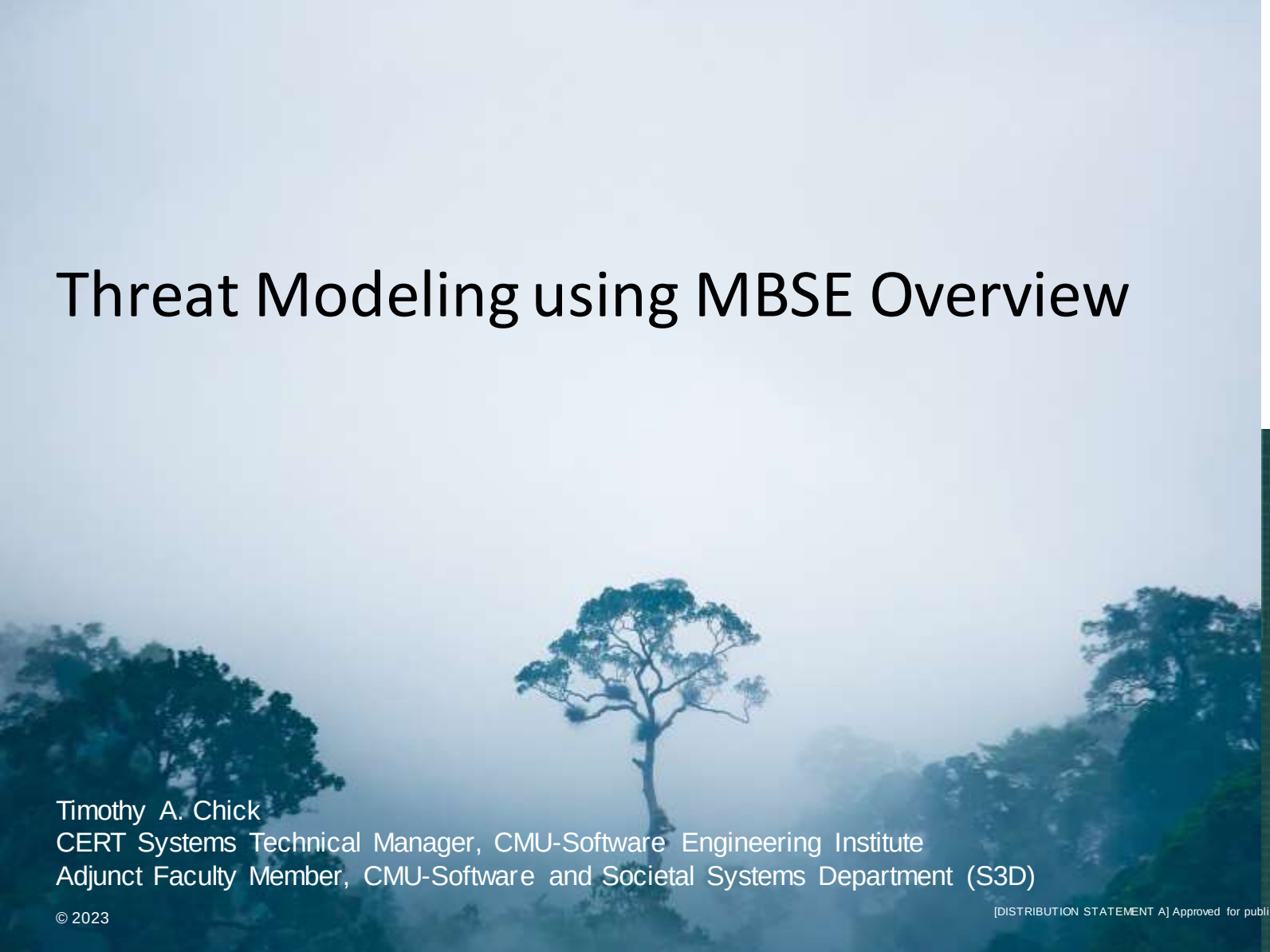
Threat Modeling using MBSE Overview



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

Carnegie Mellon University
Software Engineering Institute

Document Markings

Threat Modeling using Model-Based Engineering (MBSE)

Carnegie Mellon University Software Engineering Institute

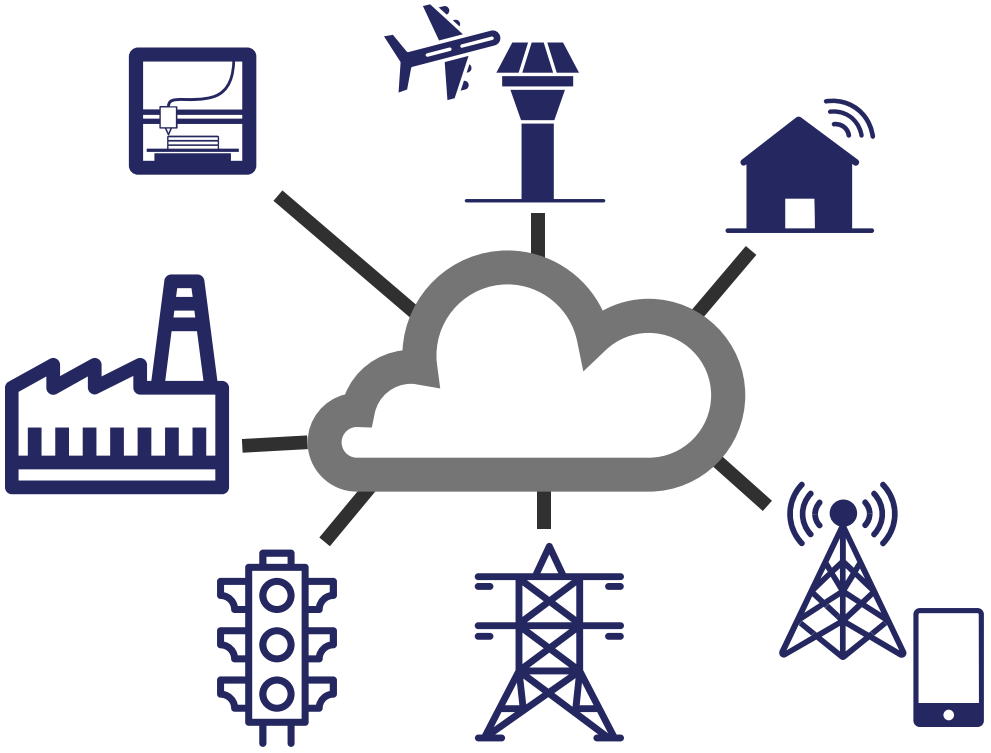
Full Course Abstract: Threat modeling helps to identify the mission-critical security requirements of a system or process in order to protect the system. The goal of this training is to inform the participants of threat modeling concepts and to work through example threat modelling scenarios. The training will use the SEI Program Independent Model (PIM) to describe assurance cases and workflows for use in threat modelling tasks.

The training will include:

- Review assurance case concepts and terminology
- Introduce threat modeling concepts and terminology
- Work through generic threat model example (threats as defeaters)
- Brainstorming session to determine potential threats
- Select threats to focus on (likelihood and impact) supported by data
- Work through modeling a selection of identified threats

Subsequently, the SEI can facilitate Threat Modeling Workshops to identify program specific threats. Followed by incorporating the identified treats and corresponding mitigations into there system models.

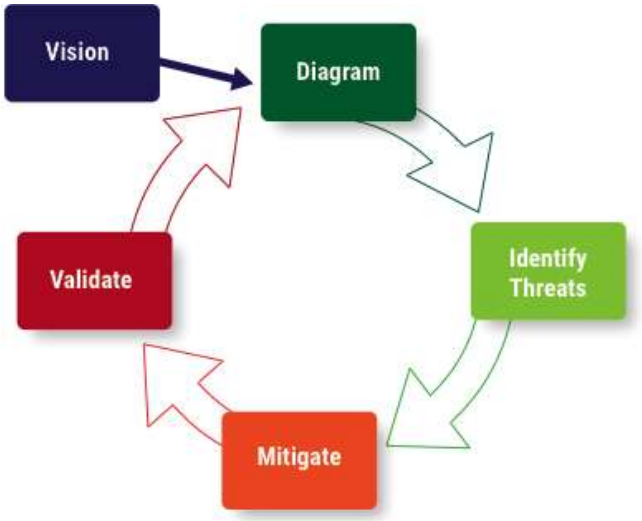
Software is the new hardware – cyber physical



- Cellular
  - Main processor
  - Graphics processor
  - Base band processor (SDR)
  - Secure element (SIM)
- Automotive
  - Autonomous vehicles
  - Vehicle to infrastructure (V2I)
  - Vehicle to vehicle (V2V)
- Industrial and home automation
  - 3D printing (additive manufacturing)
  - Autonomous robots
  - Interconnected SCADA
- Aviation
  - Next Gen air traffic control
- Smart grid
  - Smart electric meters
  - Smart metering infrastructure
- Embedded medical devices

Software vulnerabilities are ubiquitous

Threat analysis tools help derive abuse and misuse cases



STRIDE Threat Types

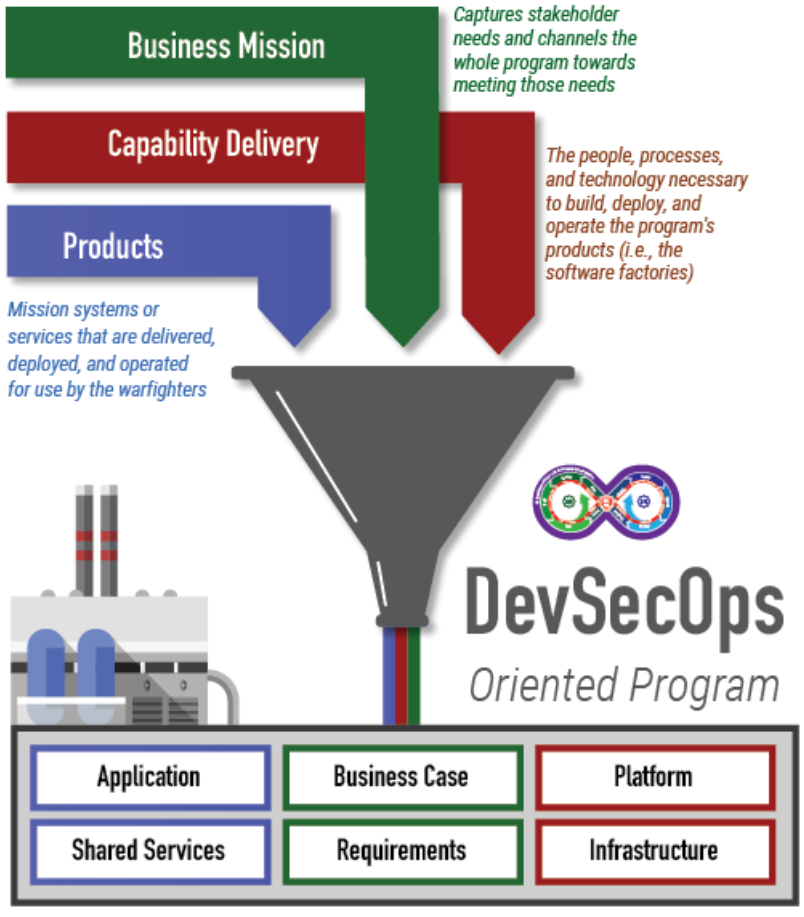
Desired Property	Threat	Definition
Authentication	Spoofing	Impersonating something or someone else
Integrity	Tampering	Modifying code or data without authorization
Non-repudiation	Repudiation	The ability to claim to have not performed some action against an application
Confidentiality	Information Disclosure	The exposure of information to unauthorized users
Availability	Denial of Service	The ability to deny or degrade a service to legitimate users
Authorization	Elevation of Privilege	The ability of a user to elevate their privileges with an application without authorization

