# Threat Modeling With MBSE

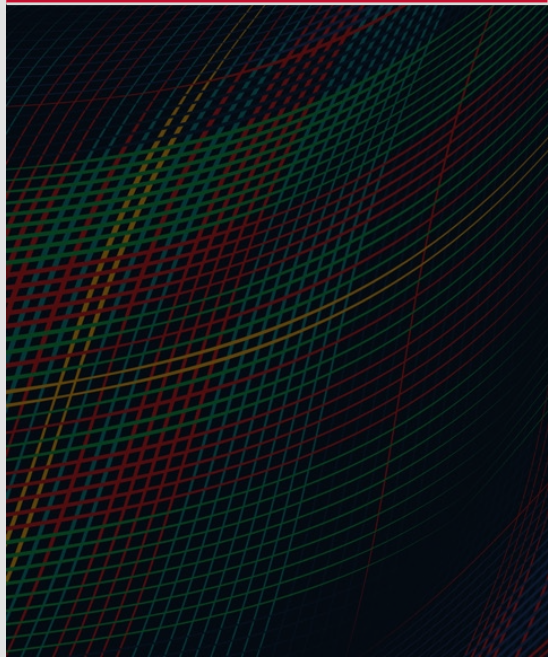
**JUNE 12, 2023**

Nataliya Shevchenko
Brent Frye





Carnegie Mellon University
Software Engineering Institute



# Document Markings

# Agenda

- What is Threat Modeling?
- Threat Scenarios
- Involvement Matrix Profile
- Threat Modeling Profile
- Threat Modeling with MBSE and UAF

Threat Modeling Training

# What is Threat Modeling?

Carnegie Mellon University
Software Engineering Institute

# Definition




*"Threat modeling is a process by which potential threats, such as structural vulnerabilities can be identified, enumerated, and prioritized—all from a hypothetical attacker's point of view. The purpose of threat modeling is to provide defenders with a systematic analysis of the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker."**

* Wikipedia contributors. "Threat model." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 22 May. 2019. Web. 19 Aug. 2019.

# Terminology




- **Asset** – a resource of value, or something that an attacker wants to access, control, or destroy
- **Threat** – a potential occurrence of an event or events that might damage or compromise an asset or objective
- **Vulnerability** – a weakness in some aspect or feature of a system that makes an exploit possible
- **Attack** – an action taken that utilizes one or more vulnerabilities to realize a threat to compromise or damage an asset

# Key Questions



1. What are we building?

   ***System's model***

2. What can go wrong?

   ***Threats scenarios***

3. What should we do about those wrongs?

   ***Mitigation strategies***

4. How good is our analysis?

   ***Validate the threat model***

Threat Modeling Training

# Threat Scenarios



Carnegie Mellon University
Software Engineering Institute

# Six Part Threat Scenario Template



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

- **ACTOR** – the person or group that is behind the threat scenario
- **ACTION** – a potential occurrence of an event that might damage an asset or goal of a strategic vision
- **ATTACK** – an action taken that utilizes one or more vulnerabilities to realize a threat to compromise or damage an asset or circumvent a strategic goal (method or technique)
- **ASSET** – a resource, person, or process that has value
- **EFFECT** – the desired or undesired consequence
- **OBJECTIVE** – the threat actor's motivation or objective for conducting the attack

# Threat Scenario Actor



An ACTOR may be:

- An authorized user who is working within the bounds of their authorized actions, but to cause a harmful effect.
- An authorized user who has exceeded their authority to achieve their effect or objective on the system.
- An unauthorized user who has obtained access to the system.
- Multiple individuals, possibly from any combination of the above listed user groups.

# Threat Scenario Effect or Objective



A security-relevant effect or objective:

- The data, functionality, service, or process are available to individuals who are not authorized to view the data or use functionality/services/process.
- The user is able to make changes to the data or process beyond what is authorized for that user; the data/process is no longer trustworthy.
- The data, functionality, services, or process are no longer accessible by users who should be allowed to access them; denial of service.
- A process or a step in a process is not performed.

# Steps for Generating Threat Scenarios



1. Gather stakeholders for brainstorming.
2. Identify the system or subsystem you will do the threat modeling for, including assets and data flows.
3. For each prioritized asset (“the crown jewel”), find what can get wrong (events/actions) and the expected losses.
4. Identify methods and resources the threat actor would need in order to succeed at causing the specified loss with the specified action.
5. Based on the actions and resources needed, determine viable actors for the scenario.
6. Identify goals or objectives related to the identified loss that are relevant to the identified threat actor(s).
7. Document statements: An [ACTOR] performs an [ACTION] to [ATTACK] an [ASSET] to achieve an [EFFECT] and/or [OBJECTIVE].

# Form Threat Scenario



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 |

Carnegie Mellon University
Software Engineering Institute

Threat Modeling Training

# Threat Modeling with MBSE and UAF

Threat Modeling Training

# Involvement Matrix



Carnegie Mellon University
Software Engineering Institute

# Involvement Matrixes

Types of relationships between a relevant stakeholder and an operational process:

RSIM – Relevant Stakeholder Involvement Matrix

- Unaware
- Resistant
- Neutral
- Supportive
- Leading

SRAM or RACI – Responsible, Accountable, Consulted, Informed Matrix

- Responsible
- Accountable
- Consulted
- Informed

# Involvement Profile



Definitions

- *Producer* – a role responsible for performing the activity or producing the deliverable. This role's action is to perform.
- *Approver* – a role accountable for approving the activity or deliverable. This role's action is to approve.
- *Contributor* – a role that needs to be given an opportunity to provide input on the activity or deliverable before it is completed. This role's action is to contribute.
- *Observer* – a role that needs to be informed of the activity or deliverable after it is completed. This role's action is to observe.

