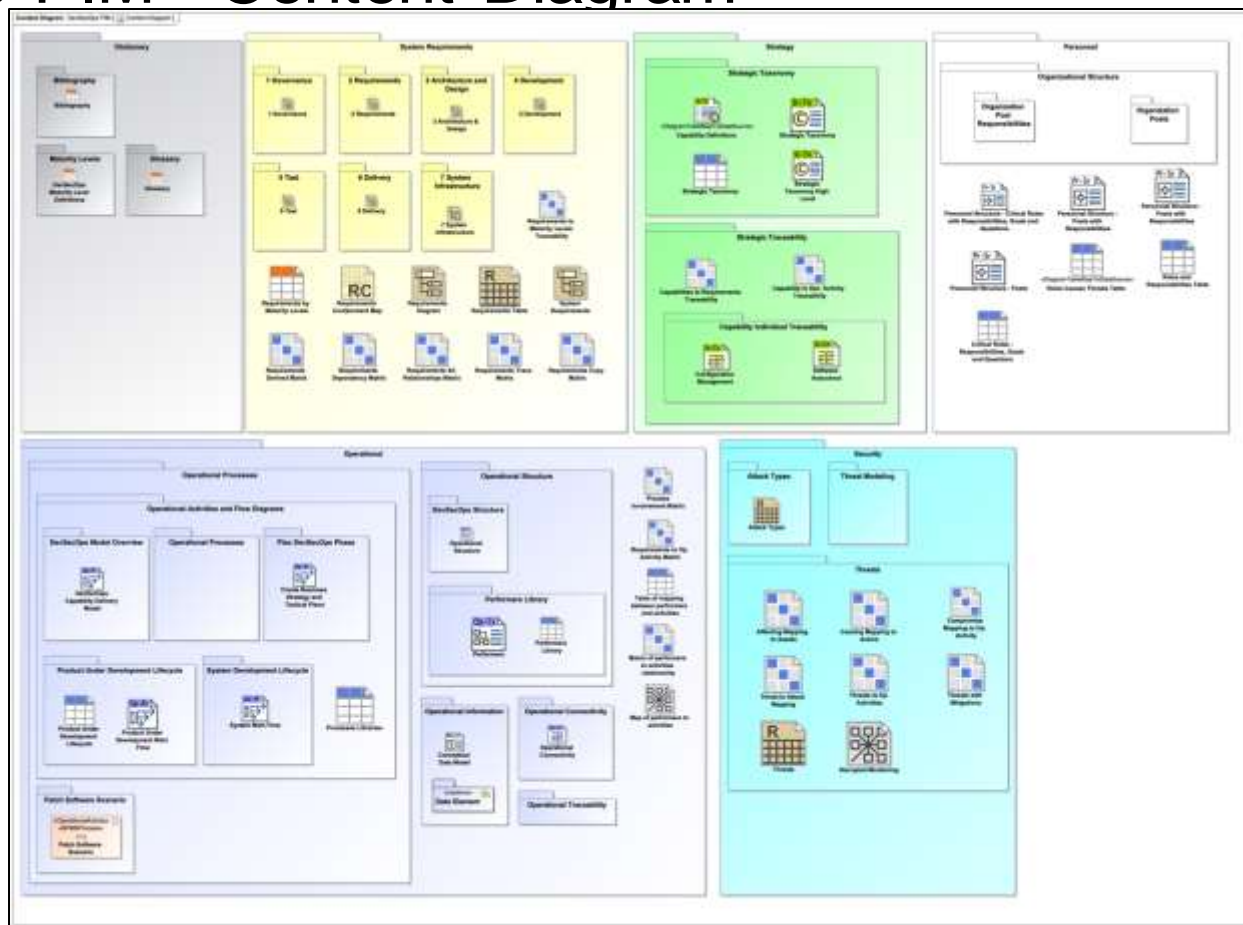
A PIM is a general and reusable model of a solution to a commonly occurring problem in software engineering within a given context and is independent of the specific technological platform used to implement it.



NOTE: PSM = Platform Specific Model

[1] DoD Reference Architecture Description, https://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf

DevSecOps PIM - Content Diagram

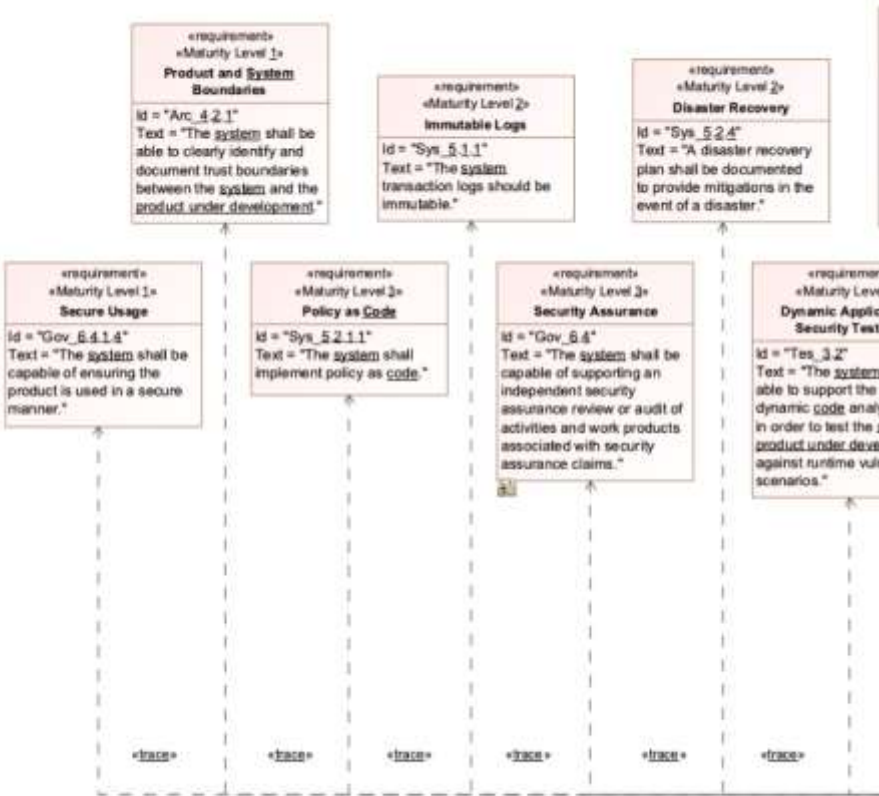


<https://cmu-sei.github.io/DevSecOps-Model/>

DevSecOps Requirements

All requirements are organized into categories based on logical and functional groupings:

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



[Requirements Table Link](#)

Example of Requirements Representation in Diagrams from PIM

DevSecOps Capability/Strategic Viewpoint

A capability is a high-level concept that describes the ability of a system to achieve or perform a task or a mission.

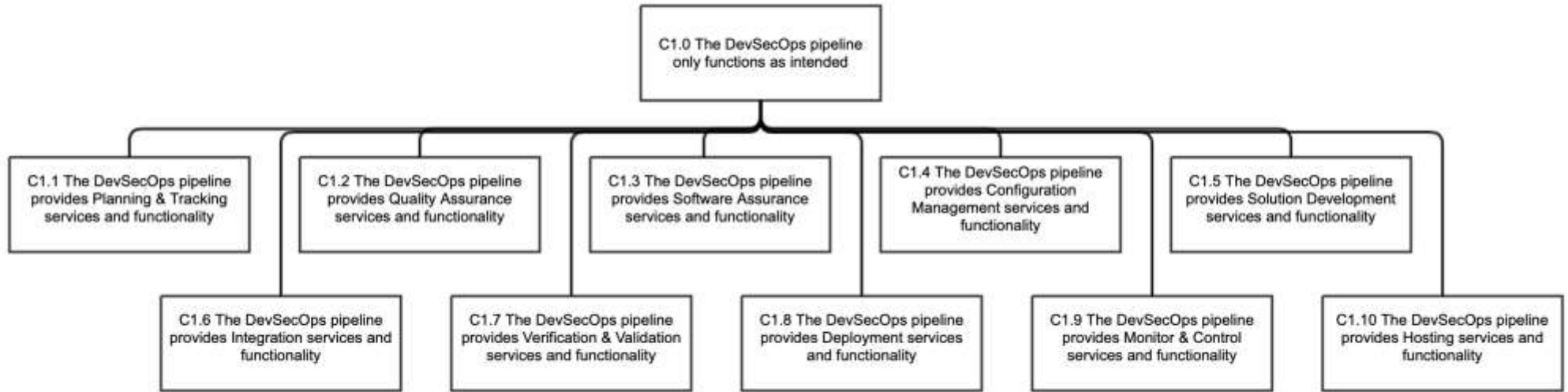
All requirements in the DevSecOps PIM were allocated to corresponding capabilities.

Legend		
	Trace	
	System Requirements	
	DevSecOps Pipeline [Strategic Taxonomy]	
	Configuration Management	28
	Deployment	10
	Hosting Services	37
	Integration	6
	Monitor & Control	50
	Planning & Tracking	34
	Quality Assurance	17
	Software Assurance	65
	Solution Development	41
	Verification & Validation	25

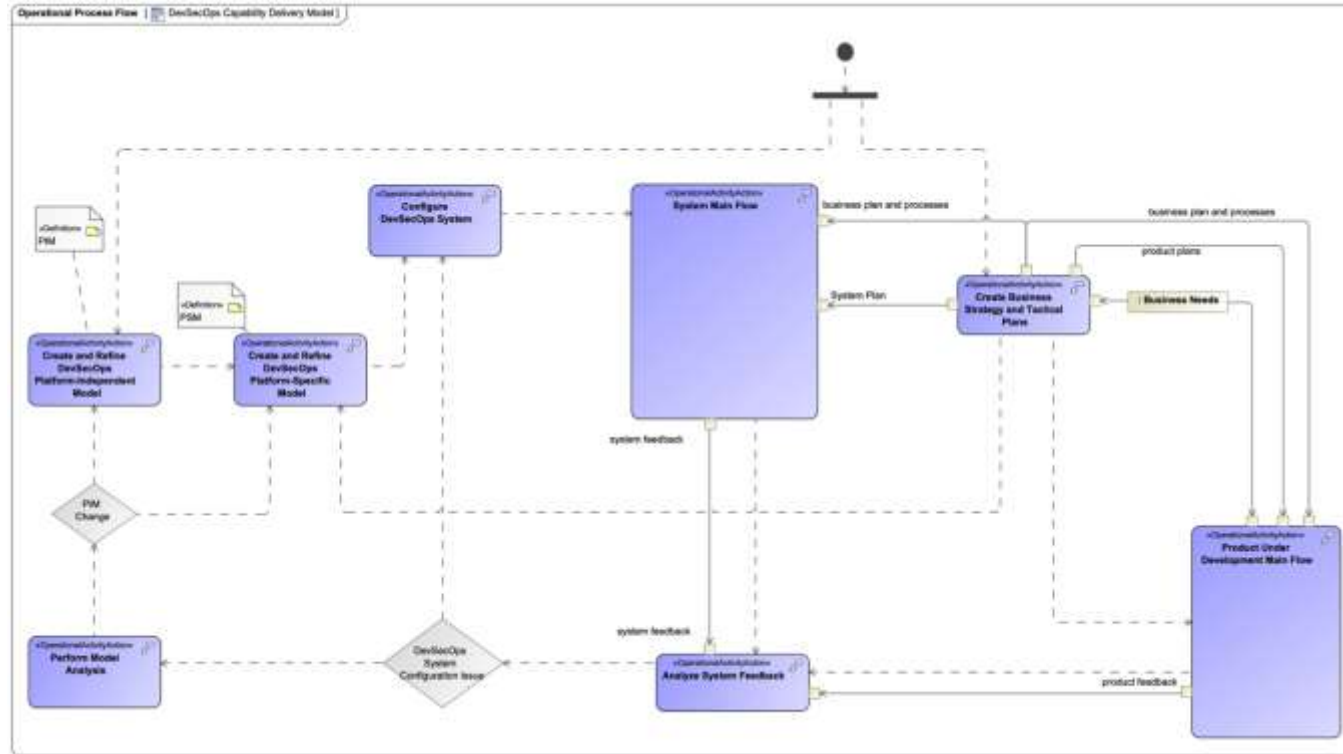
- [Capability to Requirements Traceability Link](#)
- [Capability to Operational Activity Traceability Link](#)
- [Capability Definitions Link](#)
- [Strategic Taxonomy High Level](#)

