COLLABORATIVE THREAT MODELING

Getting out of your Bubble

By Avi Douglen

Bounce
SECURITY

BLUF:

Threat modeling is not JUST technical

Intentionally leverage social techniques

Maximize stakeholders’ participation

I am… **Avi Douglen**

Researcher / Consultant / Architect / Advisor

AviD@BounceSecurity.com

Socials: @sec_tigger

He / Him

Product Security Consulting Bounce SECURITY

- OWASP Israel Leader
- Global Board of Directors
- Privacy Reference Project Leader
- Moderator Security.StackExchange
- Co-Author, TM Manifesto

Answer These Key Questions

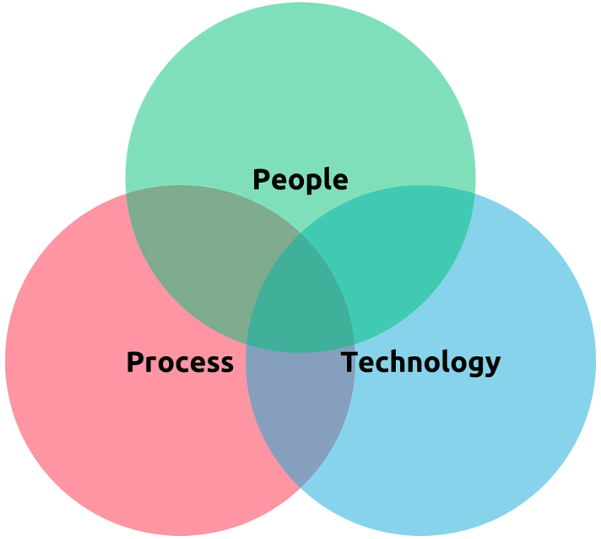
(aka Adam’s Framework)

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good (enough) job?

Threat Modeling Best Practices

<u>People and collaboration</u>

over processes, methodologies, and tools.



- Threat Modeling Manifesto

Threat Modeling Patterns

Varied Viewpoints

*Assemble a **diverse** team with appropriate subject matter **experts** and cross-functional **collaboration.***