Microsoft STRIDE Threat Types

Denning, Friedman, Kohno
The Security Cards: Security Threat Brainstorming Toolkit

Jane Cleland-Huang's Persona non Grata
http://www.infoq.com/articles/personae-non-gratae

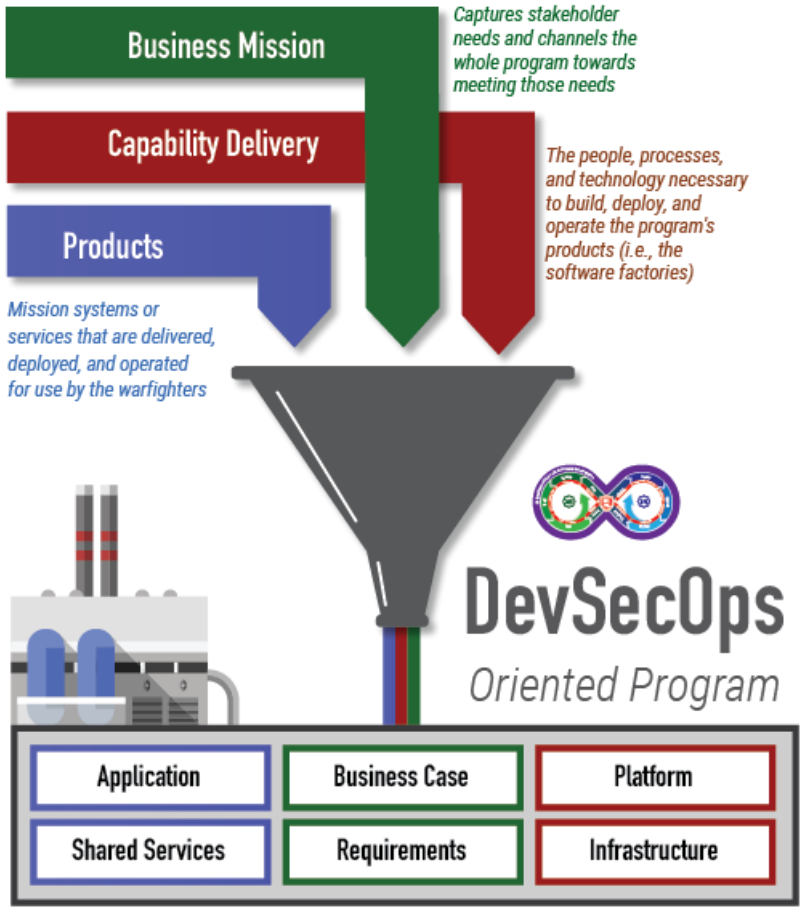
A Program View



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.

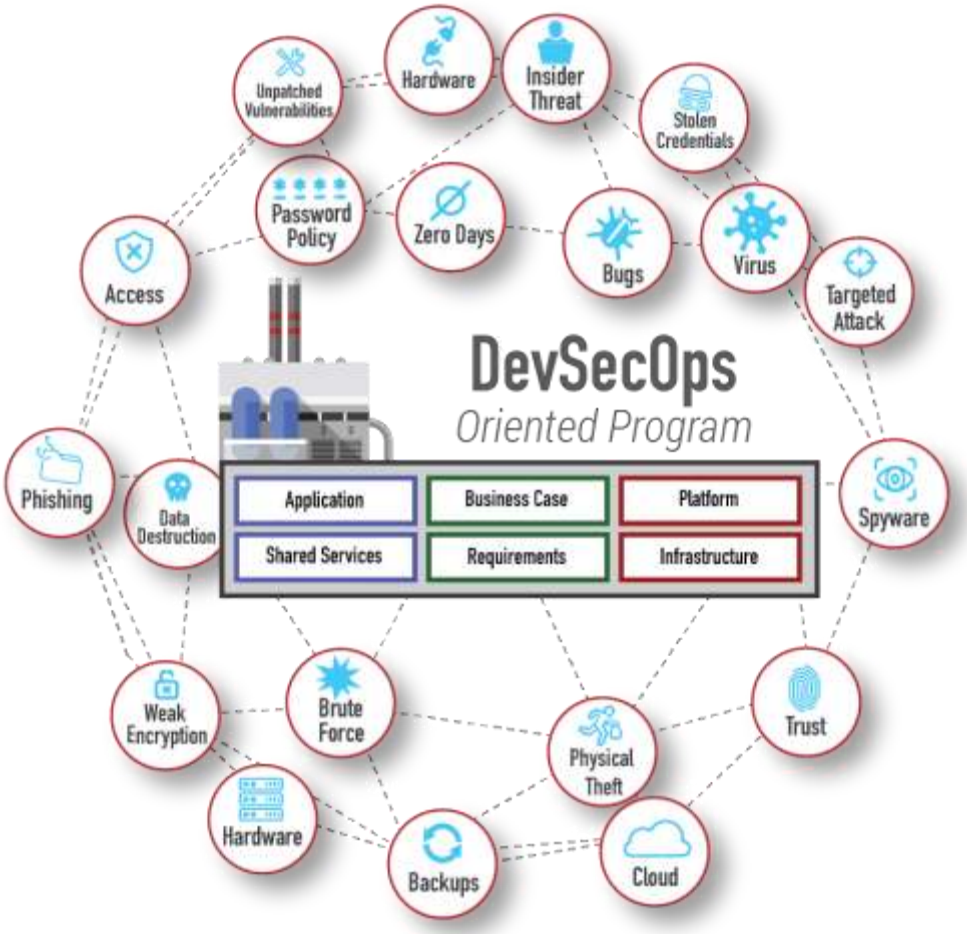
Challenge 1: connecting process, practice, and tools



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?

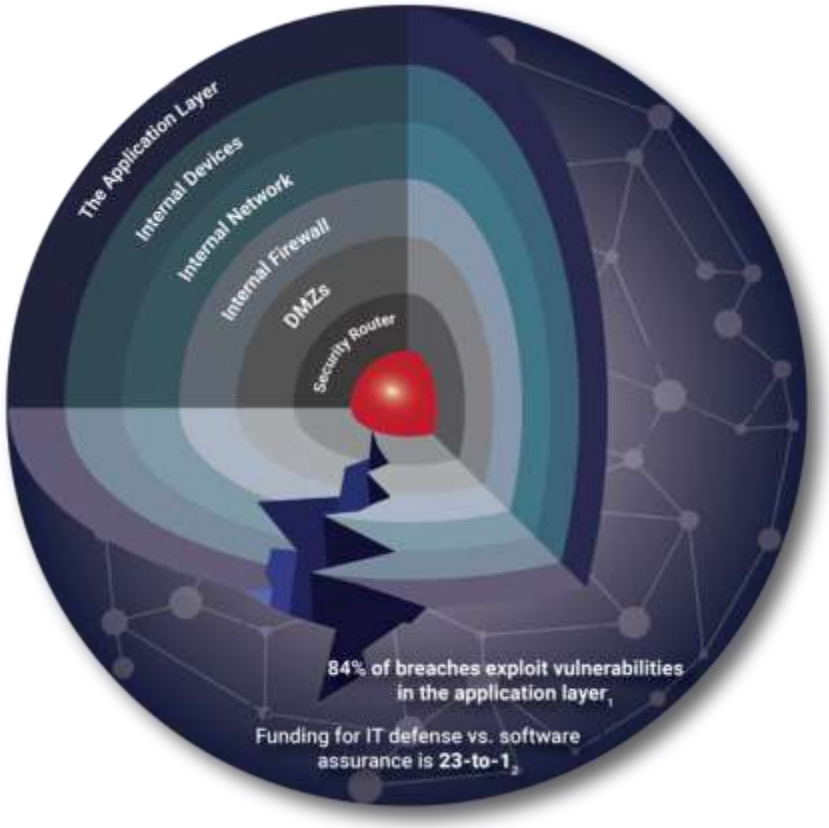
Using a capability service to attack a product isn't new

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."

One Opening is all an Adversary Needs



The Application Layer is the new perimeter exploited by 84% of breaches

Security must be Engineered into the Lifecycle of Applications changing the way we build and buy technology

1. Clark, Tim, *Most cyber Attacks Occur from this Common Vulnerability*, Forbes. 03-10-2015
2. Feiman, Joseph, *Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves,* Gartner. 09-25-2014. G00269825

Software Assurance (SwA)

Carnegie Mellon University Software Engineering Institute

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]

Mitigating Risk with Assurance Cases

Carnegie Mellon University Software Engineering Institute

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.