The screenshot displays a detailed view of the DevSecOps Pipeline. It features a legend on the left with a 'Trace' icon. The main area is a hierarchical tree structure under the heading 'System Requirements'. The tree is organized into several major sections: 1. Governance, 2. Requirements, 4. Development, 5. Test, 6. Delivery, and 7. System Infrastructure. Each section contains numerous sub-items, many of which are expanded to show further detail. The interface uses a consistent color scheme and icons to represent different levels and types of requirements.

Structuring a DevSecOps Assurance Case Around Capability



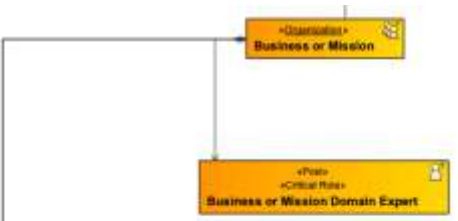
DevSecOps Operational Viewpoints



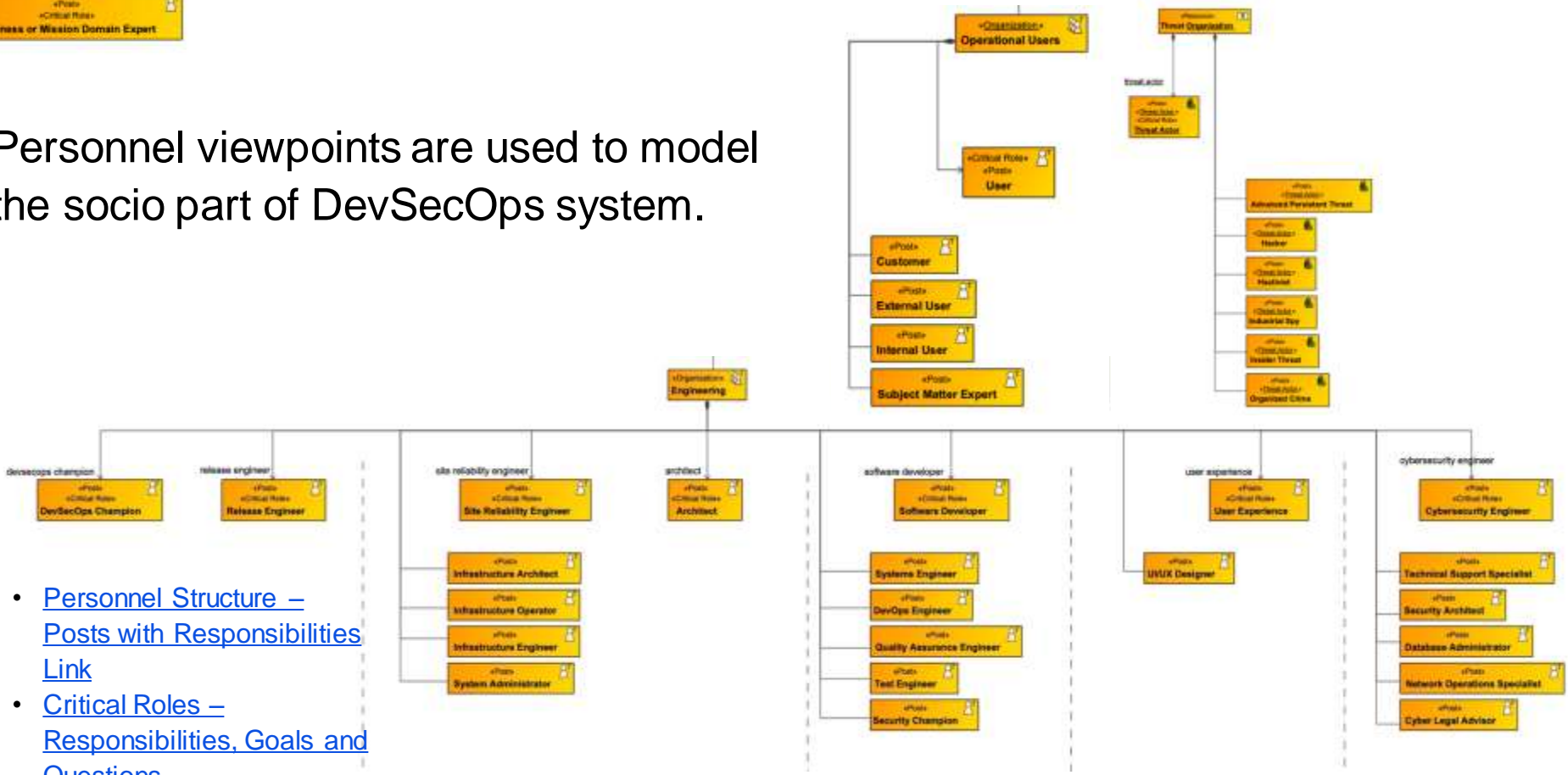
- [DevSecOps Capability Delivery Model Link](#)

An operational model for a system describes behavior of the system to conduct enterprise operations. The main operational processes for DevSecOps includes development process for the product, as well as the DevSecOps process itself.