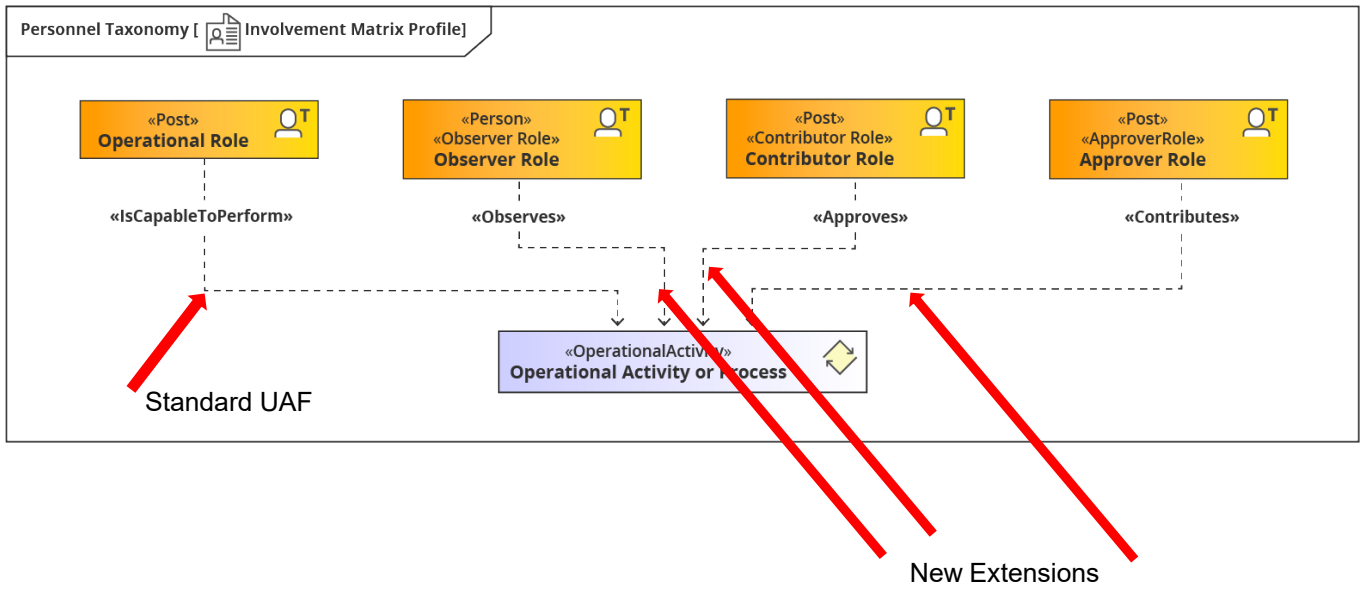
Existing UAF Element and Relationship:

- Performer/Operational Performer – *Producer*
- IsCapableToPerform

New Element and Relationship:

- Approver element
- Observer element
- Contributor element
- Approves relationship (from a role element to Operational Activity)
- Observes relationship (from a role element to Operational Activity)
- Contributes to relationship (from role element to Operational Activity)

# Involvement Profile in the Model



Carnegie Mellon University
Software Engineering Institute

Threat Modeling Training

# Extending Security Viewpoint

# UAF Security Viewpoint



Standard

- Main elements
  - Security Enclave
  - Risk
  - Security Control
  - Mitigation
  - Security Process
- Main relationships
  - Affects
  - Protects
  - Mitigates
  - Owns Risk

