

# Threat Modeling Capabilities

**Organizational Planning for efficient  
developers involvement**

**by Jonathan Marcil**

**ConFoo 2024**



**THREAT  
MODELING  
CAPABILITIES**

# Content overview

- Introduction
- What's Threat Modeling?
- Capabilities definition and areas
- What matters for developers?
- Sample Capabilities
  - Small, Medium & Large scale



# Introduction to the team

- **Threat Modeling Manifesto, 2020**
- **15 people with diverse backgrounds**
  - industry professionals
  - academics
  - authors
  - hands-on experts
  - trainers
- **Released a catalog of capabilities in 2024**
  - Lots and lots of brainstorming and editing
  - Friendly group consensus
  - Base content for this presentation

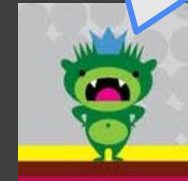


# Threat Modeling

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

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

**Shostack's  
Four  
Question  
Framework**



**THREAT  
MODELING  
CAPABILITIES**

# Threat Modeling Example

- **What are we working on?**
  - This presentation you're viewing right now
- **What can go wrong?**
  - Lack of clarity
  - Spelling mistakes
  - Busting allocated time
  - Spectators outrage due to wild ideas
- **What are we going to do about it?**
  - Peer reviews
  - Making some slides optional
  - Leaving time for questions and interaction
- **Did we do a good job?**
  - You tell me at the end of it 😊



THREAT  
MODELING  
CAPABILITIES

# Developers can use Threat Modeling

- **To review their architecture or design**
- **To find security and privacy issues**
- **To create security and privacy requirements**
- **To understand the security posture of their systems**
- **The learn and think about security**



**THREAT  
MODELING  
CAPABILITIES**

# Capability Definition

*A capability is something an organisation do or do not have*

- **measurable or provable**
- **actionable objective, identifies a goal**
- **more means better equipped your org is**



THREAT  
MODELING  
CAPABILITIES

# Capability Limits

*A capability is something you can do*

- **does not tell how to do it**
- **does not tell why you would do it**
- **is not maturity**
  - feel free to implement according to desired maturity level





# Threat Modeling Capabilities

*What your organization can do for threat modeling*

- **Lego pieces to help build a threat modeling program**
- **Single page Web document**
  - <https://www.threatmodelingmanifesto.org/capabilities/>
- **List capabilities with short description**



THREAT  
MODELING  
CAPABILITIES

# Capabilities Areas

- **Strategy**
- **Education**
- **Creating Threat Models**
- **Acting on Threat Models**
- **Communications**
- **Measurement**
- **Program Management**

# For Developers

- **Capabilities empower them to threat model**
  - Each capability should help them do better threat models
  - The organization supports them in that work
- **Better organization reduce toil**
  - Management leads effective results



# Questions?

- Threat Modeling?
- Capabilities?
- Where can I get more coffee?

# 38 Threat Modeling Capabilities

- **Strategy**
  - Execution Governance
  - Life Cycle Integration
  - Resource Allocation
- **Education**
  - Training Assignment
  - Adaptive Learning
  - Active Practice
  - Execution Support
  - Convention Alignment
  - Continuing Education
- **Creating Threat Models**
  - Experience Availability
  - Fostering Participation
  - Shared Responsibility
  - Active Collaboration
  - Portfolio Prioritization
  - System and Threat Comprehension
  - Pattern Cataloging
  - Format Consistency
  - Continuous Changes
  - Change Control
  - Threat Model Distribution
  - Tool Assisted Process
- **Acting on Threat Models**
  - Definition of Done
  - Seamless Alignment
  - Baseline Improvement
  - Risk Management
- **Communications**
  - Positive Reinforcement
  - People-Skills Development
  - Feedback Collection
  - Constructive Conversations
  - Listen To Diverse Viewpoints
- **Measurement**
  - Value Assessment
  - Status Tracking
  - Quantified Risk Management
- **Program Management**
  - Value-Driven Management
  - Simple Changes
  - Methodological Openness
  - Metrics-Driven Management
  - Collaborative Program Development



# 38 Threat Modeling Capabilities

- Can you recall 7 of them?

**30**

**Just kidding!**



# Organization profiles

- **Don't implement the 38 capabilities right away!**
- **Selection depends on org size and needs**

**We'll have key  
takeaways for  
each concept!**

- **Next slides: small/medium/large orgs**
  - **Lots of content ahead**
  - **Non exclusive to size**
    - Larger orgs still needs smaller org capability



# Organization profile: small

- 6.5 developers
- Minimal risk
- Looking to get started in Threat Modeling



# Organization profile: small

- **Strategy / Resource Allocation**
  - Teams commit the appropriate amount of time, people, and money to perform threat modeling.