DevSecOps Personnel Viewpoints



Personnel viewpoints are used to model the socio part of DevSecOps system.



- [Personnel Structure – Posts with Responsibilities Link](#)
- [Critical Roles – Responsibilities, Goals and Questions](#)

Everyone Plays a Role in DevSecOps

Legend		Organization Posts																																															
<ul style="list-style-type: none"> ➤ Approves ➤ Contributes To ➤ Is Capable To Perform ➤ Observes ➤ Multiple (one-way) 		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	Specialist	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	
Operational Activities and Flow Diagrams		93	69	1	3			99	3	58										2					4	14			10	1		10	10							14						29	92		
DevSecOps Model Overview		6	5					5	5																				5		5															2	5		
Plan DevSecOps Phase		17	16					15	15																				15		15	16														7	15		
Product Under Development Lifecycle		70	47	1	3			79	3	38										2						4	14			8	1		8	1												20	72		
P2 Product Under Development Main Flow																																																	
P2-1 Plan Product		40	23		2			40	1	18										2						4	11			4			4	1												14		15	40
P2-2 Develop Product		10	3					10	4																																								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
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, PI		9																																															

• [Process Involvement Matrix Link](#)

Critical Roles are mapped to Operational Activities.

Threat Scenarios

Template:

Part	Description
Activity	The activity diagrammed in the PIM or PSM. There can be more than one activity applied to the Threat Scenario.
Actor	The person, or group, that is behind the threat scenario. Threat actors can be malicious or unintentional. Developing a standard set of actors is beneficial for this step. Persona non grata could be useful in determining malicious actors. Threat actor may be a person, or group, internal to an organization structure.
Action	A potential occurrence of an event that might damage an asset, a mission, or goal of a strategic vision.
Attack	An action taken that utilizes one of more vulnerabilities to realize a threat to compromise or damage an asset, a mission, or goal of a strategic vision.
Asset	A resource, person, or process that has value.
Effect	The desired or undesired consequence resulting from the attack.
Objective	The threat actor's motivation or objective for conducting the attack
Statement	Structured prose summarizing the 6-part security scenario

Example:

Part	Description
Activity	Develop Product, Static and Dynamic Analysis
Actor	Insider Threat
Action	Results from analysis are disclosed for effect
Attack	Information Disclosure
Asset	Analysis Results
Effect	Damage organization, vulnerabilities are publicly enumerated for a product under development
Objective	Develop a targeted exploit for the product under development, financial attack
Statement	An insider threat publicly releases the results of static and dynamic analysis to the public to damage the organization's reputation.

Threat Scenario Generation Workshop

Purpose	Identify threat scenarios for a given system	
Entry Criteria:	The following Unified Architecture Framework (UAF) defined views have been created for the system under evaluation: <ul style="list-style-type: none"> • Requirements Diagrams • Operational Process Flows • Relationships between Operational Activities and System Requirements • Operational resource structure, Posts (<u>i.e.</u> roles) and corresponding responsibilities including the Involvement relationships. 	
General	<ul style="list-style-type: none"> • As the system architecture and associated system instantiation evolves, so will the threats and corresponding mitigations. While this process defines an approach to systematically define applicable threat scenarios for the given system, threats should be identified, evaluated, and captured continuously outside this process. • During the structured and unstructured brainstorming activities, there are no right or wrong ideas. The goal is to identify any reasonable action that can be taken to exploit the various activities within the system to ultimately impact the final product. The ideas will be evaluated later in the process. 	
Step	Activities	Description
1	Planning	<ul style="list-style-type: none"> • Identify relevant stakeholders. Participants must contain a mix of engineering, operational, user, business, and cyber security experience. • Schedule a date and time, or series of events, in which all relevant stakeholders can actively participate.
2	Kick-off Event	<ul style="list-style-type: none"> • Review the workshop process and introduce participants • Discuss the goals and objectives of the workshop • Introduce participants to the concept of system threats and review a few example threat scenarios that follow the format of the Threat Scenario Template.
3	System and Architectural Overview	<ul style="list-style-type: none"> • Outline system purpose and constraints • Review system's architectural views and relationships <ul style="list-style-type: none"> ○ Requirements ○ Strategy ○ Personnel ○ Operational
4	Operational Process Flow Focus Area	<ul style="list-style-type: none"> • Select an operational process flow to focus the threat scenario generation • Review the selected operational process flow to gain understanding of the process, data flow between operational activities, and performers involved. This may include reviewing associated requirements to understand the scope and context of the various operational activities.
5	Unstructured Brainstorming	<ul style="list-style-type: none"> • Select an operational activity within the operational process flow • Either working individually or in pairs, brainstorm threats for the selected operational activity and write them down. Threats can bridge multiple operational activities. The brainstormed ideas should be captured in the individual's natural language. • Using an affinity diagram, organize the threats identified by the whole group and remove duplicates. • Create a list of potential threats to the system.
6	Structured Brainstorming	<ul style="list-style-type: none"> • Use the same operational activity as in step 5. • Break into groups of 2-3 people.