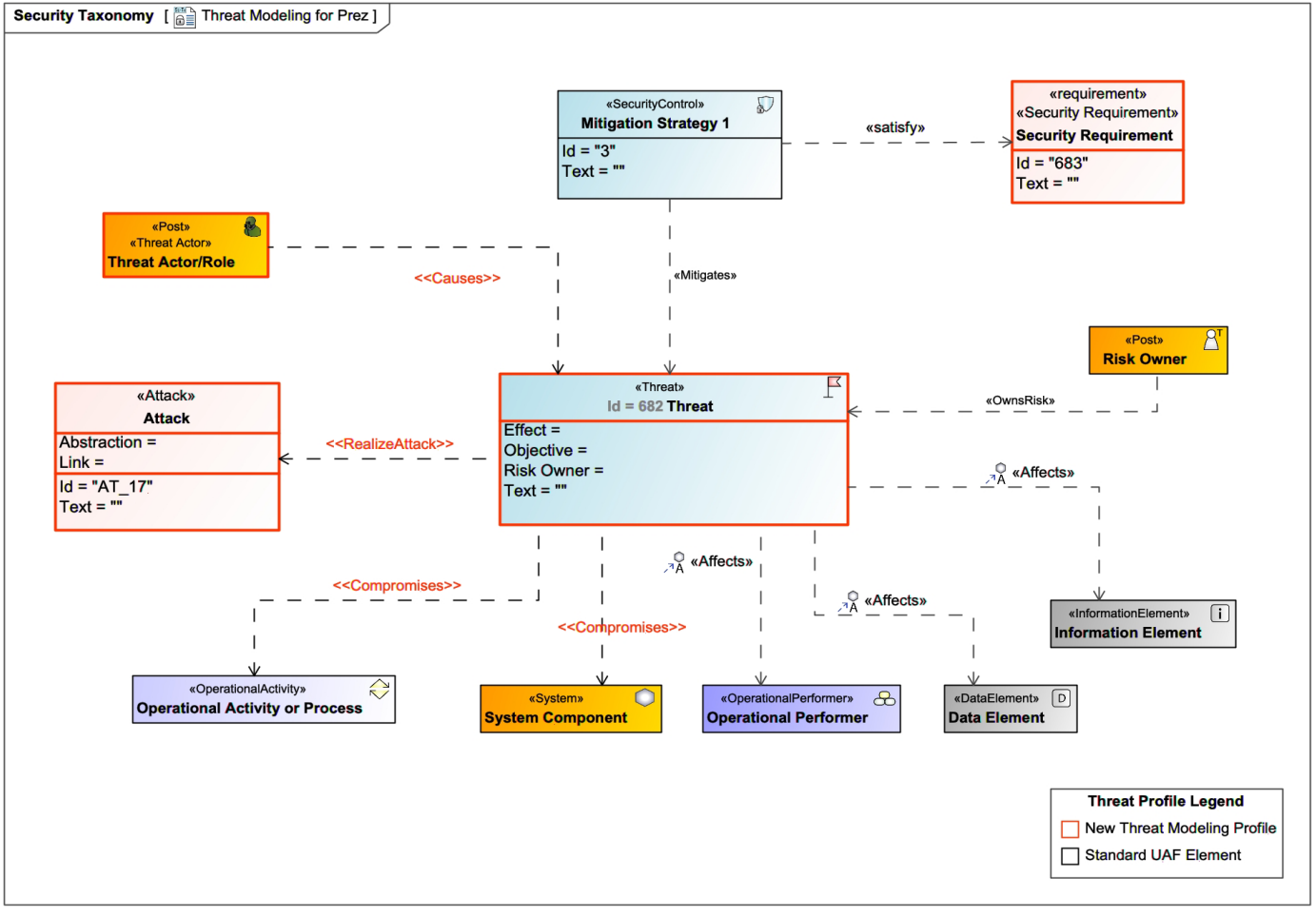
# Threat Modeling Profile



Extension

- New elements
  - Threat
    - ID, Name, Text, Effect, Objective
  - Attack
    - ID, Name, Text, Abstraction, Link
- New stereotypes
  - Threat Actor (to apply to Post element representing external threat actors)
  - Security Requirement (from Threat element to Operational Activity element)
- Main relationships
  - Compromises (from Threat element to Operational Activity element)
  - RealizesAttack (from Threat element to Attack element)
  - Causes (from Post element to Threat element)