**Make it part of  
the official tasks!**



# Organization profile: small

- **Education / Active Practice**

- Practitioners use experiential learning to develop threat modeling skills by performing hands-on threat modeling.
  - Learning through direct experience and observation, rather than just reading or listening about a topic.

**Get something  
out now!  
You'll reiterate  
and learn  
more later!**

**there's no  
such thing as a  
bad threat  
model**



# Organization profile: small

- **Creating / System and Threat Comprehension**
  - Analysis, as part of the creation process, is informed by ingesting system architecture. Conclusions are enriched by utilizing outside threat knowledge.

**Know about your  
own systems and  
find inspirations  
for threats!**



# FAQ: Inspiration for threats

- Threat Modeling Methodology
  - STRIDE for security
  - LINDDUN for privacy
- Threat Enumerations
  - CAPEC
- Anything
  - OWASP Top 10
  - Random internet posts
  - Latest news about security

# Organization profile: small

- **Acting / Seamless Alignment**
  - Threat modeling outcomes influence the implementation or operational workflows. For example, guiding testing in the SDLC.

**Make sure your threat models change designs when needed!**



# Organization profile: small

- **Communications / Positive Reinforcement**
  - Value propositions based on threat modeling outcomes are communicated to leadership, stakeholders, and participants. The organization celebrates successes in threat modeling and learns from failures.

**Recognize and  
talk about the  
value of threat  
modeling  
results!**



# Organization profile: small

- **Program Management / Value-Driven**
  - The threat modeling program is managed, structured, and defined at an organizational level and provides recognizable value.

**Value, value, value!**

**Keep doing things  
that provide value!**





# FAQ: Value examples

- Changes in design or code
- Learning about new threats
- Evaluate current security posture
- Knowledge is shared between people
  - System X does Y
  - Component A is critical
  - Missing security controls

# Organization profile: medium

- 50 developers
- Medium risk, will grow in the future
- Looking to standardize Threat Modeling
- Threat Modeling skills needs to be solidified



# Organization profile: medium

- **Strategy / Life Cycle Integration**

- Threat modeling is incorporated into organizational processes such as the development life cycle or an SDLC and is a prerequisite for critical life cycle phases.

**Formalize when  
threat models  
are done!**

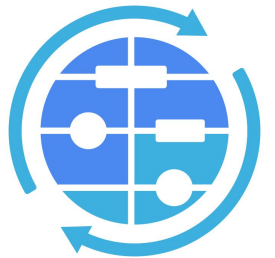


# Organization profile: medium

- **Education / Execution Support**

- A support structure is in place to strengthen the performance of threat modeling.
- Developers are encouraged to learn about security and privacy concepts.

**Give knowledge  
assistance to  
threat model  
practitioners!**



# Organization profile: medium

- **Creating / Portfolio Prioritization**

- Organizations evaluate all of their in-scope systems to decide in which order to execute threat modeling.

**Make sure you  
threat model  
everything that  
needs to be!**



# Organization profile: medium

- **Measurement / Value Assessment**

- Return on investment compares the effort put into threat modeling against its effectiveness.
- This valuation can be used to show improvement and consider changes before you move forward.

**Value, value...**

**Have metrics on  
flaws found and  
changes done!**

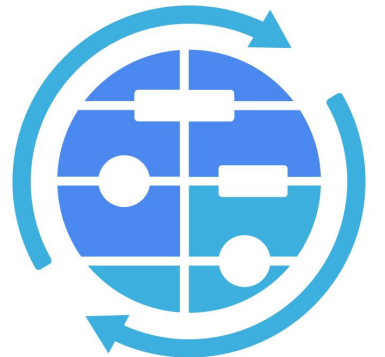


# Quick pause

- Take a breath of air
- Take a sip of water
- Any question?

# Organization profile: large

- 1000+ developers
- Medium risk with most projects
- Some projects are high risk
- Looking to make Threat Modeling sustainable



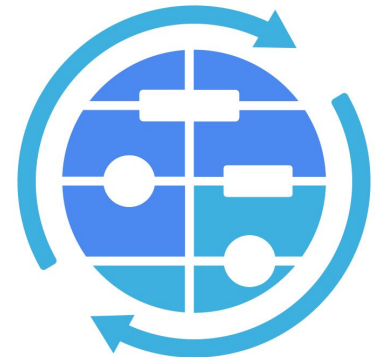


# Organization profile: large

- **Strategy / Execution Governance**

- Documentation exists requiring or mandating that threat modeling occur. Actions are taken by leadership to encourage threat modeling. Goals are set to ensure proper analysis of threat models.