		<ul style="list-style-type: none"> • In small groups, identify ways that the operational activity may be exploited to interrupt the confidentiality, integrity, and/or availability of the system. Utilize the Process Specific STRIDES Threat Modeling Taxonomy to reduce individual bias and to holistically identify threats to the given activity. • Using an affinity diagram, organize the threats identified by the whole group and remove duplicates. • Add new threats to the list of potential threats to the system created in step 5.
7	Define Threat Scenarios	<ul style="list-style-type: none"> • If this is the first time any of the participants have written threat scenarios, select a threat from the list and complete the Threat Scenario Template as a group. Repeat until everyone understands how to complete the Threat Scenario Template. • Break into small groups of 3-4 people. • Divide the list of potential threats to the system between the small groups. Alternatively, create a pull system in which the small groups claim a potential threat from a centralized list as needed. • In small groups, complete the Threat Scenario Template for each assigned, or pulled, potential threat. • Review and update all completed threat scenarios as a whole group, removing or consolidating duplicates.
8	Operational Activity Threat Identification	<ul style="list-style-type: none"> • Select next operational activity within the selected operational process flow. • Repeat steps 5-7. • Repeat step 8 until threats have been identified for all operational activities within the selected operational process flow.
9	Identify Operational Process Flow Threats	<ul style="list-style-type: none"> • Repeat steps 4-8 until threats have been identified for all operational process flows for the given system.
10	Consolidate and Review	<ul style="list-style-type: none"> • Consolidate all threat scenarios into a central list. • Review and accept the threat scenarios
Exit Criteria		A list of structured threat scenarios that cover the operational activities in the given system.

The Makeup of Your Threat Modeling Team Matters

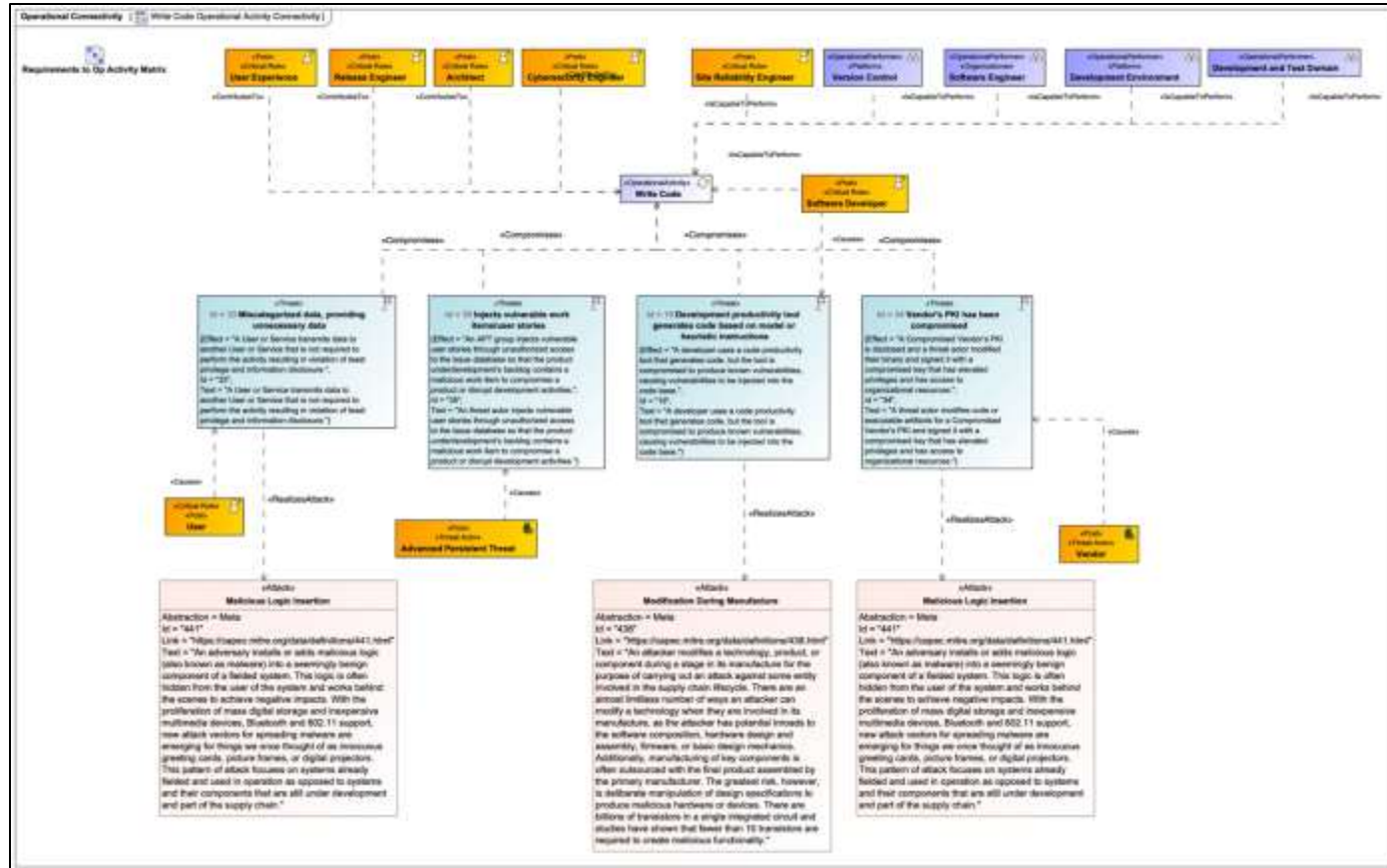
Research shows that consistency associated with threats reported using STRIDE is based on the makeup of specific teams and their background or experience.