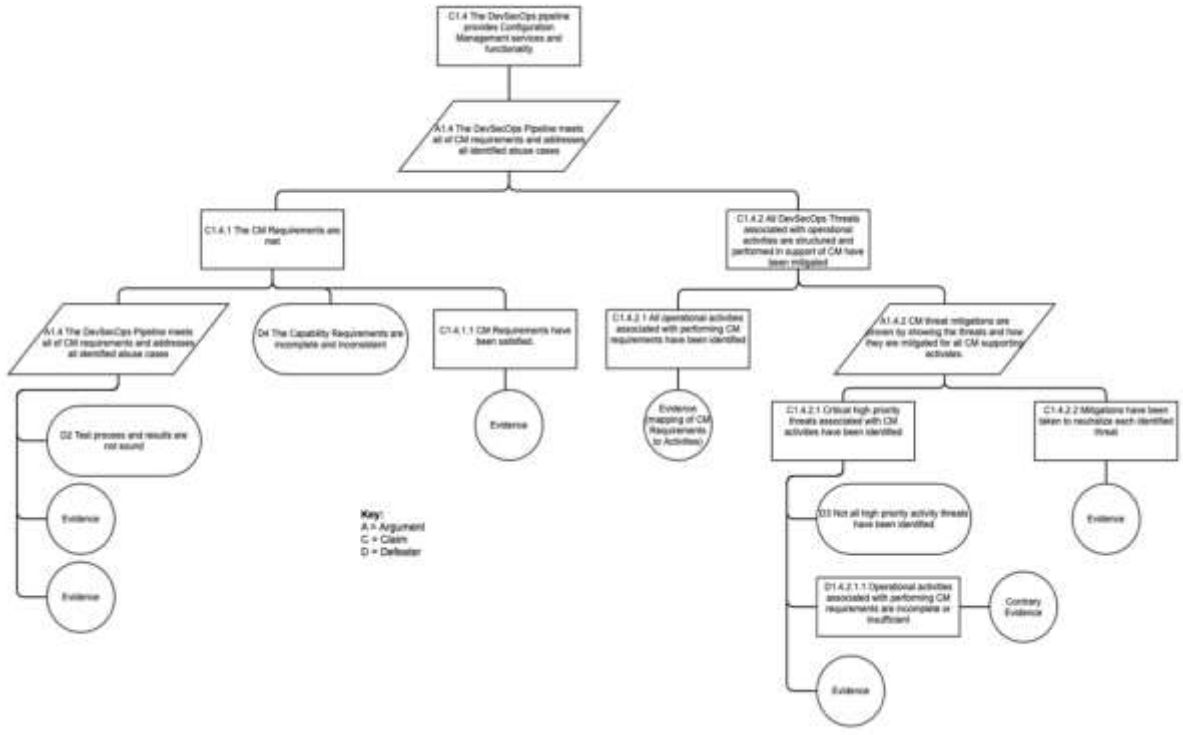
- It is a structured approach used to argue that available evidence supports a given claim
- It provides the organization with the basis for making risk-based choices tied to assuring that the pipeline only functions as intended.
- It provides requirements for automated systems testing, or other evidence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

Assuring that your Program only Functions as Intended

Carnegie Mellon University Software Engineering Institute

Assurance cases are composed of the following elements:

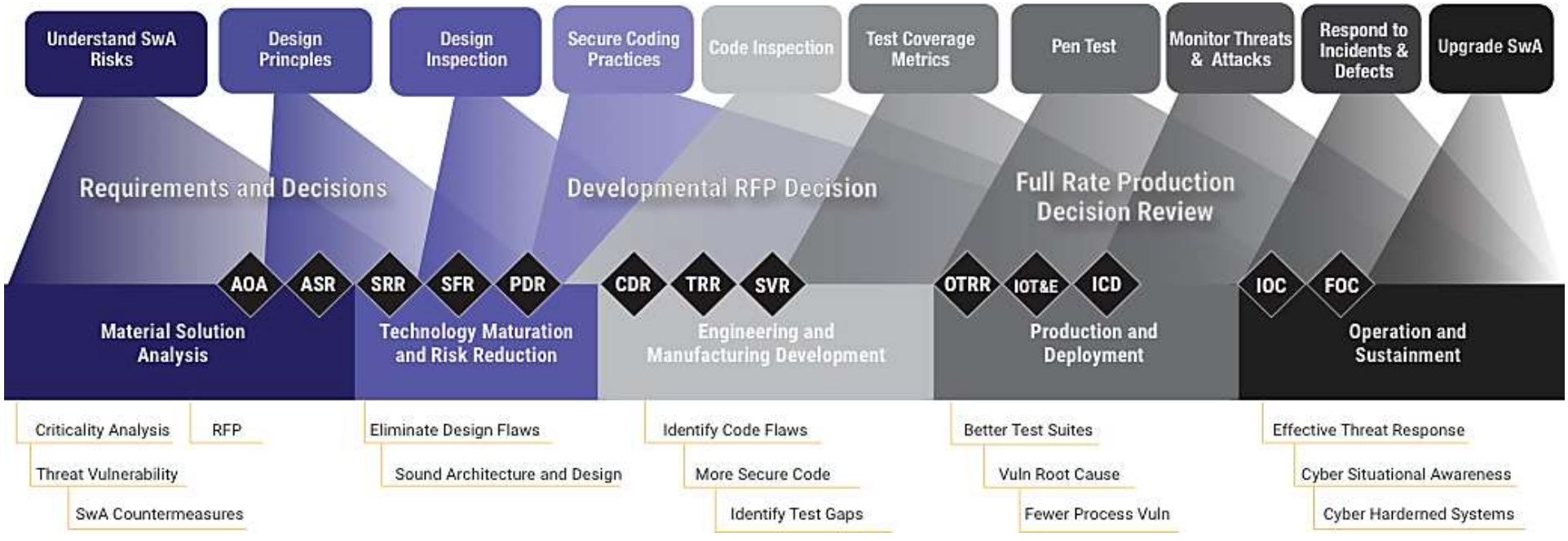
- Claims– “assertions put forward for general acceptance. They are typically statements about a property of the system or some subsystem. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called subclaims [1].”
- Arguments – “link the evidence 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.

