Threat Modeling Discussion

Jonathan Marcil

SAMM User Day

June 26, 2024 - Lisbon, Portugal

What is Threat Modeling?

- Business function: Design
- Security Practice: Threat Assessment
- Stream B: Threat Modeling

Threat modeling is a structured activity for identifying, evaluating, and managing system threats, architectural design flaws, and recommended security mitigations

Threat Modeling Philosophical Supplement

Have you ever asked yourself if the core **values and principles** reflected in your activities are aligned with that has been observed elsewhere to get good results?

threatmodelingmanifesto.org

Manifesto - What is Threat Modeling?

Threat modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics.

At the highest levels, when we threat model, we ask four key questions:

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good enough job?

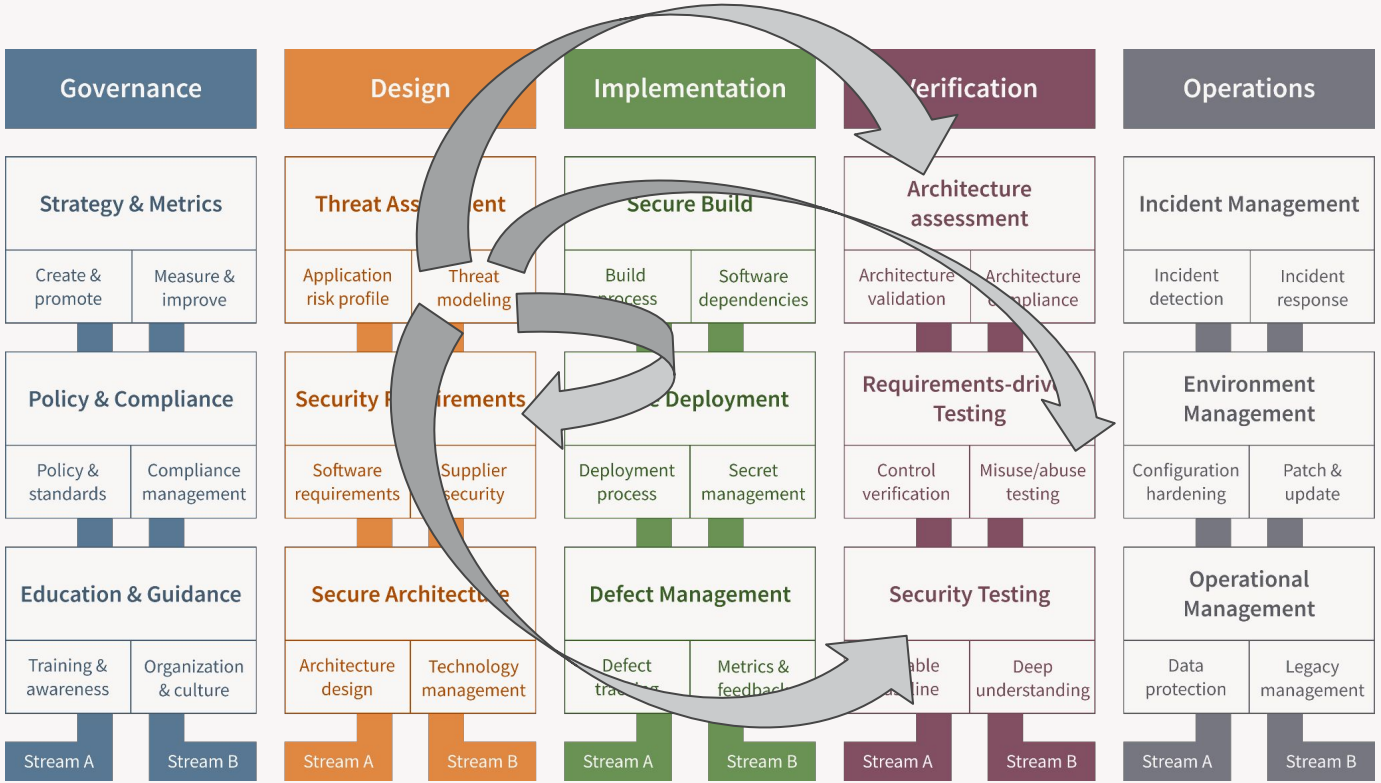
Objectives of this session

- Think about how a single security practice impacts others
  - One practice can be the “proxy” to many others for the end users of your security program
- Share and learn from others based on real examples
  - Both successes and failures are valuable for learning
  - See how different maturity levels implement threat modelings, and infer what works best for a given level