# Threat Modeling Profile in the Model

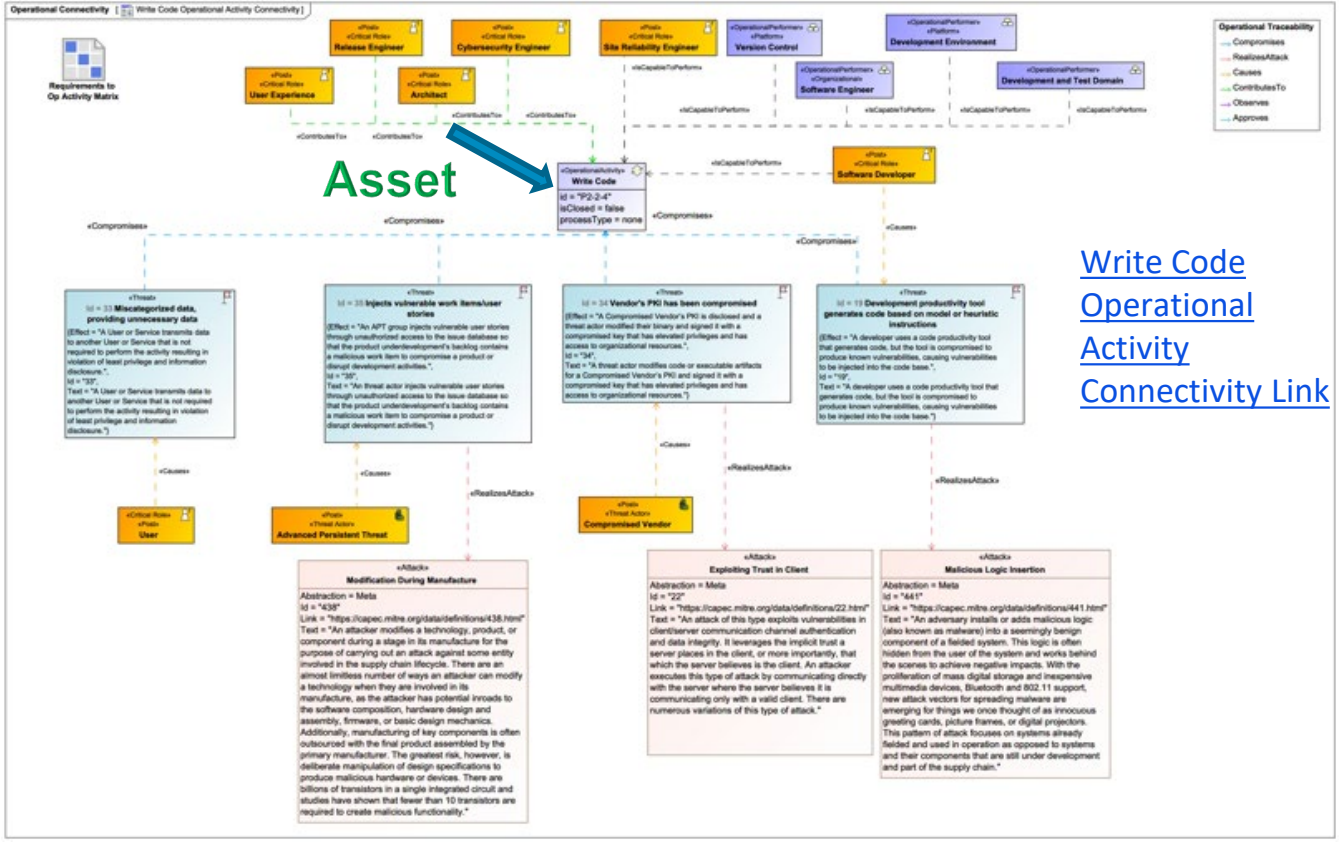


Threat Modeling Training

# Example

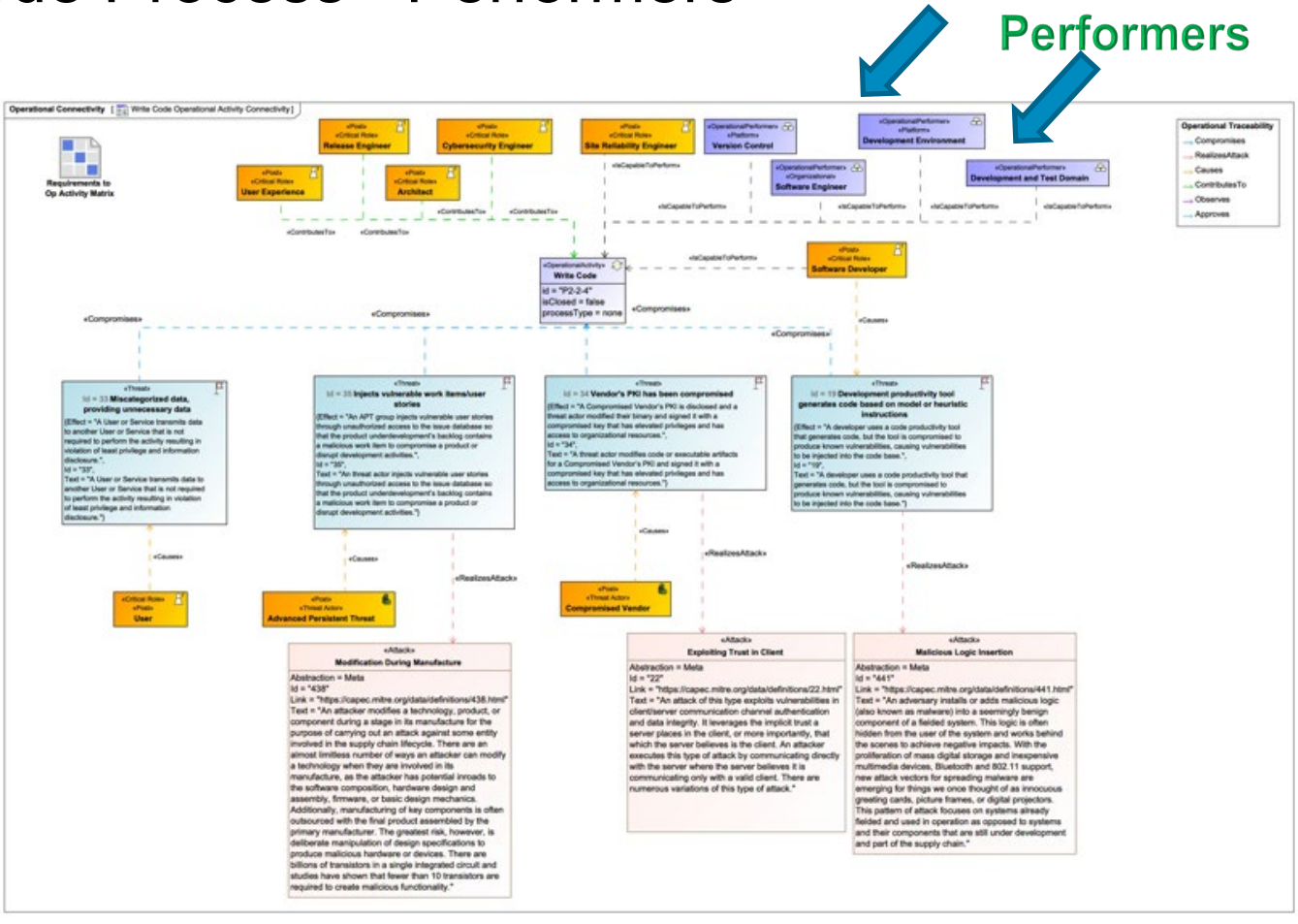
Carnegie Mellon University
Software Engineering Institute