Just like Quality, Security is a lifecycle challenge

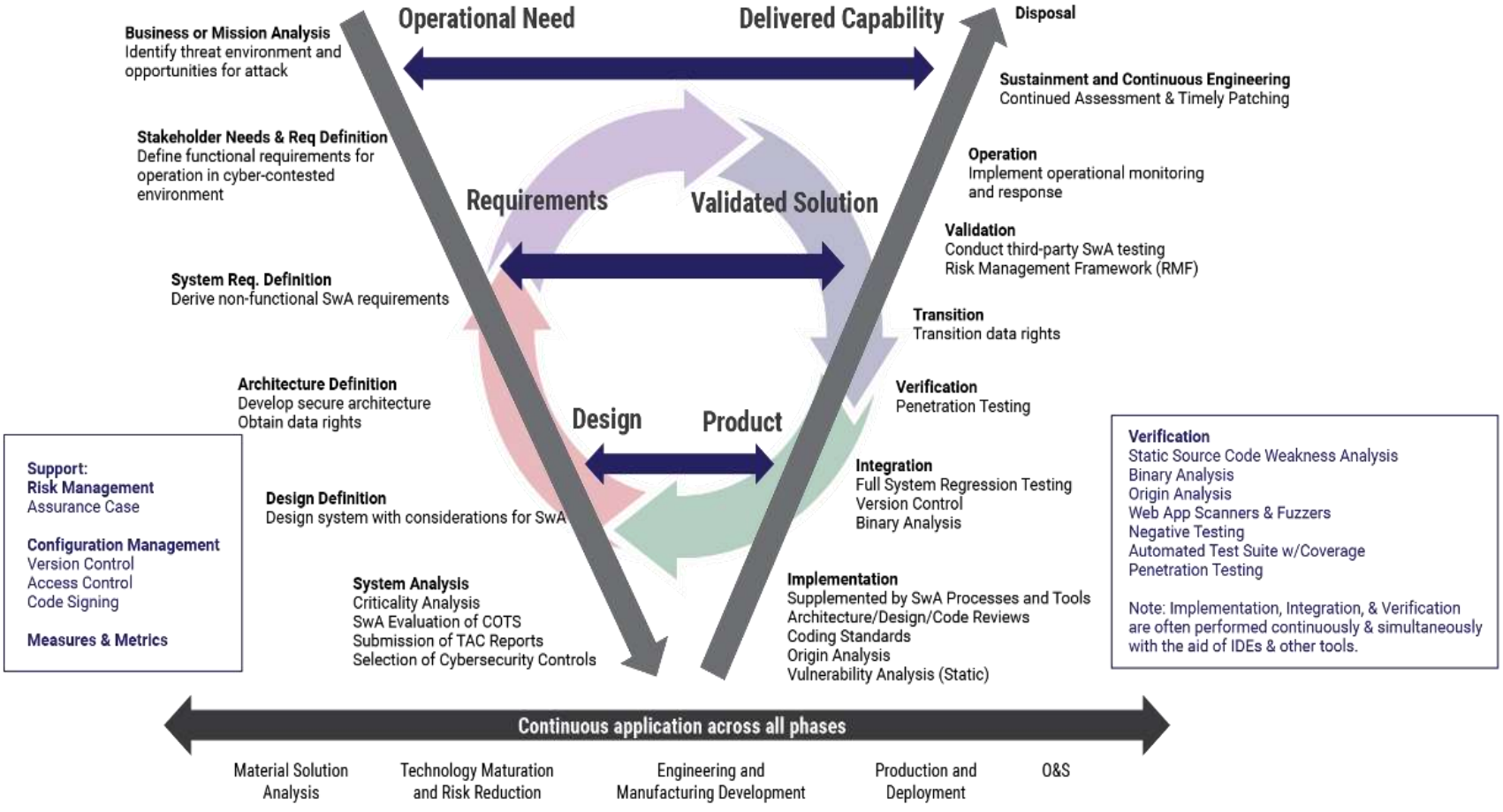


Threat Modeling

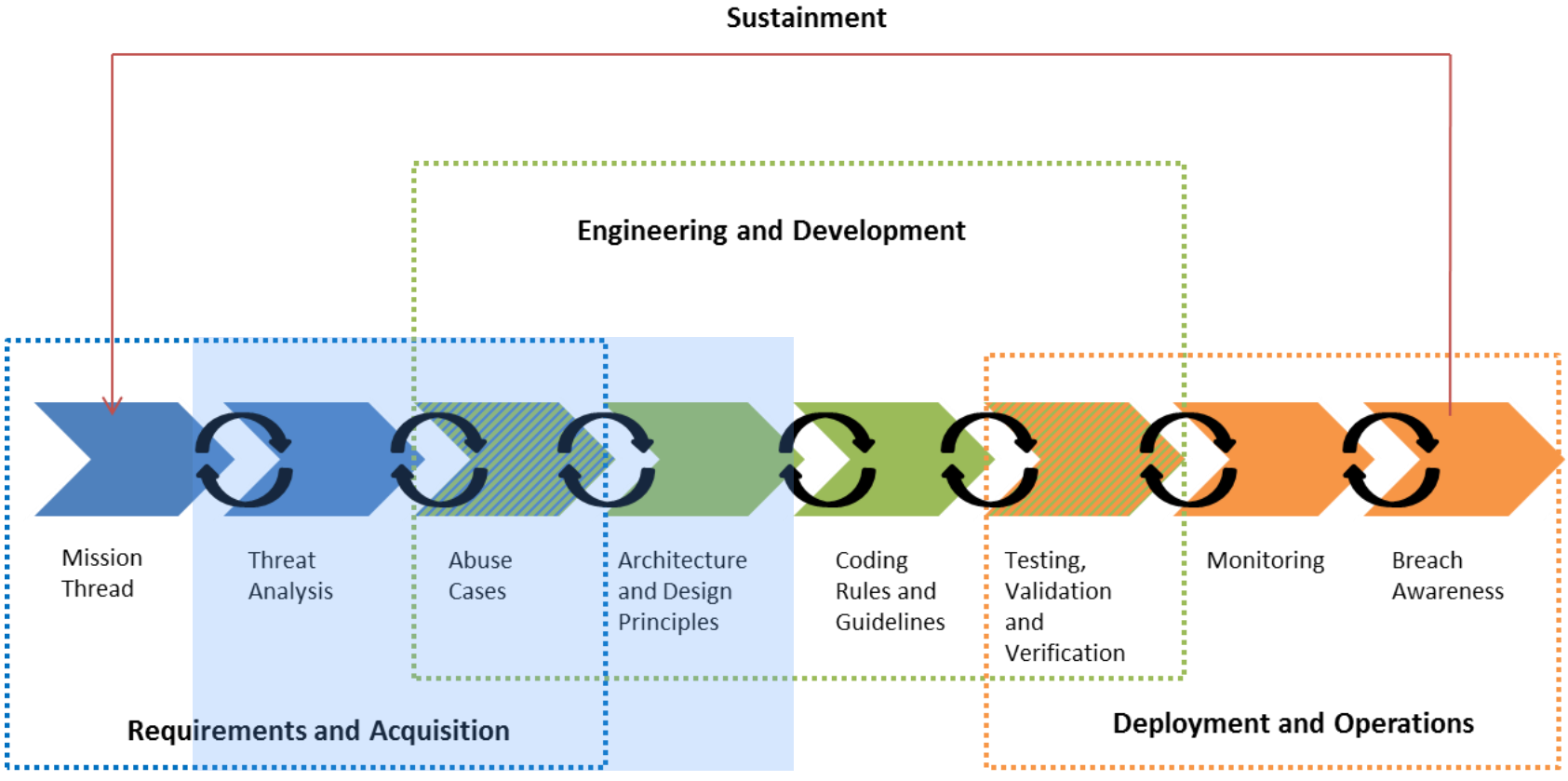
- **Threat Modeling** is the process of creating an abstraction of a system, aimed at identifying attackers' abilities and goals, and using that abstraction to generate and catalog possible threats that the system must mitigate.
- While security can be analyzed at the networking and code levels to prevent 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/

Software Assurance Activities Mapping



Requirements and Architecture



Security Requirements Challenges

Carnegie Mellon University Software Engineering Institute

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.*"

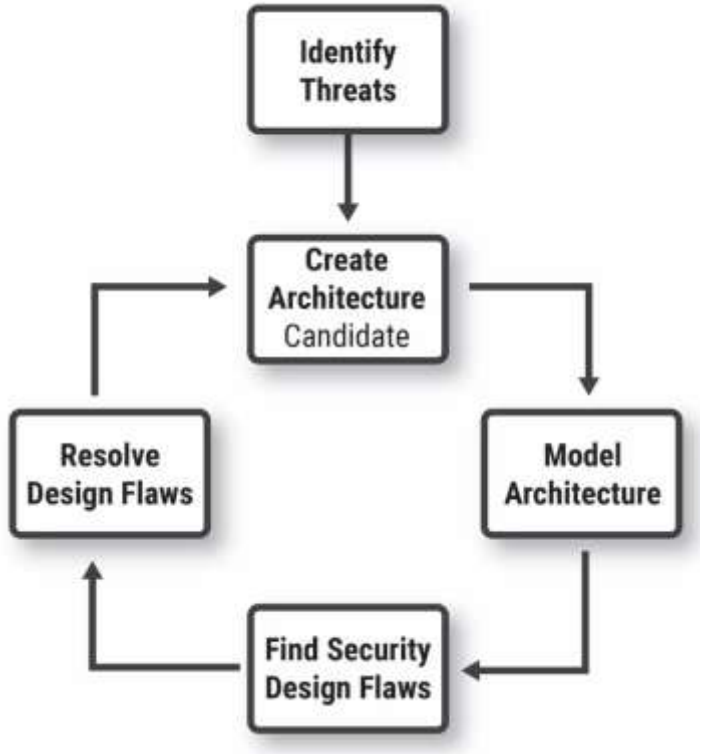
https://resources.sei.cmu.edu/asset_files/TechnicalNote/2018_004_001_516627.pdf

Value of Modeling Security

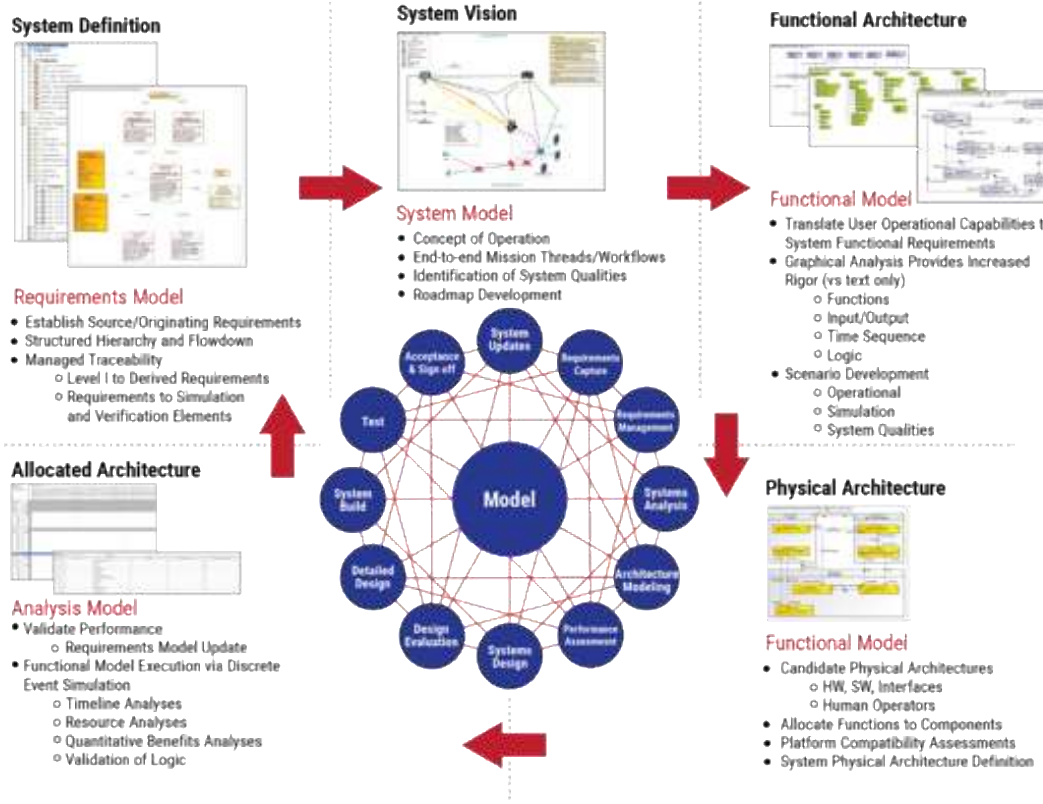
Crucial security decisions to address threats are made in the architecture.

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.



Model Based Systems Engineering



*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.

- ***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

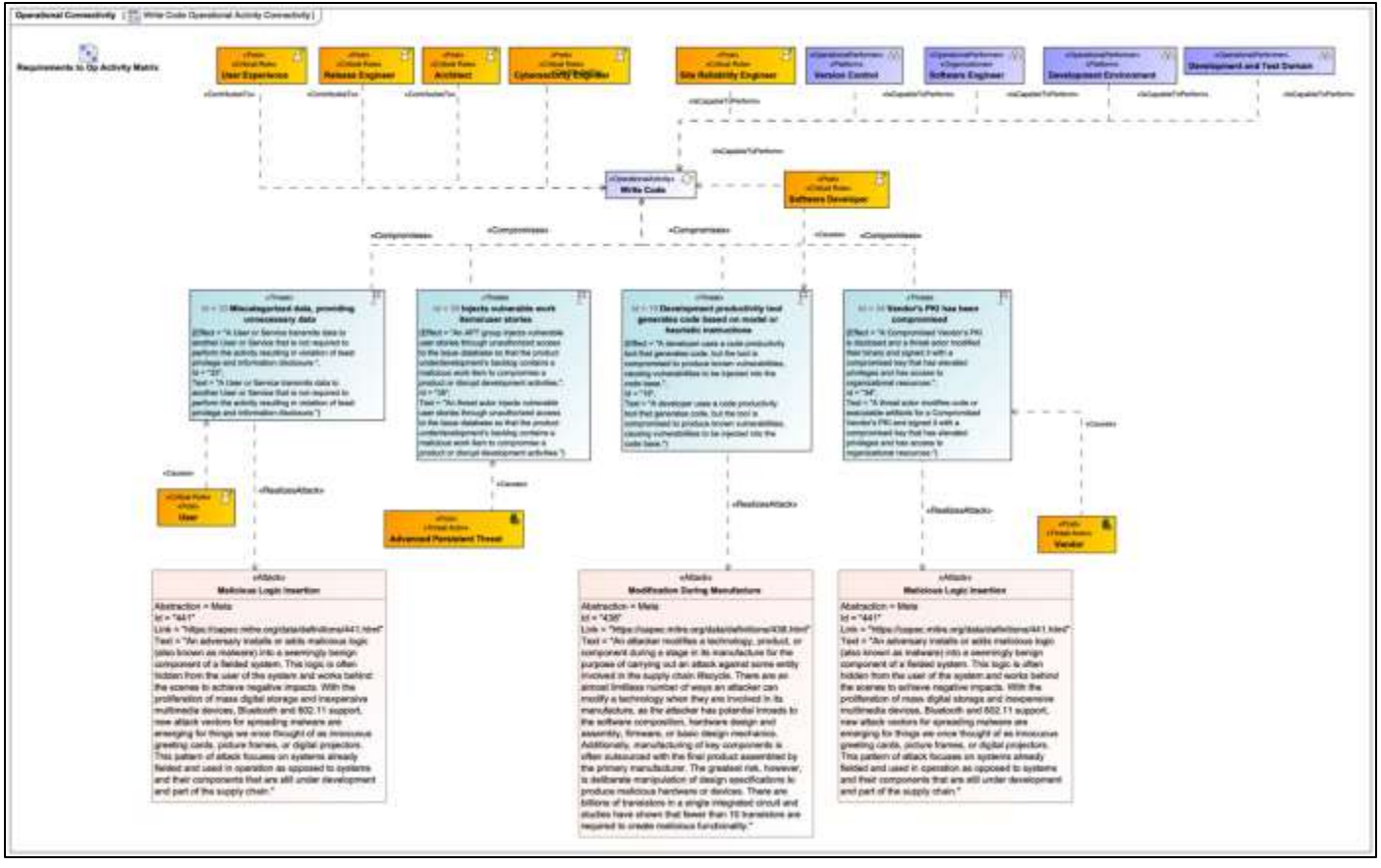
Threat Scenario Generation Workshop

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: • Requirements Diagrams • Operational Process Flows • Relationships between Operational Activities and System Requirements • Operational resource structure, Posts (i.e. roles) and corresponding responsibilities including the Involvement relationships.	
General	• 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	• 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	• 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	• Outline system purpose and constraints
		• Review system's architectural views and relationships
		  ○ Requirements
		  ○ Strategy
		  ○ Personnel
		  ○ Operational

4	Operational Process Flow Focus Area	• 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	• 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	• Use the same operational activity as in step 5. • Break into groups of 2-3 people. • 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	• If this is the first time any of the participates 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	• 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 activates within the selected operational process flow.
9	Identify Operational Process Flow Threats	• Repeat steps 4-8 until threats have been identified for all operational process flows for the given system.
10	Consolidate and Review	• 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.