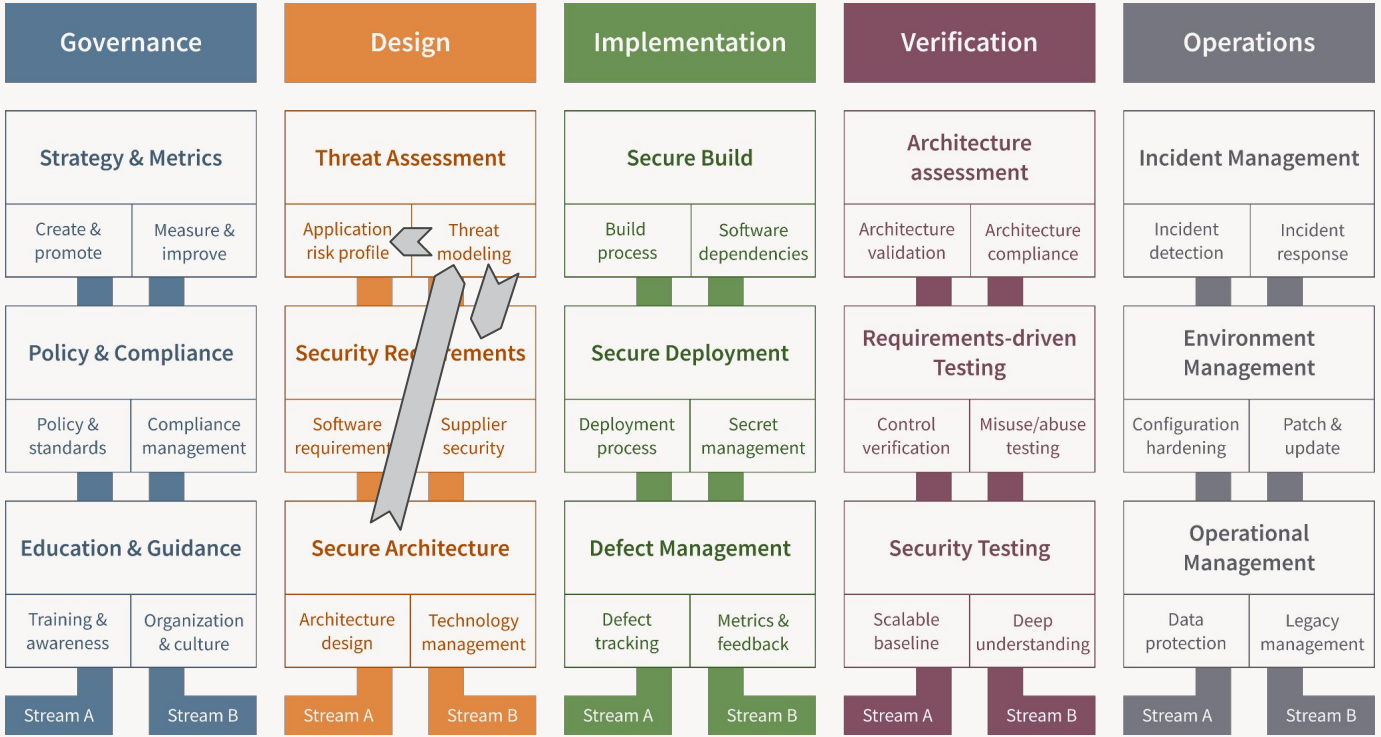
Quick overview

Threat Modeling relationship to the rest of OWASP SAMM

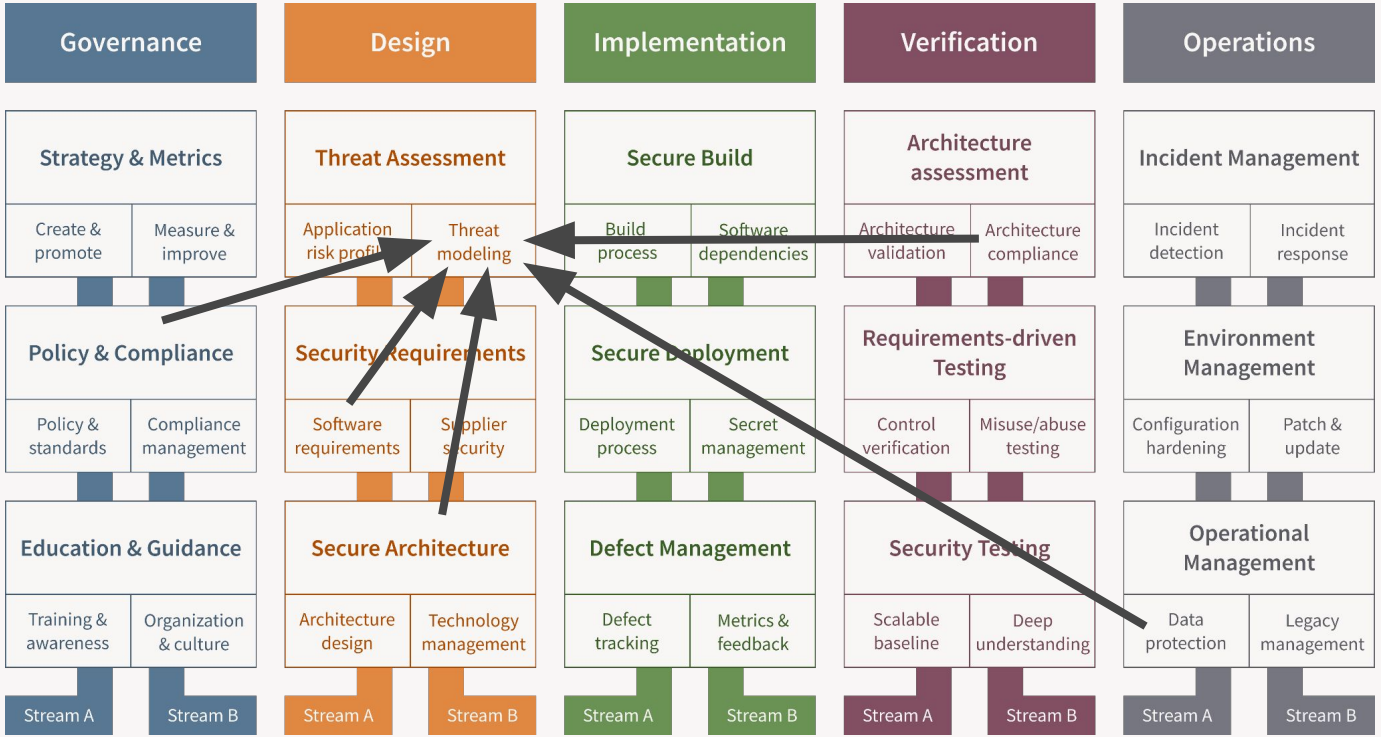
Threat Modeling outputs



Threat Modeling adjacent dynamics



Threat Modeling ingest / leverage



TM and the rest of SAMM

What are your examples of relationships between security practices?

Next

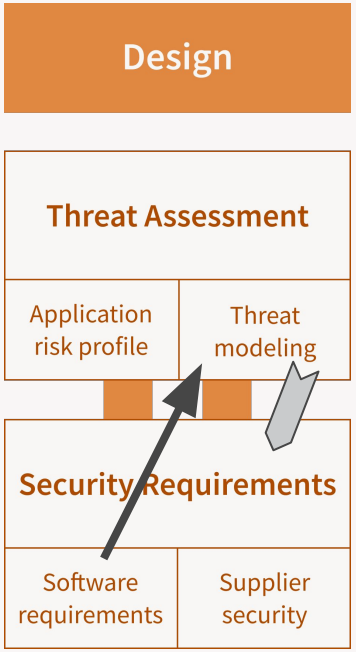
Jonathan's example bank

Threat Modeling informs Risk Profile

- At first you create a risk profile in order to prioritize what you should threat model first
- While performing threat modeling, you notice that for one system, collected information was incorrect
- After doing many systems, you notice that your risk profile formula doesn't reflect the situation of the system