# Write Code Process - Asset

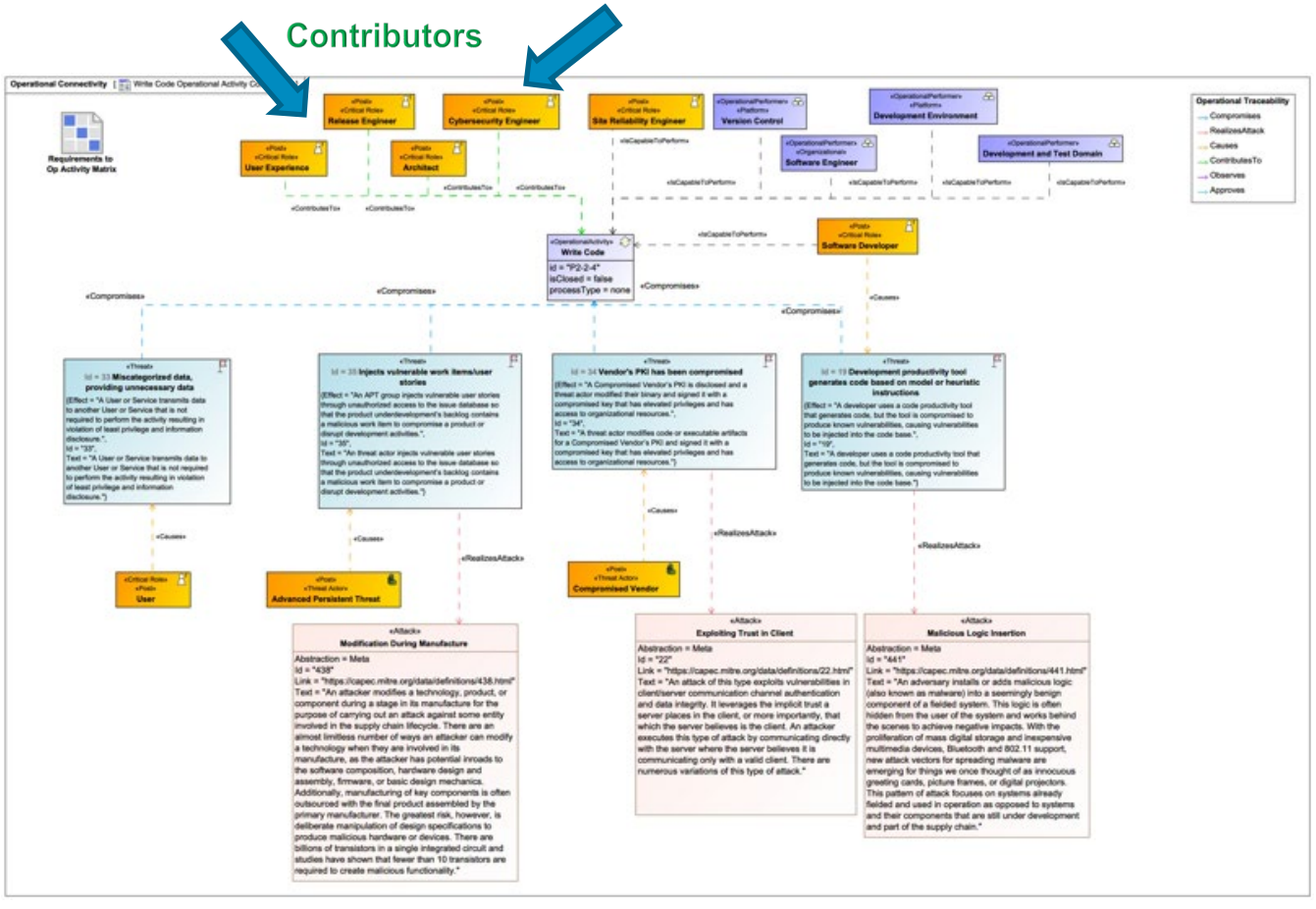



[Write Code Operational Activity Connectivity Link]