**Set goals that says  
“Threat Modeling  
must be done”**

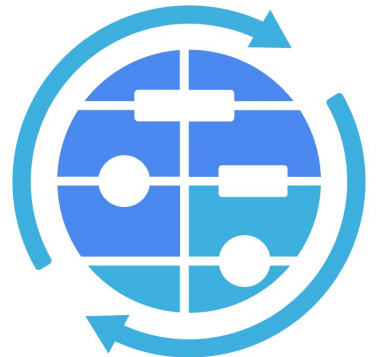


# Organization profile: large

- **Education / Training Assignment**

- Threat modeling training is part of the organization's curriculum. Stakeholders assign resources so that everyone in their organization can learn.

**Create corporate training based on what practitioners needed in the past!**

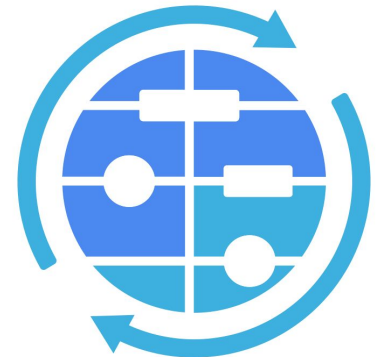


# Organization profile: large

- **Creating / Format Consistency**

- The organization promotes uniformity of threat models. Predefined templates of threat models can be used to ensure completeness.

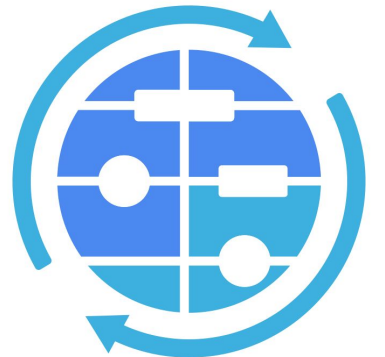
**Different teams  
should produce  
similar threat  
models!**




# Organization profile: large

- **Measurement / Status Tracking**
  - Dashboards and metrics are used to show the impact of outcomes and invite feedback.
  - These metrics may indicate either progress or regression.

**Create  
dashboards that  
are aligned with  
value-related  
metrics!**



# That's it for the examples!

- Questions
  - Discussions
  - But one more thing...
- 

# Maturity Gotcha

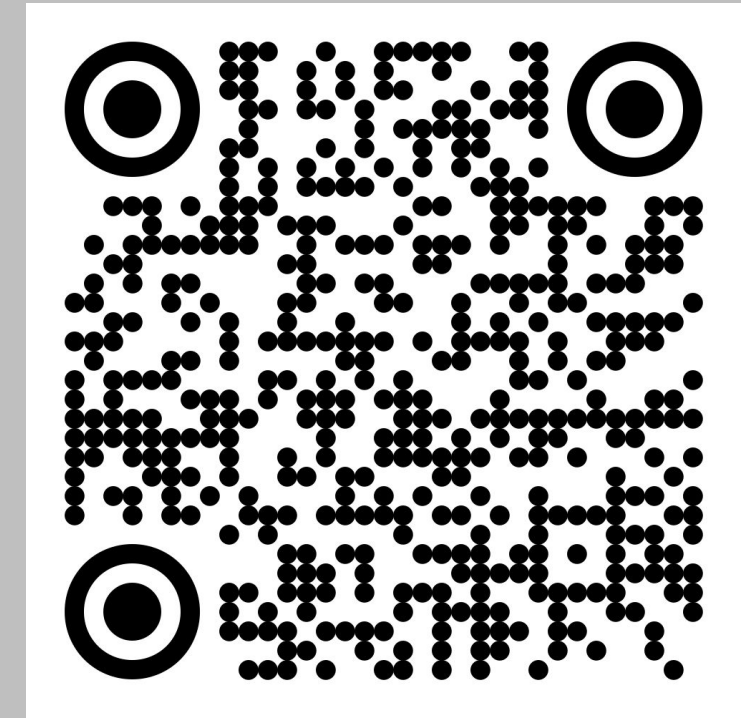
- All previous capabilities could be done regardless of organization sizes
- For example, in Training Assignment, you can refine the level of training given to people as the organization grows
- Each capability can be done differently at its own maturity level



# Thanks!

*Slides and links on:*

<https://about.jonathanmarcil.ca>



<https://www.threatmodelingmanifesto.org/capabilities/>

*Special thanks to:*

The Threat Modeling Group  
Yann (ConFoo 2024)

ConFoo.CA



THREAT  
MODELING  
CAPABILITIES

**JONATHAN MARCIL**  
INTERNATIONAL