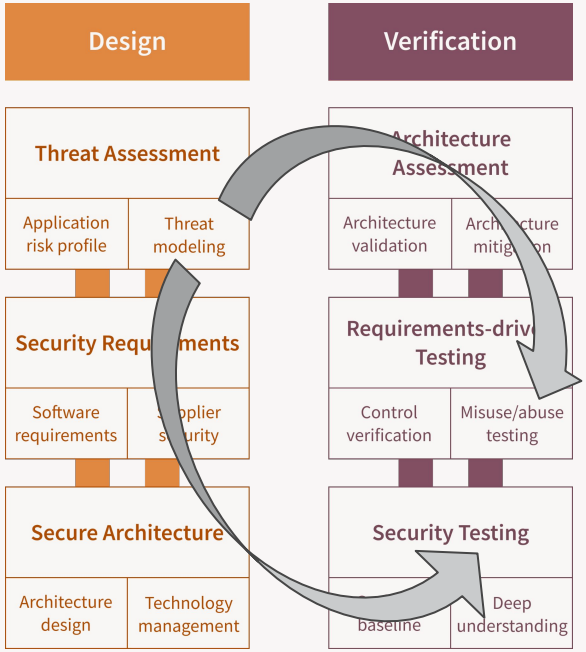
Threat Modeling <> Security Requirements

- Security requirements are written and available somewhere but not consulted
- Threat modeling becomes an enforcement step for requirements, as you can map a threat, design flaw or mitigation to a given security requirement; synergy!
- Findings during threat modeling could help refine existing requirements or create new ones



Threat Modeling <> Verification

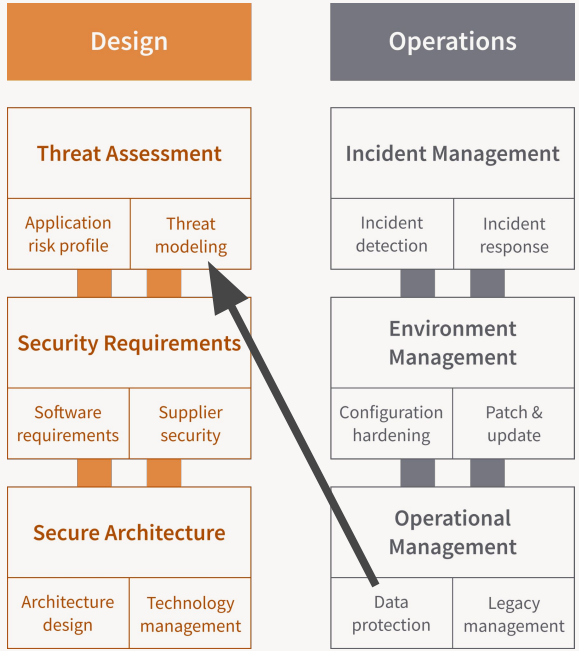
- Threat Modeling findings are implemented as a test case to ensure completion and prevent future mistakes
- Threat Modeling artifacts are being reused, not for their usual outputs, but as a security oriented view to guide pentesting that facilitated a deeper understanding of the system context



Threat Modeling Dataflows == Data Elements

- Threat Modeling is performed at a good time to prepare, populate and validate your data catalog by having a common touchpoint

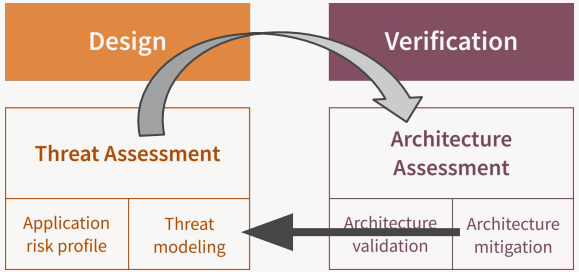
- Dataflow diagrams enables visualisation of data element moving between systems
- Threat Model can collect and show data storage details intention before operations
- Enforce data protection policy at the design phase



Threat Modeling <> Architecture Assessment

- Simply do them at the same time!
  - Architecture Mitigation QC L2: You systematically review each threat identified in the Threat Assessment
- Back and forth process costs more

- Most organizations don’t have a difference between an architecture reference and one implementation of a given system
- The architecture is often the infrastructure as code + the software code



if time..

Bonus!

Threat Modeling Success

What approach clearly provided value and success for your security posture?

Make it part of the official tasks for developers

Perform training alongside a real threat modeling session

Work together* into productive dialogues to share knowledge and experiences

* no ball tossing

Recognize in your program the value added proposition of the relationships between security practices

Learn from past mistakes, but don’t turn something more urgent into threat modeling

Thanks!

Slides and links on:

about.jonathanmarcil.ca →

Special thanks to:

Seba

Threat Modeling Manifesto Group

OWASP
Open Web Application
Security Project

OWASP
SAMM

Thank you!

owaspsamm.org