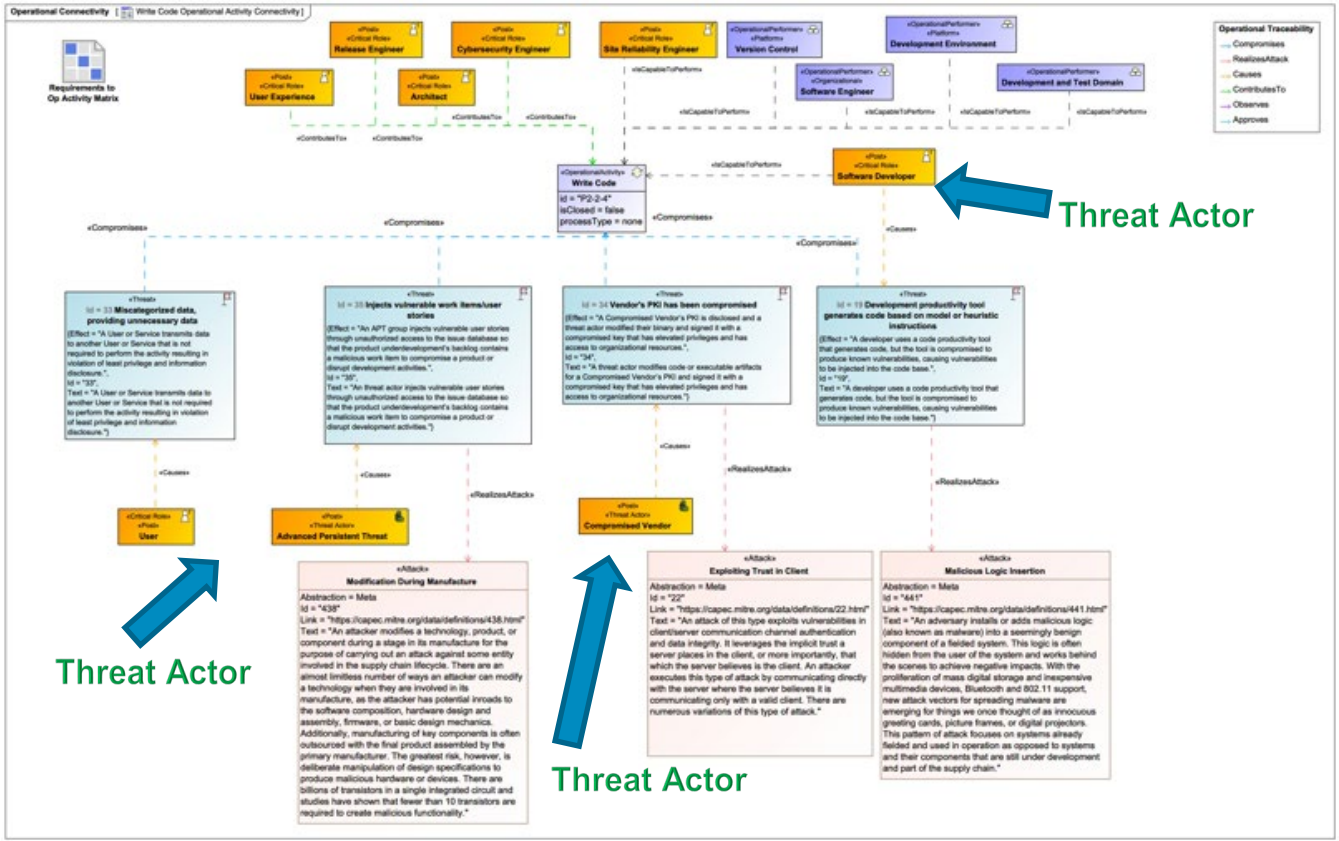
# Write Code Process - Performers



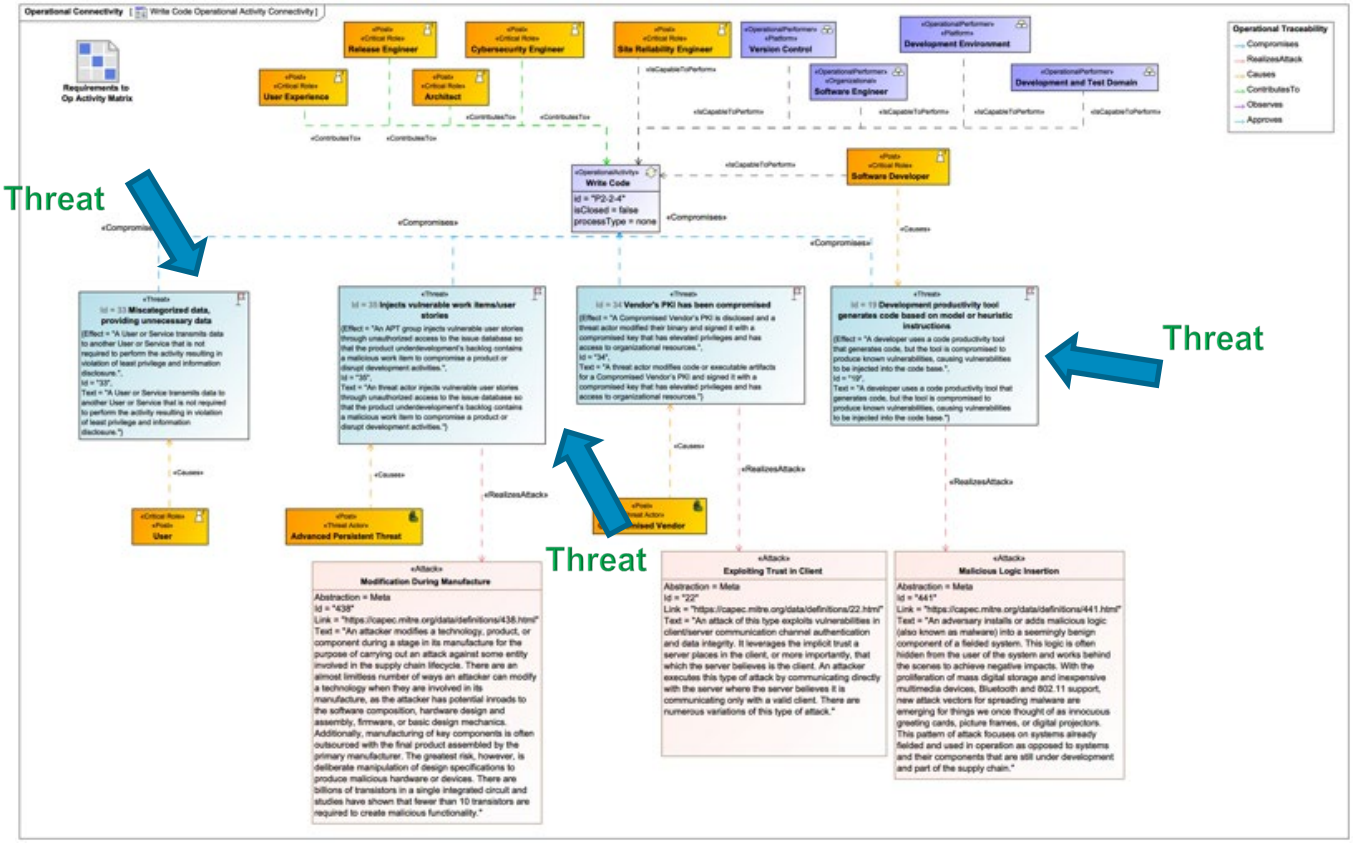
# Write Code Process - Contributors



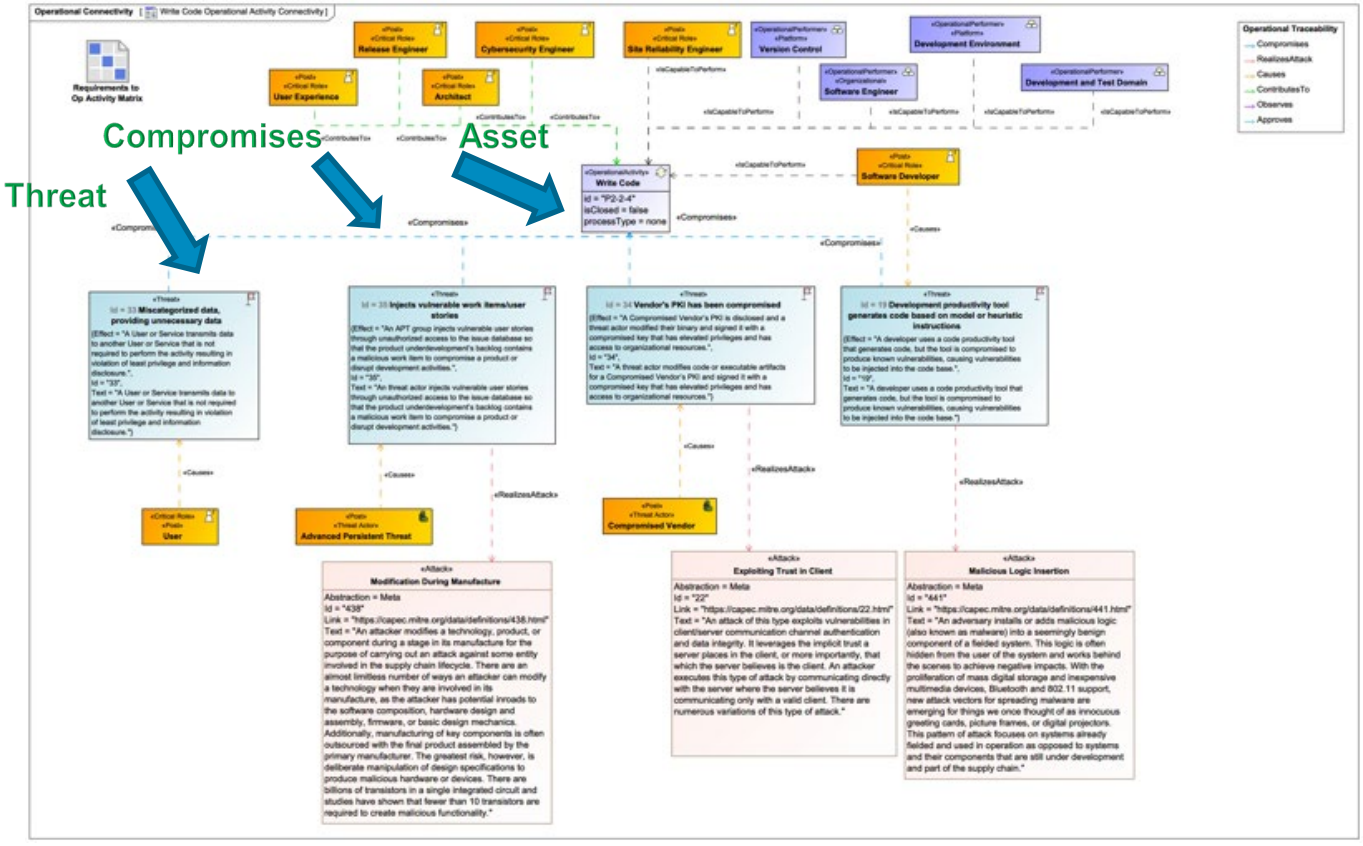
# Write Code Process – Threat Actors



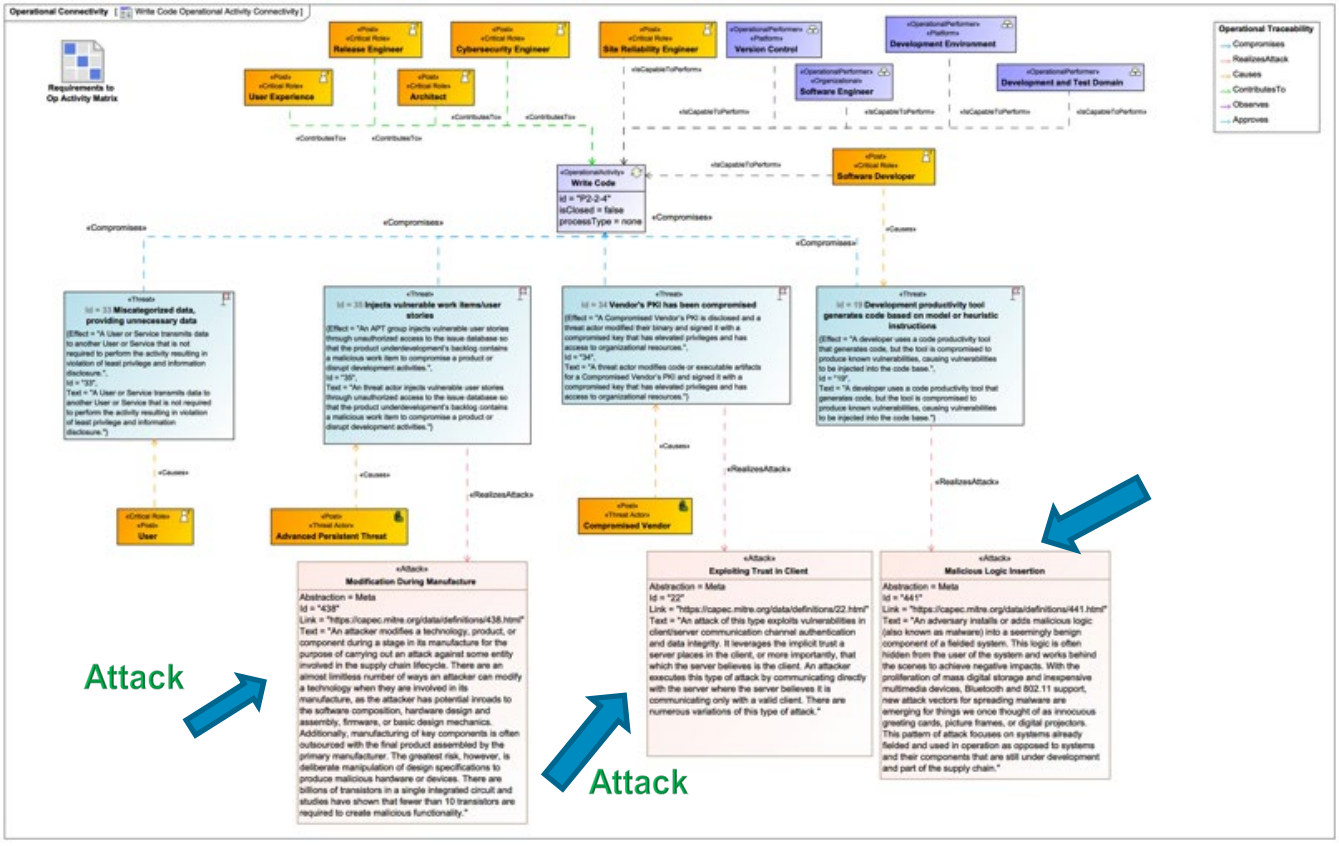