Thus, teams should include representative of at least the following groups:

- **System users/purchasers:** includes those acquiring the system, end users, maintainers, and other groups with a vested interest in the system
- **Cybersecurity Experts:** could include roles such as system administrators, penetration testers, ethical hackers, threat modelers, security analysts, etc.
- **System Engineers/Developers:** covering a range of perspectives such as, systems engineers, requirements analysts, architects, developers, testers, release engineers, site reliability engineers, etc.

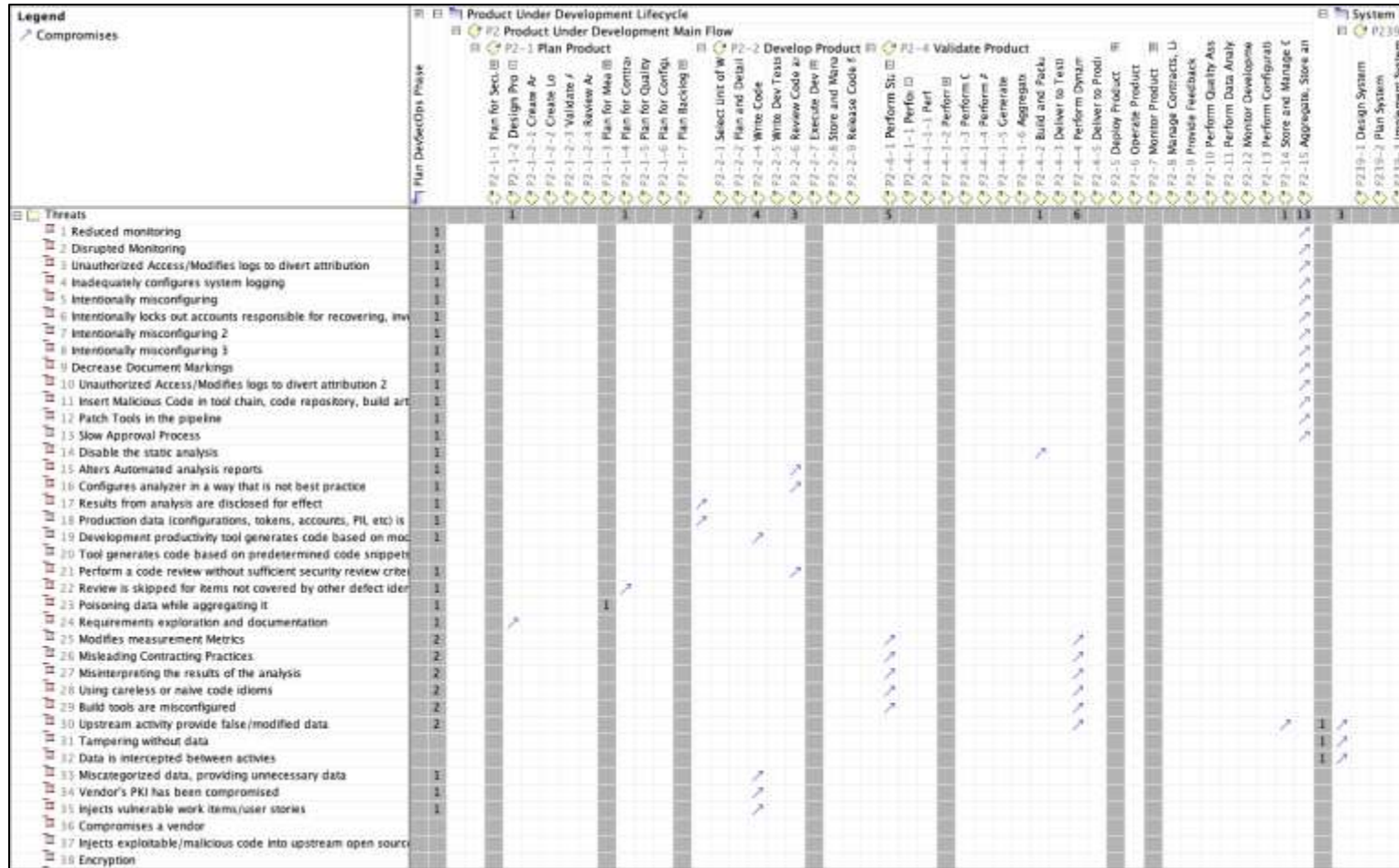
<https://insights.sei.cmu.edu/blog/the-hybrid-threat-modeling-method/>

Example Threat Modeling Diagram for Write Code Operational Activity



[Write Code](#)
[Operational Activity](#)
[Connectivity Link](#)