Example Threat Modeling Diagram for Write Code Operational Activity



[Write Code Operational Activity Connectivity Link]

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: • Requirements Diagrams • Operational Process Flows • Relationships between Operational Activities and System Requirements • Operational resource structure, Posts (i.e. roles) and corresponding responsibilities including the Involvement relationships.	
General	• 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	• 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	• 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	• Outline system purpose and constraints
		• Review system's architectural views and relationships
		  ○ Requirements
		  ○ Strategy
		  ○ Personnel
		  ○ Operational

4	Operational Process Flow Focus Area	• 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	• 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	• Use the same operational activity as in step 5. • Break into groups of 2-3 people. • 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	• If this is the first time any of the participates 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	• 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 activates within the selected operational process flow.
9	Identify Operational Process Flow Threats	• Repeat steps 4-8 until threats have been identified for all operational process flows for the given system.
10	Consolidate and Review	• 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/

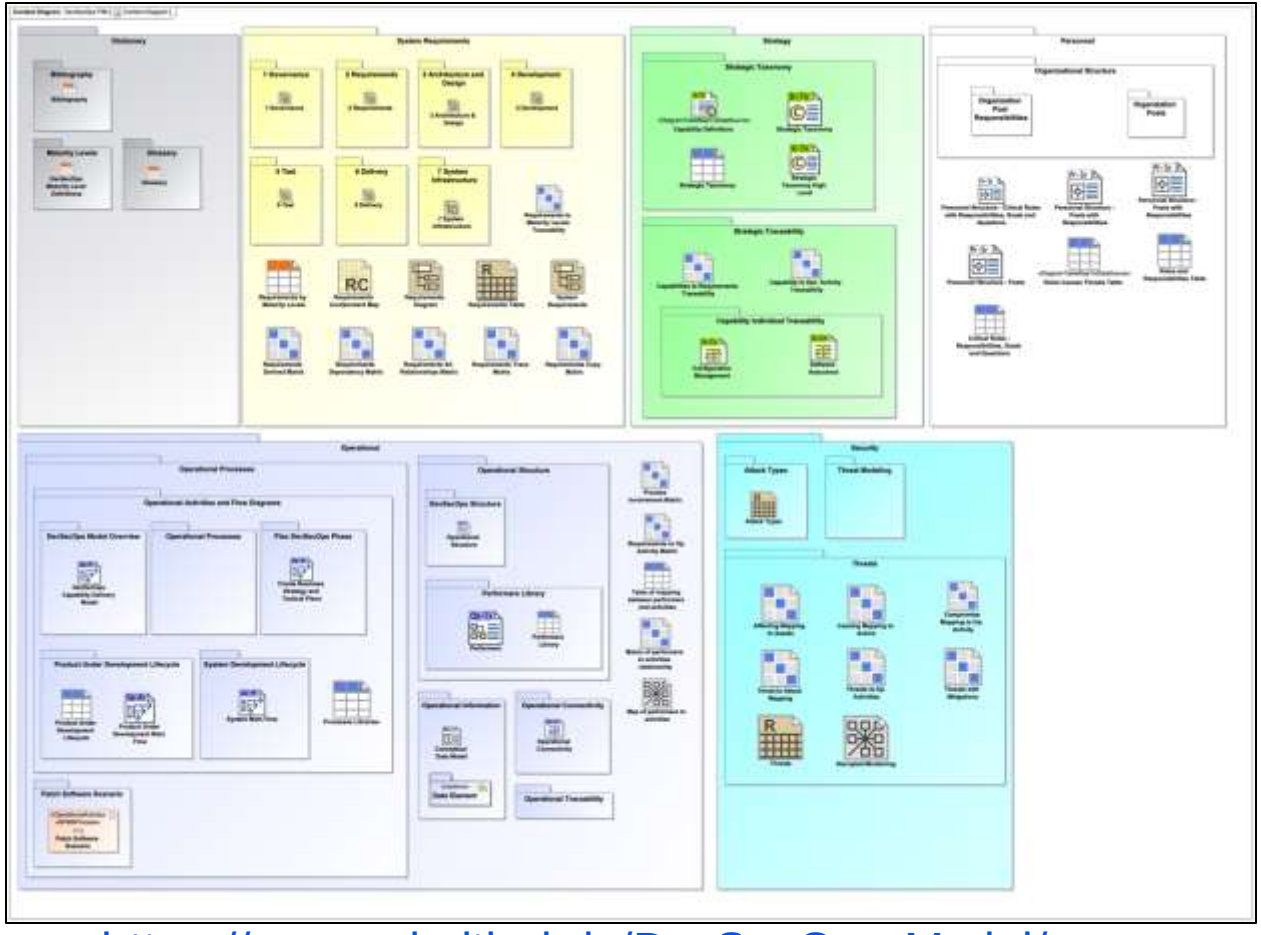
Threat Scenario Generation Workshop

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: • Requirements Diagrams • Operational Process Flows • Relationships between Operational Activities and System Requirements • Operational resource structure, Posts (i.e. roles) and corresponding responsibilities including the Involvement relationships.	
General	• 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	• 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	• 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.

	System and Architectural Overview	• Outline system purpose and constraints
		• Review system's architectural views and relationships
		  ○ Requirements
		  ○ Strategy
		  ○ Personnel
		  ○ Operational

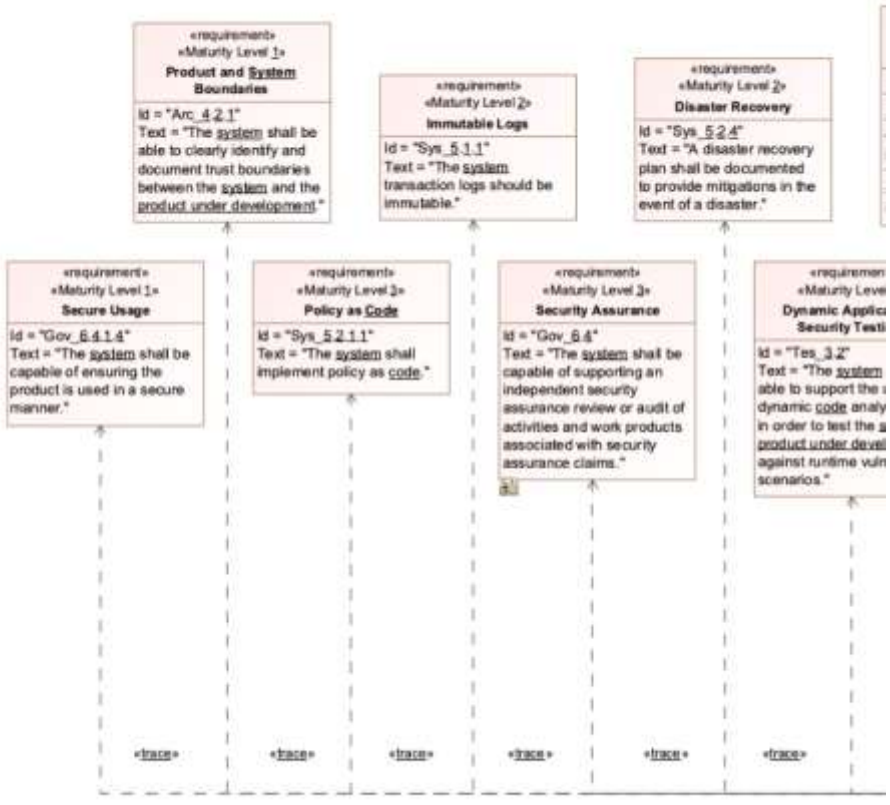
4	Operational Process Flow Focus Area	• Select an operational process flow to focus the threat scenario generation • Review the selected operational process flow to gain understanding of the process, data flow between operational activities, and performers involved. This may include reviewing associated requirements to understand the scope and context of the various operational activities.
5	Unstructured Brainstorming	• 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	• Use the same operational activity as in step 5. • Break into groups of 2-3 people. • 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	• If this is the first time any of the participates 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	• 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 activates within the selected operational process flow.
9	Identify Operational Process Flow Threats	• Repeat steps 4-8 until threats have been identified for all operational process flows for the given system.
10	Consolidate and Review	• 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.