- Threat Modeling Manifesto

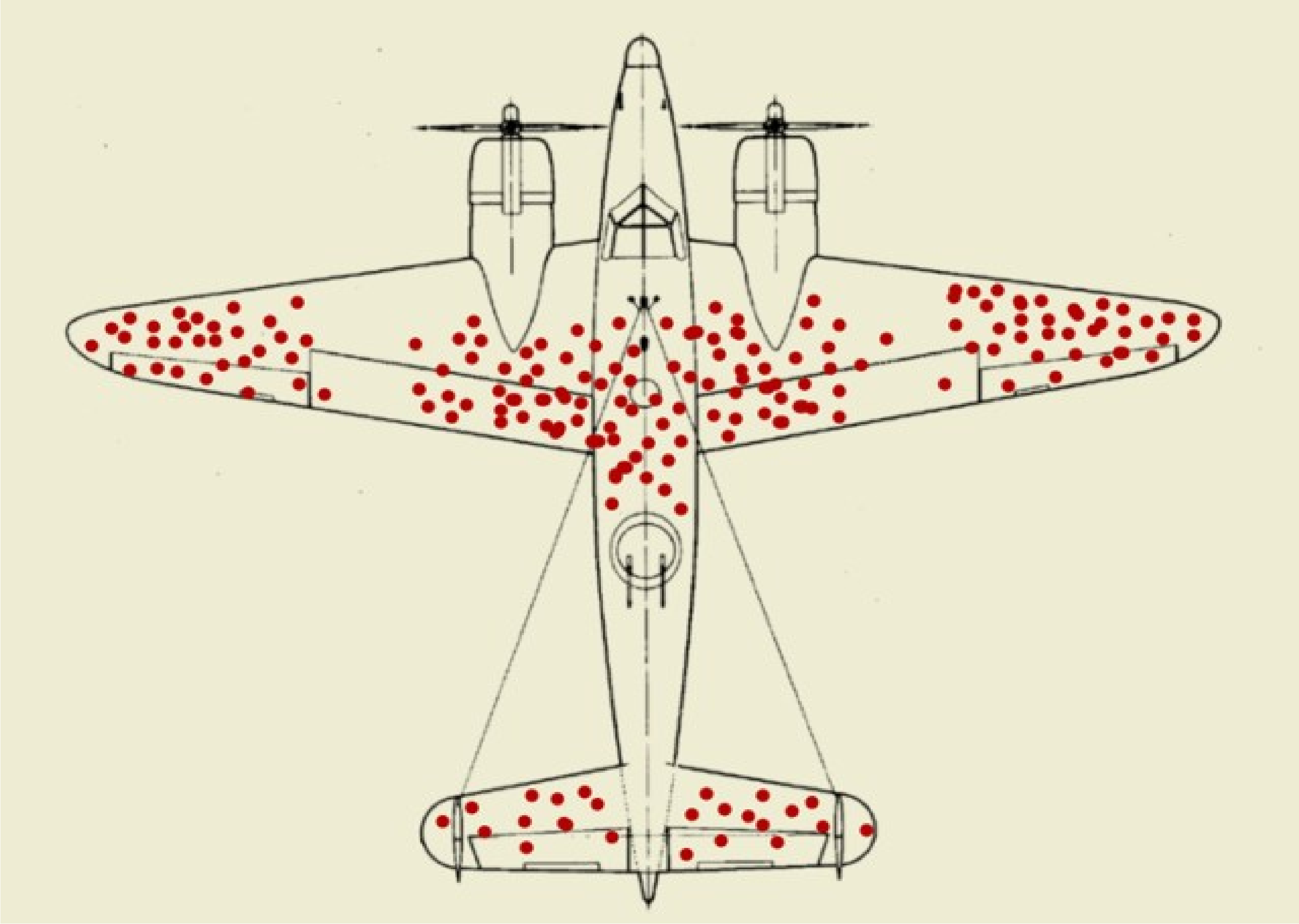
Topics

- What is Threat Modeling
- What Can Go Wrong – With Threat Modelers
- What Are We Going To Do About It – Together
- Can We Do A Better Job
- What Else Can We Do

What is Threat Modeling?

Analyzing representations of a system to highlight concerns about security and privacy characteristics

- Threat Modeling Manifesto



Bounce SECURITY

What is Threat Modeling?

- Structured security-based analysis
- Framework to understand security issues
- Review of Design Elements
- Prioritize Mitigations by Risk

STRIDE Per-Element

Spoofing → *Identity*

Tampering → *Integrity*

Repudiation → *Provability*

Information Disclosure → *Confidentiality*

Denial of Service → *Availability*

Elevation of Privileges → *Authority*

What Can Go Wrong
With Threat Modelers

aka Social Challenges

Bounce SECURITY

“Threats”: Social Challenges

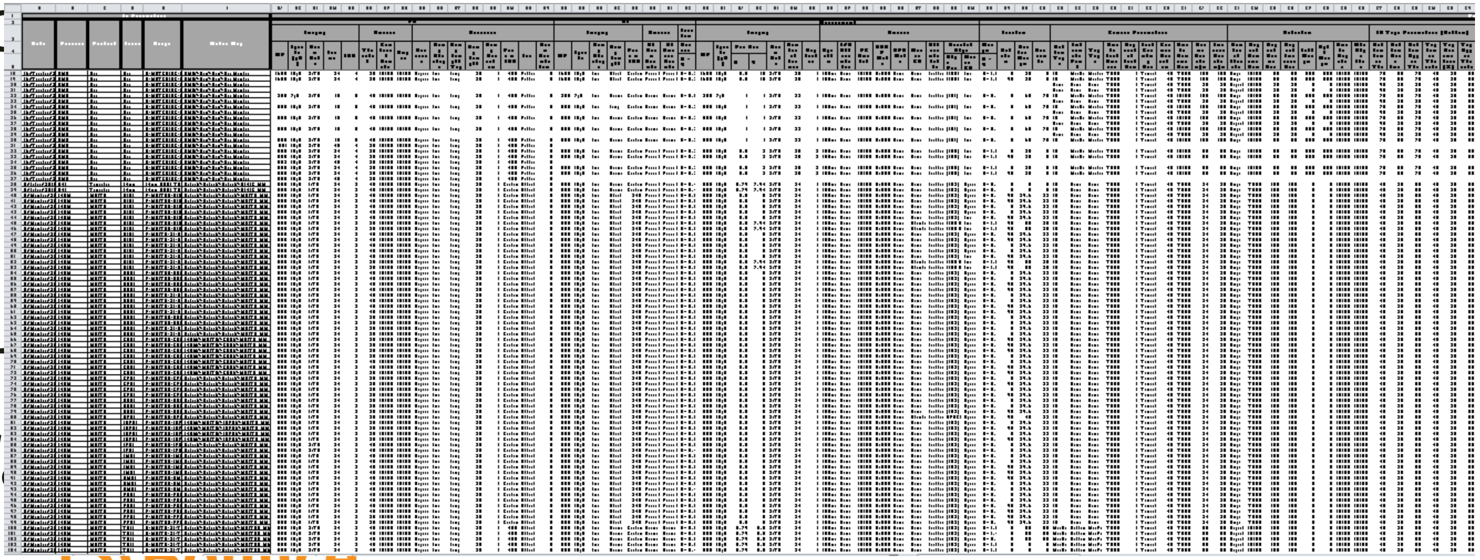
- Unusable output
- Siloed information
- Misaligned interests
- Implicit assumptions
- Passive participation
- Bullying and dominating