DevSecOps Threat to Operational Activity Matrix



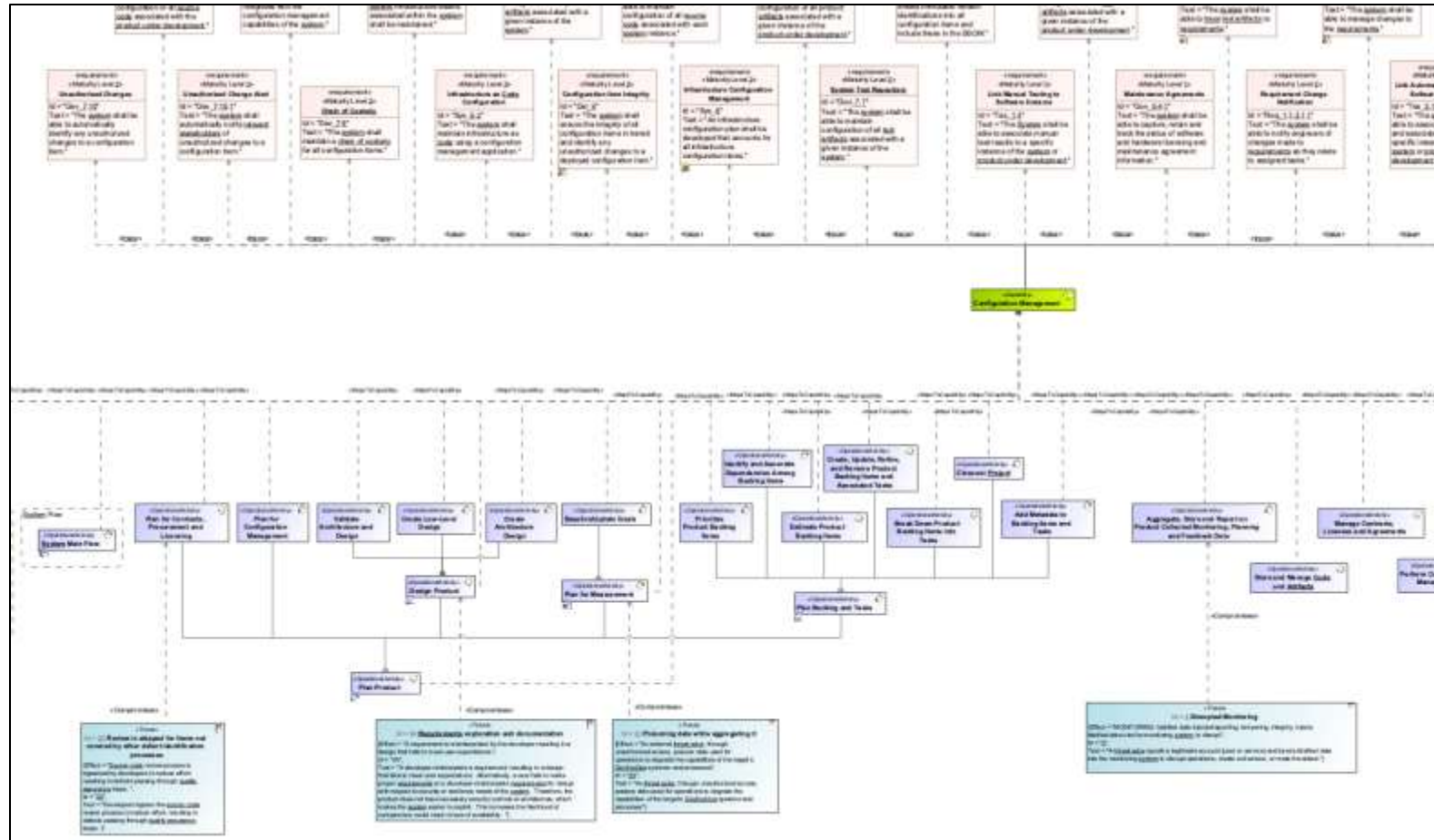
[Threats to Operational Activities Link](#)

DevSecOps Threats with Attributes

ID	Name	Text	Effect	Compromises	Realized By Attack	Caused By	Mitigated By	Document
1	Reduced monitoring	A threat actor is made aware of a monitoring system's reduced capacity resulting in regular service outages leaving an open window of opportunity for an unobservable attack.	Reduced or misconfigured monitoring allows for nefarious activity to occur	P2-15 Aggregate, Store and Report on Product Collected Monitoring, Planning and Feedback Data	607 Obstruction	Insider Threat		Much of this was pulled from CAPEC info https://capec.mitre.org/data/definitions/1000/
2	Disrupted Monitoring	A threat actor spoofs a legitimate account (user or service) and injects falsified data into the monitoring system to disrupt operations, create a diversion, or mask the attack.	MONITORING: falsified data injected/spoofing, tampering, integrity, injects falsified data into the monitoring system to disrupt	P2-15 Aggregate, Store and Report on Product Collected Monitoring, Planning and Feedback Data	151 Infrastructure Manipulation	Advanced Persistent Threat Insider Threat Architect Cybersecurity Engineer	SC1 Mitigation Strategy 1	Keep at the Meta Level and better explained in the 'star
3	Unauthorized Access/Modifies logs to divert attribution	A threat actor gains unauthorized access to logging data, alters system logs to conceal illicit activity from forensic audits, automated responses and alerts, or to divert attribution.	Logs: insider threat modifies the logs to conceal activity	P2-15 Aggregate, Store and Report on Product Collected Monitoring, Planning and Feedback Data	163 Infrastructure Manipulation	Insider Threat Site Reliability Engineer Cybersecurity Engineer		
4	Inadequately configures system logging	A threat actor has configured the collection of system logs in a way that limits the effectiveness of forensic audit activities.	Accidentally misconfiguring Logging - can't perform forensics work against what is captured	P2-15 Aggregate, Store and Report on Product Collected Monitoring, Planning and Feedback Data	176 Configuration/Environment Manipulation	Software Developer		Could be 1617 Most significant improper configuration
5	Intentionally misconfiguring	A threat actor has configured the collection of system logs in a way that limits the effectiveness of forensic audit activities in order to conceal subsequent activities.	Intentionally misconfiguring the system	P2-15 Aggregate, Store and Report on Product Collected Monitoring, Planning and Feedback Data	176 Configuration/Environment Manipulation	Insider Threat		
6	Intentionally locks out accounts responsible for recovering, investigating, or repairing the system	A threat actor spoofs an individual's account in order to create user action logs with the objective of making a targeted user in violation of security policy and reducing the targeted individual's organizational effectiveness.	Targeting individual with the intent that their login is denied, locking out individuals who should have access	P2-15 Aggregate, Store and Report on Product Collected Monitoring, Planning and Feedback Data	212 Functionality Misuse	Insider Threat		Could be a CAPEC - 184 So Attack
		Unit testing is insufficient to cover the requirements and abuse cases. A software or site reliability engineer doesn't		P2-15 Aggregate, Store and Report on Product Collected	176 Configuration/Environment	Software Developer		