Unified Architecture Framework (UAF) - Content Diagram



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

Requirements



Example of Requirements Representation in Diagrams from PIM

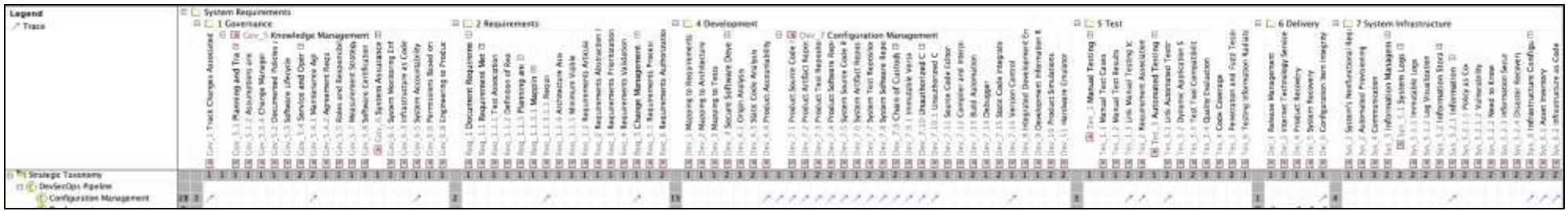
Requirements are organized into categories based on logical and functional groupings

Requirements Table Link

Capability/Strategic Viewpoint

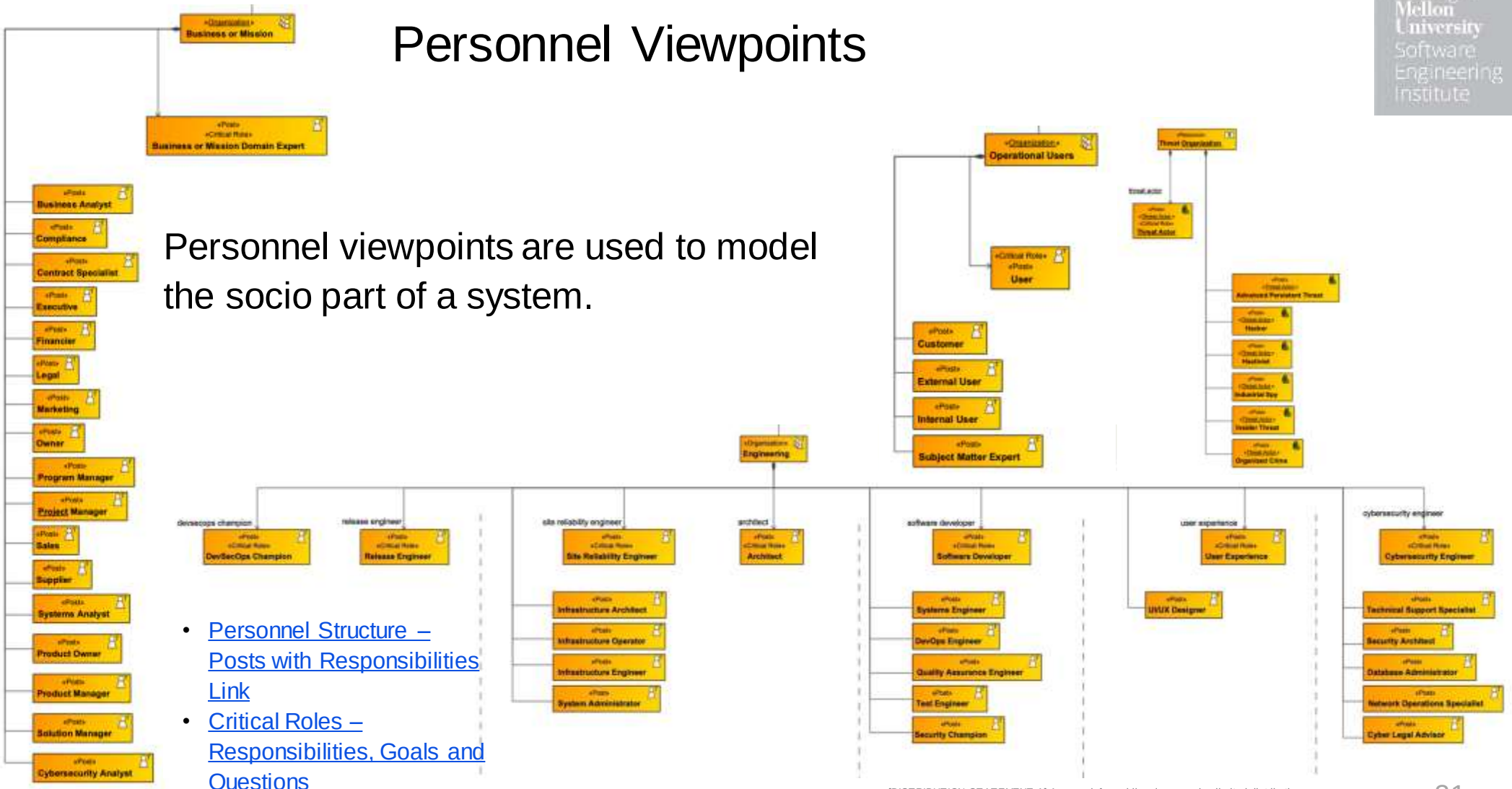
A capability is a high-level concept that describes the ability of a system to achieve or perform a task or a mission.

- Capability to Requirements Traceability Link
- Capability to Operational Activity Traceability Link
- Capability Definitions Link
- Strategic Taxonomy High Level



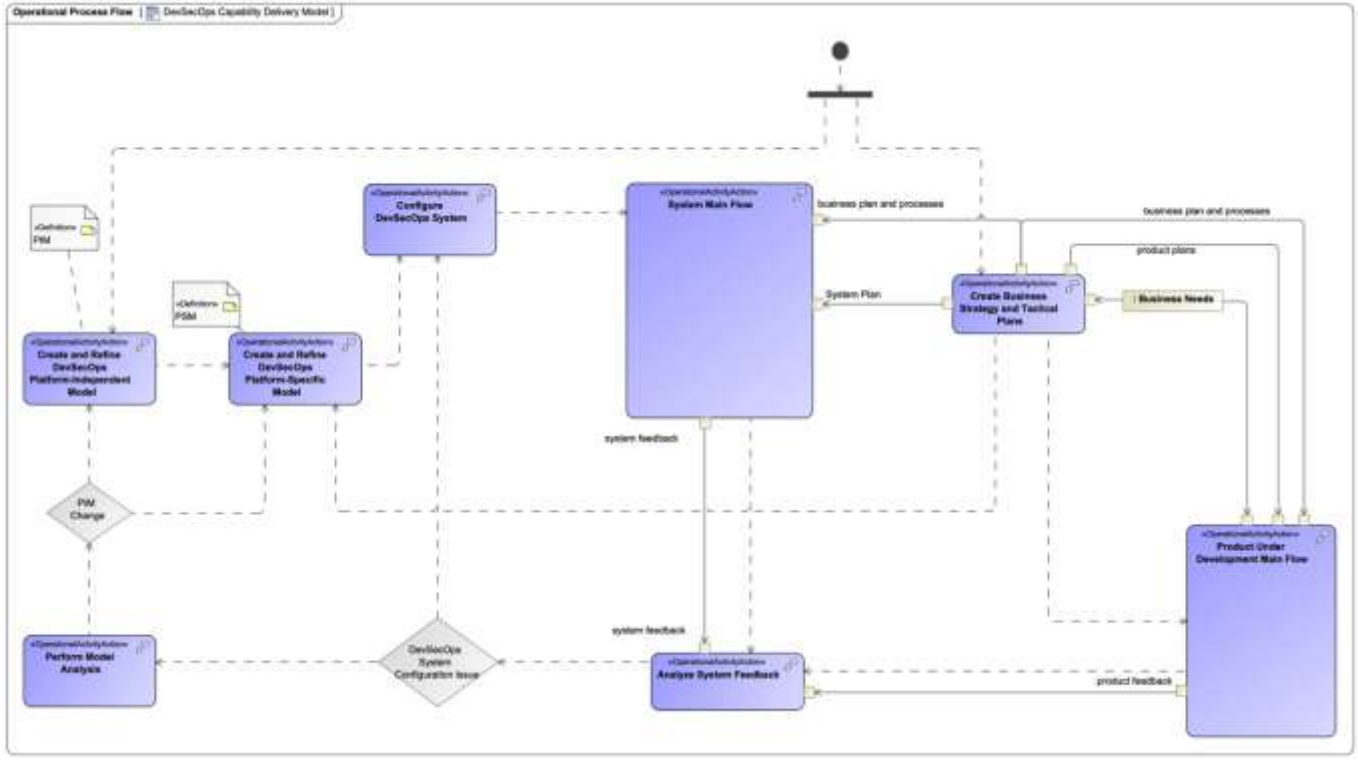
Personnel Viewpoints

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



- Personnel Structure – Posts with Responsibilities Link
- Critical Roles – Responsibilities, Goals and Questions

Operational Viewpoints



- DevSecOps Capability Delivery Model Link

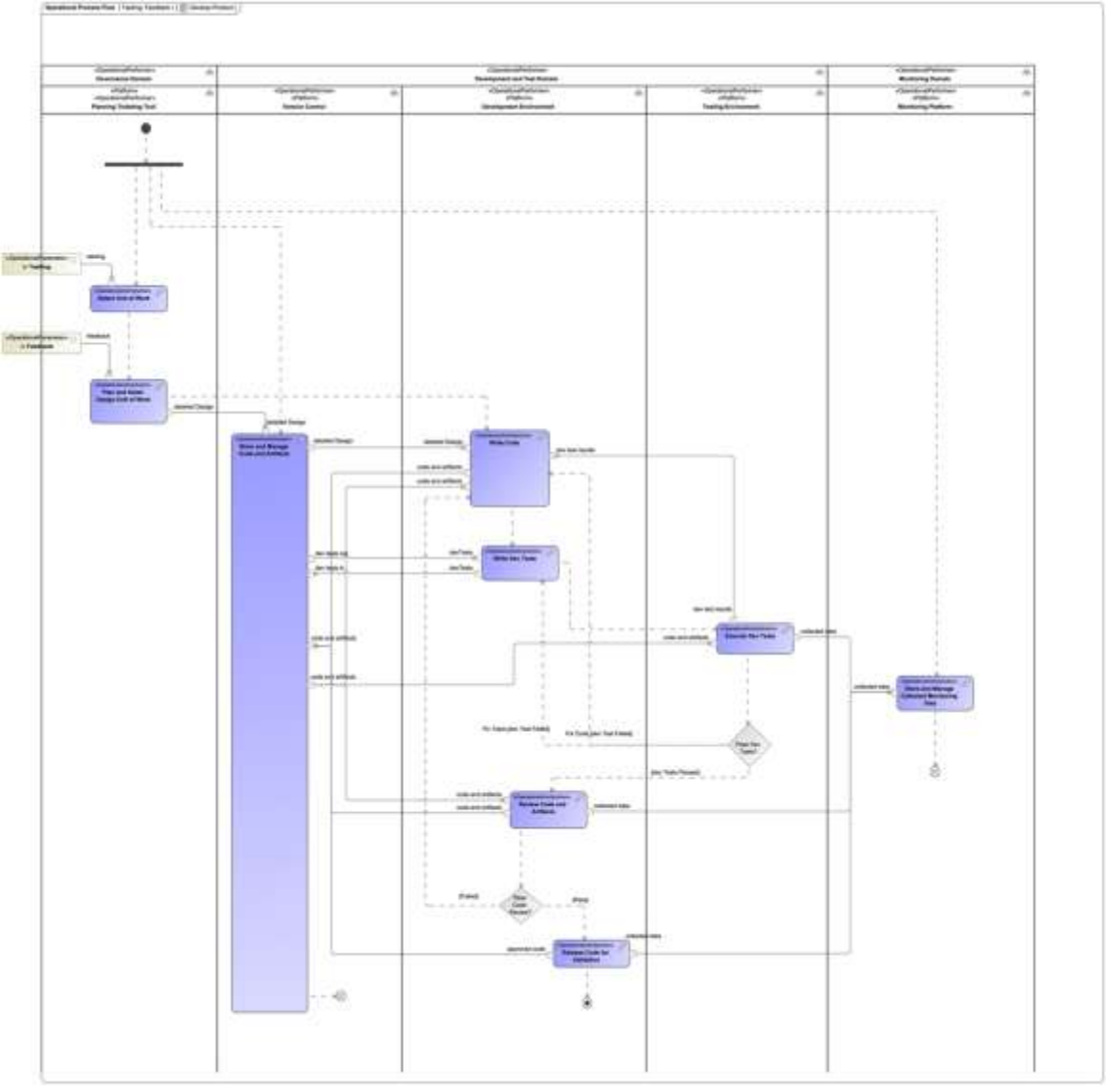
An operational model for a system describes behavior of the system to conduct program operations