# Write Code Process - Threats



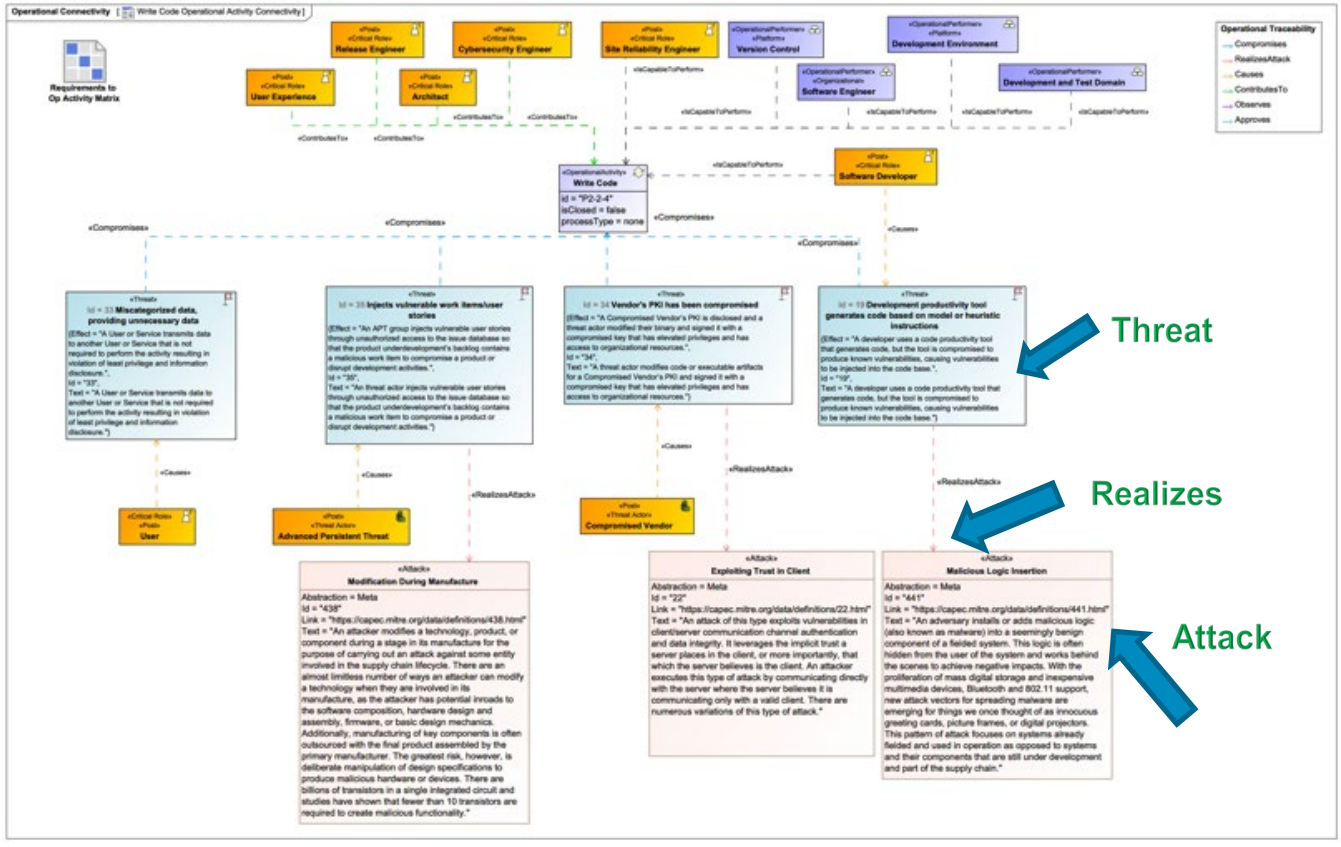
# “Threat Compromises Asset”



# Write Code Process - Attacks

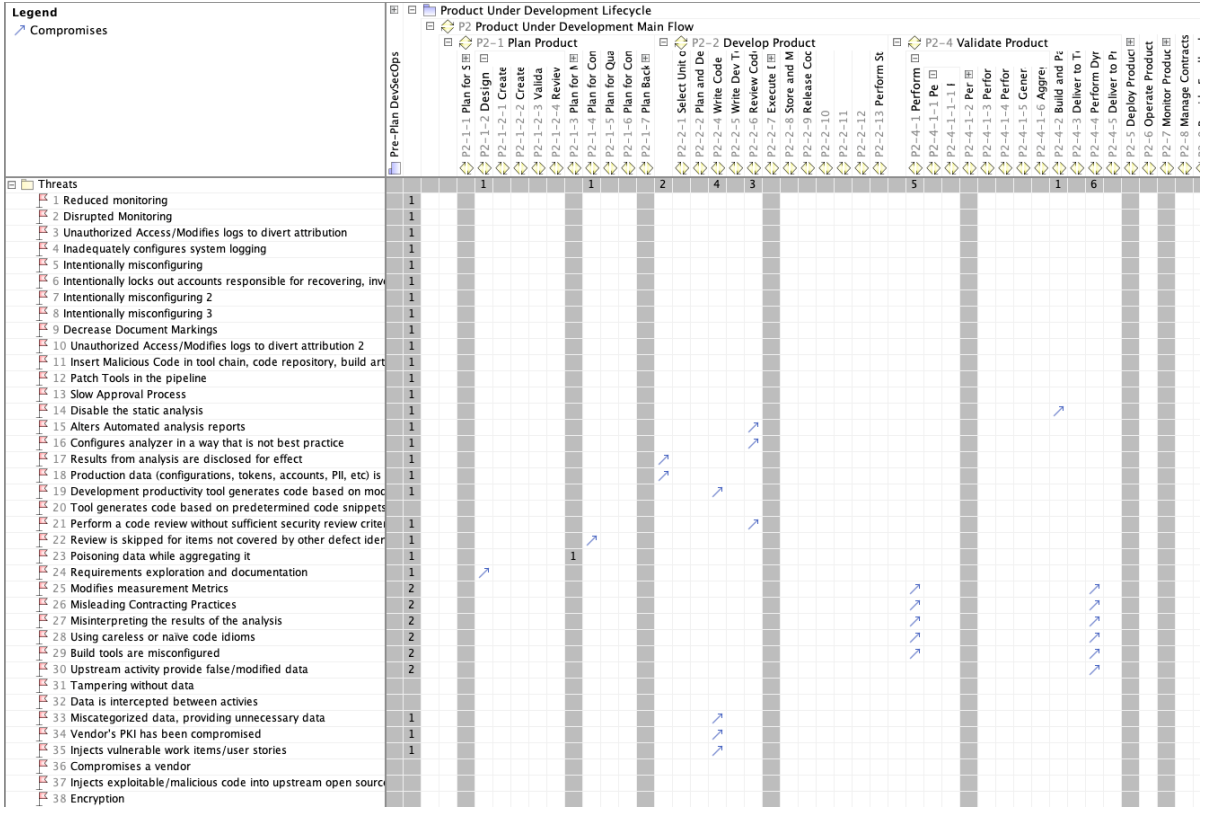


# “Threat Realizes Attack”



# Analysis

- Threats to Assets
  - Processes
  - Components
- Threats to Attack Methods
- Threats to Threat Actors



# Contact Information



https://www.sei.cmu.edu

**Nataliya Shevchenko**
Senior Member of the Technical Staff
CERT Division - Applied Systems
CMU-Software Engineering Institute
san@sei.cmu.edu