[Threats Link](#)

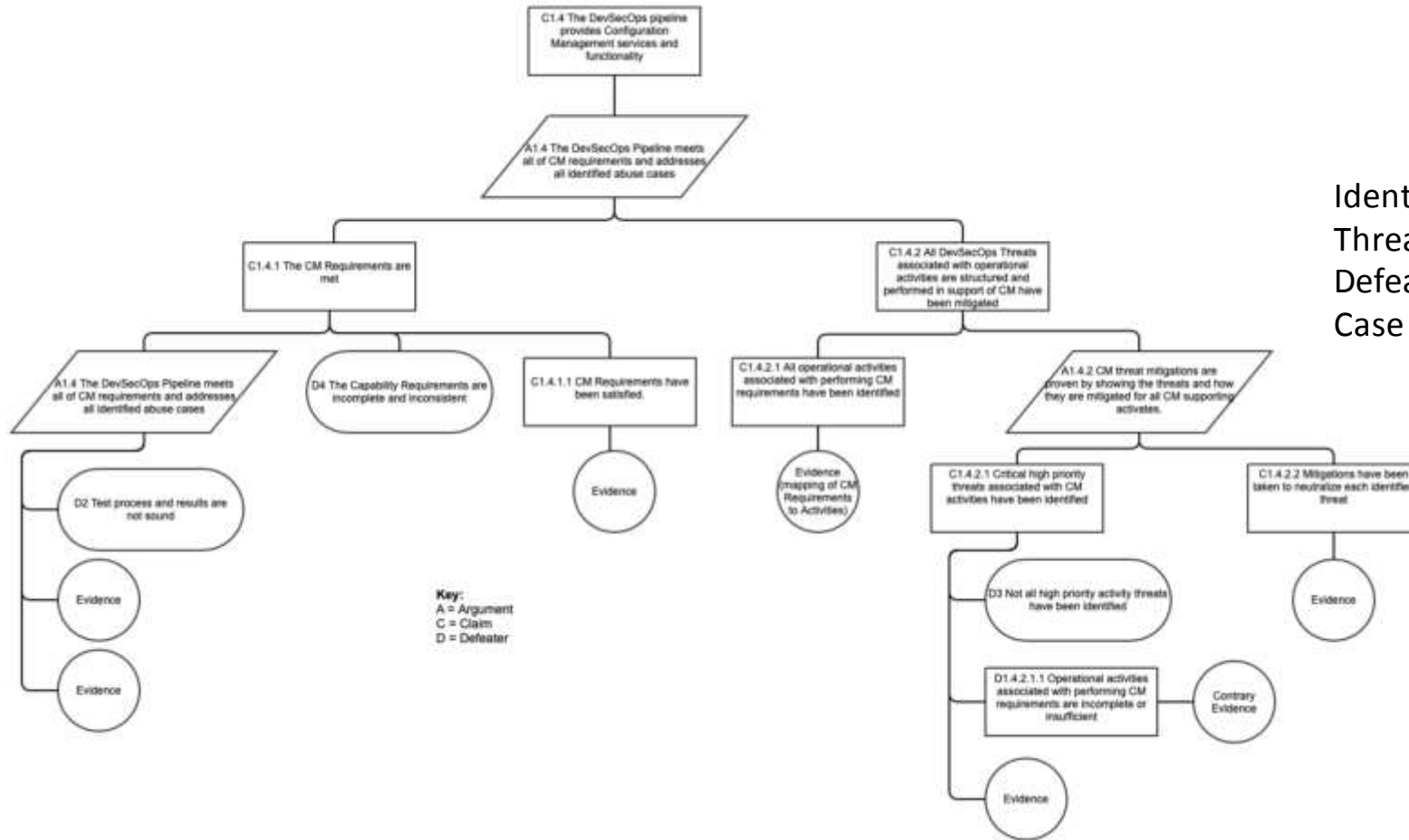
Capturing the Complexity of the DevSecOps System



Example of Threats Traced to Capabilities via Operational Activities

[Configuration Management Complexity Link](#)

Addressing Assurance Case Defeaters



Identifying and Mitigating Threats helps to address Defeaters in your Assurance Case

The DevSecOps PIM enables Organizations, Projects, Teams, and Acquirers to

- specify the DevSecOps requirements to the lead system integrators tasked with developing a platform-specific solution that includes the designed system and continuous integration/continuous deployment (CI/CD) pipeline
- assess and analyze alternative pipeline functionality and feature changes as the system evolves
- apply DevSecOps methods to complex products that do not follow well-established software architectural patterns used in industry
- provide a basis for threat and attack surface analysis to build a cyber assurance case to demonstrate that the product and DevSecOps pipeline are sufficiently free from vulnerabilities and that they function only as intended

Summary



The use of model based systems engineering in the design, implementation, and sustainment of your DevSecOps socio-technical system will assist you in building a system that is:

- Trustworthy – No exploitable vulnerabilities exist, either maliciously or unintentionally inserted.
- Predictable – When executed, software functions as intended and only as intended.
- Timely – Features are delivered as the speed of relevance.

Contact Information



Timothy A. Chick

CERT Applied Systems Group Technical Manager, CMU-Software Engineering Institute
Adjunct Faculty Member, CMU-Software and Societal Systems Department

tchick@sei.cmu.edu

<https://www.sei.cmu.edu>

<https://s3d.cmu.edu>