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: • Requirements Diagrams • Operational Process Flows • Relationships between Operational Activities and System Requirements • Operational resource structure, Posts (i.e. roles) and corresponding responsibilities including the Involvement relationships.	
General	• 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	• 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	• 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	• Outline system purpose and constraints
		• Review system's architectural views and relationships
		  ○ Requirements
		  ○ Strategy
		  ○ Personnel
		  ○ Operational

4	Operational Process Flow Focus Area	• 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	• 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	• Use the same operational activity as in step 5. • Break into groups of 2-3 people. • 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	• If this is the first time any of the participates 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	• 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 activates within the selected operational process flow.
9	Identify Operational Process Flow Threats	• Repeat steps 4-8 until threats have been identified for all operational process flows for the given system.
10	Consolidate and Review	• 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.



Operational Process Flow Focus Area

- 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

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: • Requirements Diagrams • Operational Process Flows • Relationships between Operational Activities and System Requirements • Operational resource structure, Posts (i.e. roles) and corresponding responsibilities including the Involvement relationships.	
General	• 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	• 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	• 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	• Outline system purpose and constraints
		• Review system's architectural views and relationships
		  ○ Requirements
		  ○ Strategy
		  ○ Personnel
		  ○ Operational

4	Operational Process Flow Focus Area	• 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	• 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	• Use the same operational activity as in step 5. • Break into groups of 2-3 people. • 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	• If this is the first time any of the participates 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	• 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 activates within the selected operational process flow.
9	Identify Operational Process Flow Threats	• Repeat steps 4-8 until threats have been identified for all operational process flows for the given system.
10	Consolidate and Review	• 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.

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: • Requirements Diagrams • Operational Process Flows • Relationships between Operational Activities and System Requirements • Operational resource structure, Posts (i.e. roles) and corresponding responsibilities including the Involvement relationships.	
General	• 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	• 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	• 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	• Outline system purpose and constraints
		• Review system's architectural views and relationships
		  ○ Requirements
		  ○ Strategy
		  ○ Personnel
		  ○ Operational

4	Operational Process Flow Focus Area	• 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	• 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	• Use the same operational activity as in step 5. • Break into groups of 2-3 people. • 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	• If this is the first time any of the participates 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	• 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 activates within the selected operational process flow.
9	Identify Operational Process Flow Threats	• Repeat steps 4-8 until threats have been identified for all operational process flows for the given system.
10	Consolidate and Review	• 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.

Definition

STRIDE is currently the most mature threat finding method. Invented by Loren Kohnfelder and Praerit Garg in 1999 and adopted by Microsoft in 2002, STRIDE has evolved over time to include new threat-specific tables and the variants STRIDE-per-Element and STRIDE-per-Interaction.

It's a mnemonic.

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

STRIDE(S)

Finding Threats

- Generated set of known threats based on threat types
- Use tables and checklists for assistance

Element	Interaction	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege	Scarce (Missing or Insufficient Process)
Process	Process has outbound data flow to data managing process	Downstream data managing activity is spoofed, and main process writes to the wrong place	Tampering with outgoing data		Current activity provides to data managing activity data of wrong classification (e.g. unauthorized distribution of controlled data)			An activity is skipped entirely
	Process sends output to external process	Downstream external activity is spoofed, and the wrong activity is communicated with		Downstream external activity claims not to have been called by current activity	An external activity receives data that should not have access to	Current activity is not available due to corrupted state	An external activity can impersonate an internal activity and use its privilege	
	Process sends output to external interactor (human)	A role that is performer, approver, contributor, or observer for the activity is spoofed		Role disclaims seeing the output	Unauthorized user/role gets access to an activity	Current activity is not available due to responsible role unavailability		
	Process has inbound data flow from data managing process	Upstream data managing activity is spoofed	Activity is corrupted by data read from a data managing activity			Current activity is not available due to data flow interruption	Current activity internal state is corrupted based on data read from upstream activity	
	Process has inbound data flow from a trusted process	Current activity believes it is getting data from an upstream activity	Tampering with data incoming into activity	Downstream external activity deny receiving data from current activity		Current activity is not available due to control flow disruption	An activity passes data that allows it to change the internal flow of the current activity	
	Process has inbound data flow from external process	Current activity believes it is getting data from an upstream activity						

Finding Threats - Continued

Element	Interaction	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege	Scarce (Missing or Insufficient Process)
Data Flow (commands /responses)	Crosses machine boundary		Tampering with data incoming into activity (Man in the middle attack)		Data that passes from activity to activity is sniffed “on the wire” (intercepted by an unauthorized actor)	The data flow between activities is interrupted by an external entity		
Data Store (database /backend)	Process has outbound data flow to data store		Tampering with incoming data (corrupted in a data store)	Current activity claims not to have provided data to data managing activity	Data was disclosed by data managing activity - Mishandling of data - Unauthorized access to the activity			
	Process has inbound data flow to data store			Current activity claims not to have received data from data managing activity	Data was disclosed by data managing activity - Mishandling of data - Unauthorized access to the activity	Data managing activity fails to store information		
External Activity (An activity that is part of a separate process /flow)	External interactor passes input to process	Main activity is confused about the identity of the performer/contributor role		Current activity claims not to received data	Current activity receives unnecessary data	Data managing activity fails to provide authorized data access		
	External interactor gets input to process	Performer/contributor role is confused about the identity of the current activity						

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: • Requirements Diagrams • Operational Process Flows • Relationships between Operational Activities and System Requirements • Operational resource structure, Posts (i.e. roles) and corresponding responsibilities including the Involvement relationships.	
General	• 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	• 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	• 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	• Outline system purpose and constraints
		• Review system's architectural views and relationships
		  ○ Requirements
		  ○ Strategy
		  ○ Personnel
		  ○ Operational

4	Operational Process Flow Focus Area	• 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	• 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	• Use the same operational activity as in step 5. • Break into groups of 2-3 people. • 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	• If this is the first time any of the participates 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	• 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 activates within the selected operational process flow.
9	Identify Operational Process Flow Threats	• Repeat steps 4-8 until threats have been identified for all operational process flows for the given system.
10	Consolidate and Review	• 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.

Six part Threat Scenario

STATEMENT TEMPLATE: An [ACTOR] performs an [ACTION] to [ATTACK] an [ASSET] to achieve an [EFFECT] and/or [OBJECTIVE].

Part	Description
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

Threat Scenario Example

Statement: An insider threat publicly releases the results of static and dynamic analysis to the public to damage the organization's reputation.

Part	Description
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

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: • Requirements Diagrams • Operational Process Flows • Relationships between Operational Activities and System Requirements • Operational resource structure, Posts (i.e. roles) and corresponding responsibilities including the Involvement relationships.	
General	• 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	• 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	• 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	• Outline system purpose and constraints • Review system's architectural views and relationships o Requirements o Strategy o Personnel o Operational
4	Operational Process Flow Focus Area	• Select an operational process flow to focus the threat scenario generation • Review the selected operational process flow to gain understan 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 variou operational activities.
5	Unstructured Brainstorming	• 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	• Use the same operational activity as in step 5. • Break into groups of 2-3 people. • 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	• If this is the first time any of the participates 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.
	Operational Activity Threat Identification	• 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 activates within the selected operational process flow.
	Identify Operational Process Flow Threats	• Repeat steps 4-8 until threats have been identified for all operational process flows for the given system.
	Consolidate and Review	• 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.

Repeat until you have gone through system

Post-STRIDE/Post-Workshop

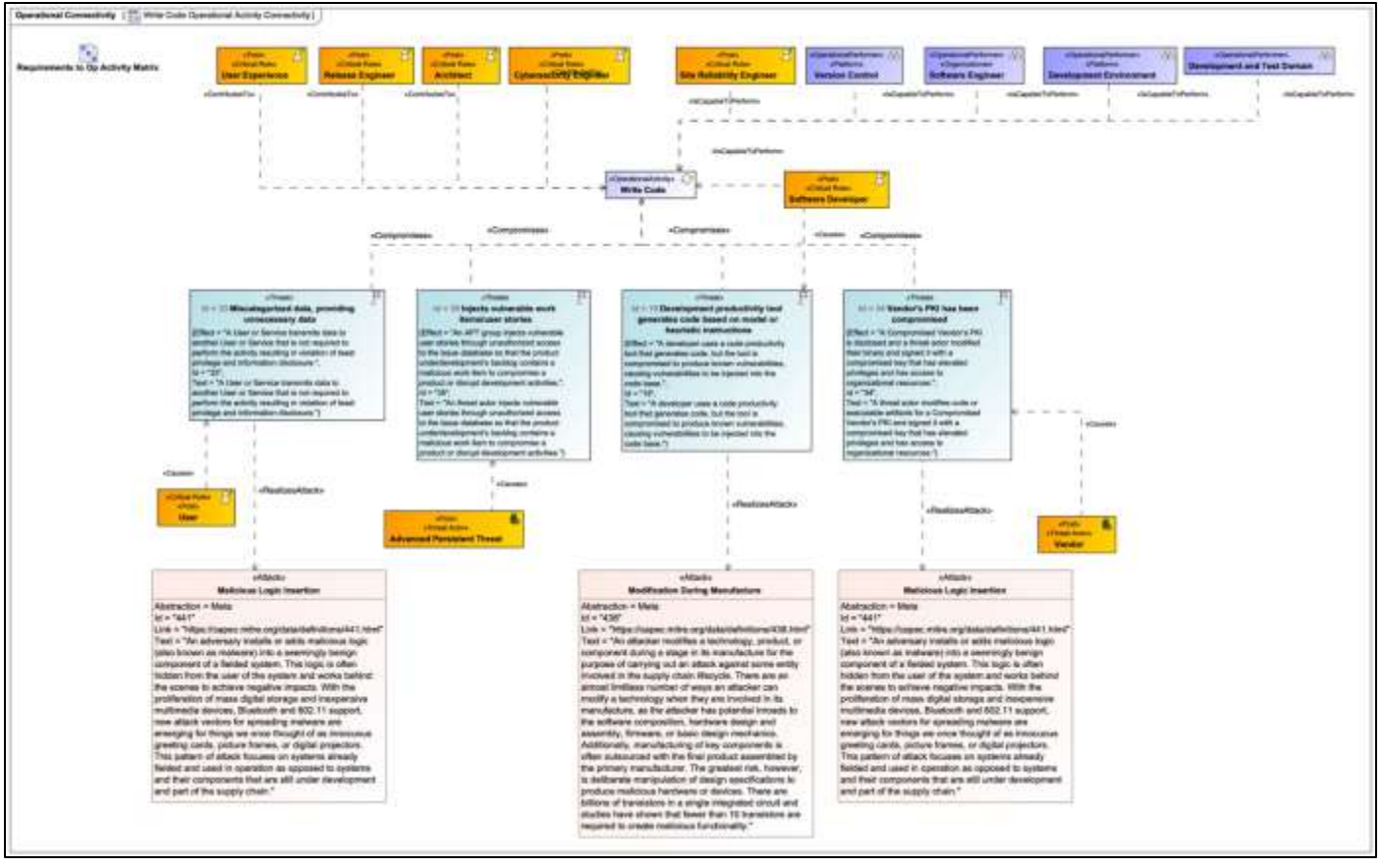
Validate the threat model

- Check and update the system model
- Work with the threats:
    - Check the validity of each of your threats
    - Verify that you have identified the likely threats to your system

Mitigating threats

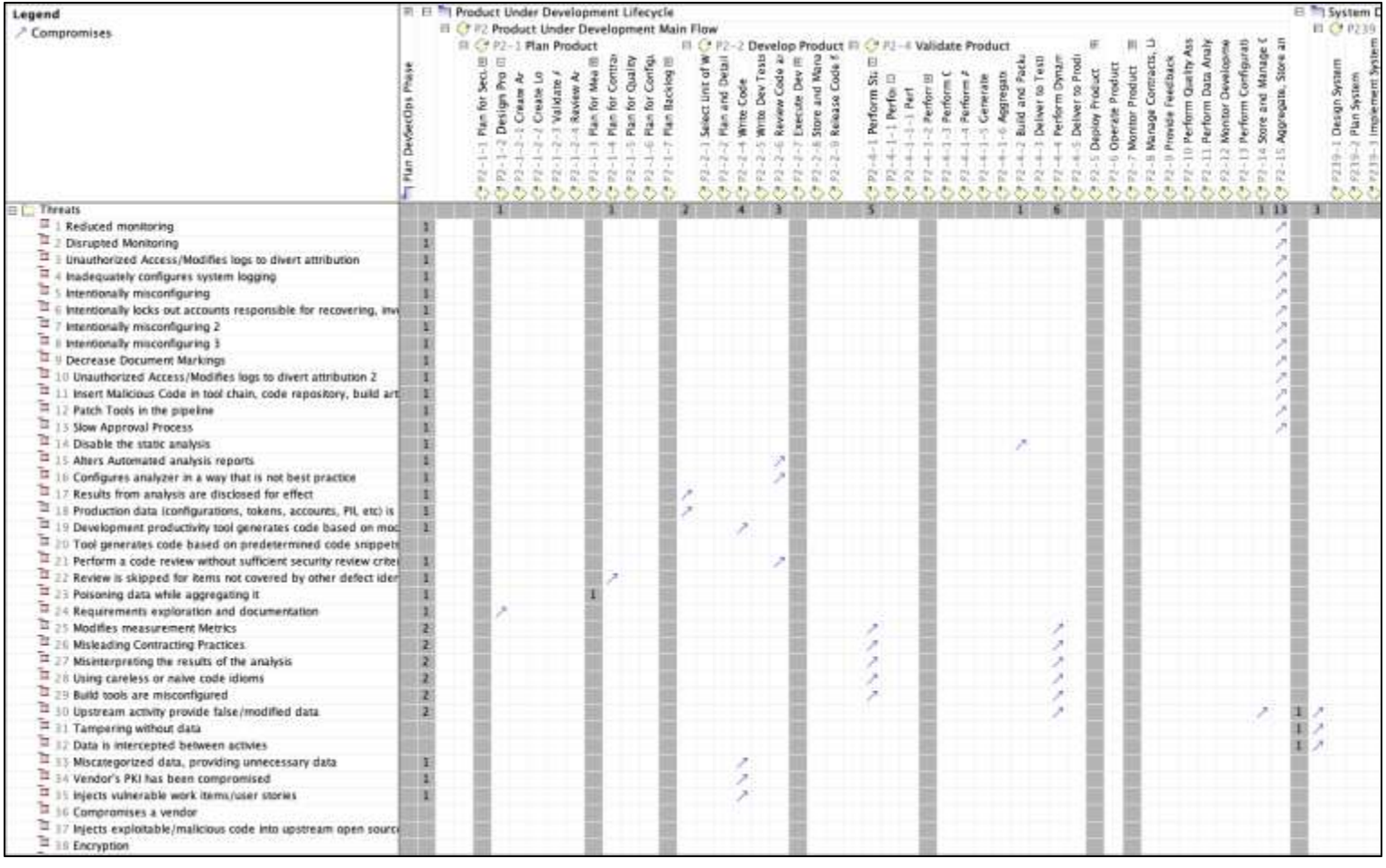
- STRIDE does not prescribe any mitigation methodology
- Identify and add mitigation strategies to valid threats within your model

Example Threat Modeling Diagram for Write Code Operational Activity



Write Code Operational Activity Connectivity Link

Threat to Operational Activity Matrix



[Threats to Operational Activities Link]

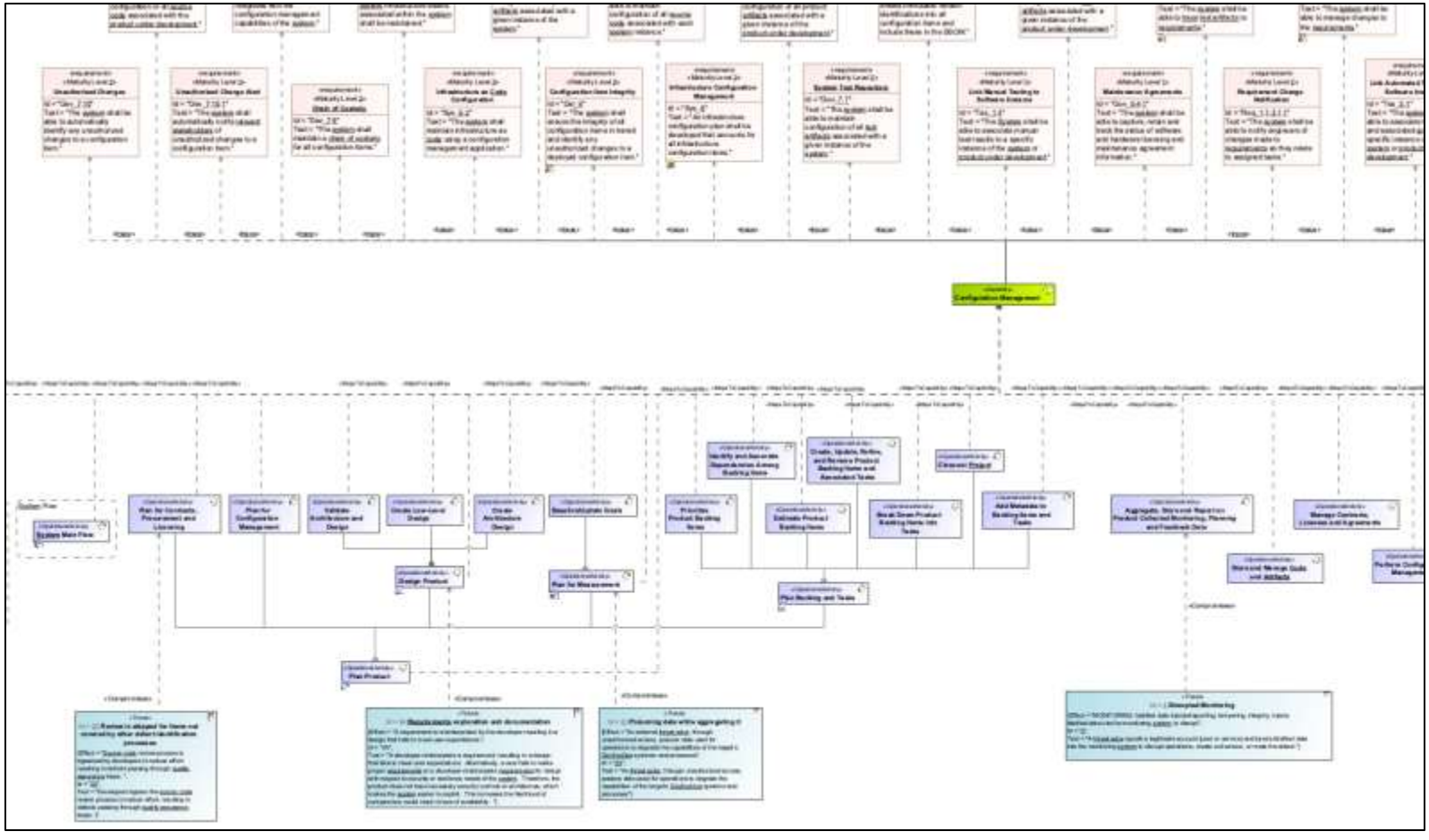
Threats with Attributes

Carnegie Mellon University Software Engineering Institute

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.html
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	161 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	161 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 significa 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 System



Example of Threats Traced to Capabilities via Operational Activities

[Configuration Management Complexity Link]

Summary/Next Steps?

Summary:

- Cyber-physical systems integrate software technology into physical infrastructures
- While innovative, cyber-physical systems are vulnerable to threats that manufacturers of traditional physical infrastructures may not consider
- Performing threat modeling on cyber-physical systems with a variety of stakeholders can help catch threats across a wide spectrum of threat types
- Threat Modeling methods can be combined with MBSE to create a more robust and well-rounded view of potential threats.

Next Steps:

- Review outline of Training? 1 or 2 days? Do you want to add additional topics? What are your desired outcomes from the training?
- Who should attend Treat Modeling Training?

Contact Information

Timothy A. Chick
CERT Systems 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