Impact: Missed Opportunities

- Lost Creativity
- Lack of shared understanding
- Low team awareness and insecure thinking
- Missing buy-in at all levels
- One time vs recurring investment

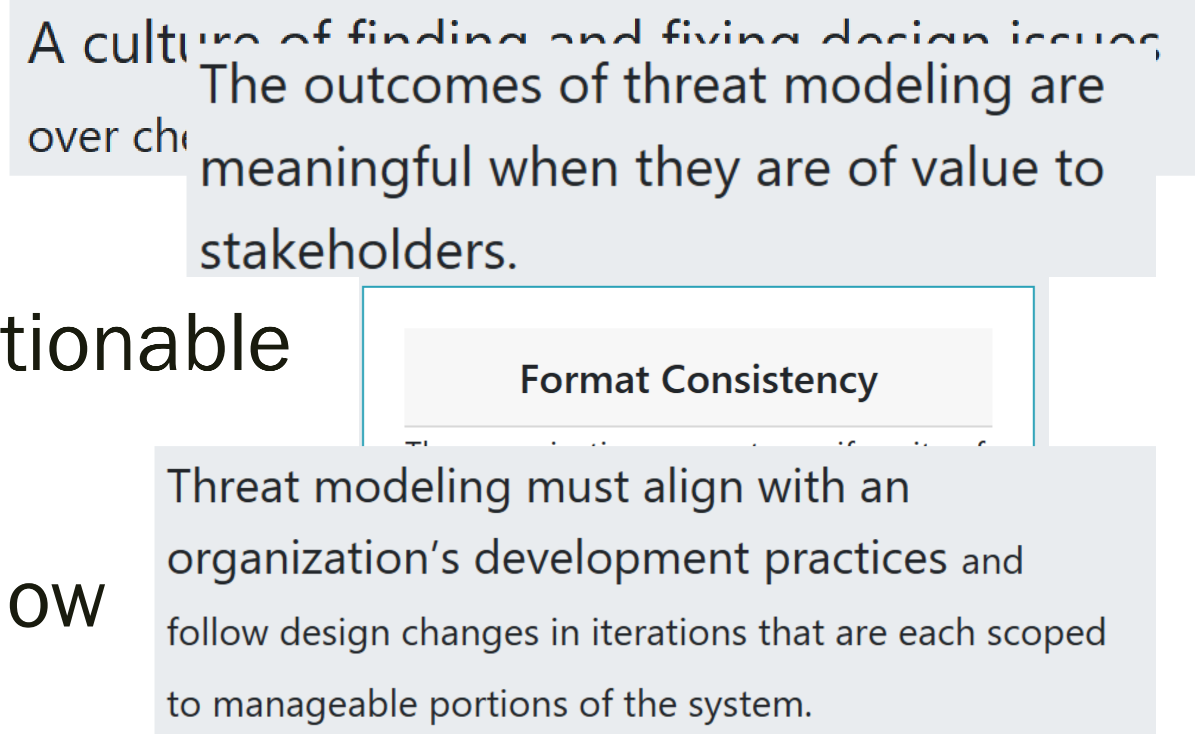
Threat: Unusable Output

- Great Big Threat Model in the Sky
  - *Dense report with hundreds of pages*
  - *Or 3000 lines in spreadsheet…*
- Significant duplicatio
- Abstract “threats”
- Non-actionable data
- “Shelfware documen
  - *Checkbox compli*



Mitigation: Focus on Stakeholders

- Prioritize productive conversations
- Always put in context
- Align with business
- Documentation must be actionable
- Leverage templates
- Integrate results into workflow



A culture of finding and fixing design issues

over ch

The outcomes of threat modeling are meaningful when they are of value to stakeholders.

Format Consistency

Threat modeling must align with an organization’s development practices and follow design changes in iterations that are each scoped to manageable portions of the system.

Threat: Siloed Information

- Low trust, low communication
- Limited design focus
- Unclear component relations
- Missing details
- Territorialism

- “Architecture archeology”

Mitigation: Trust and Communication

- Clarify goals and align interests
- Start with focused walkthrough
- Emphasize ownership
- Individual interviews
- Trust builds slowly
- Prepare answer to “WIIFM?”
  - *“What’s in it for me?” ← Offer personal value*

Threat: Misaligned Interests

- Security is not a shared goal or responsibility
- Management does not prioritize security
- No allocated time to invest in security
- “Let me just mark this bug as done and go home”

Mitigation: Reduce Friction and WIIFM

- Get management buy-in
  - *And resources*
- Provide shortcuts to do the right thing
- Developer guardrails
- Bypass checkpoints for threat models
- WIIFM:
  - *“Threat modeling lets you avoid work”*
  - *(or at least, get done sooner)*

Threat: Implicit Assumptions

- Undocumented requirements
- Internalized bias
- Lack of detailed communication
- Teams don’t listen to other teams
- “Everyone knows that!”
  - *Nope, they don’t*

Mitigation: Asking Questions

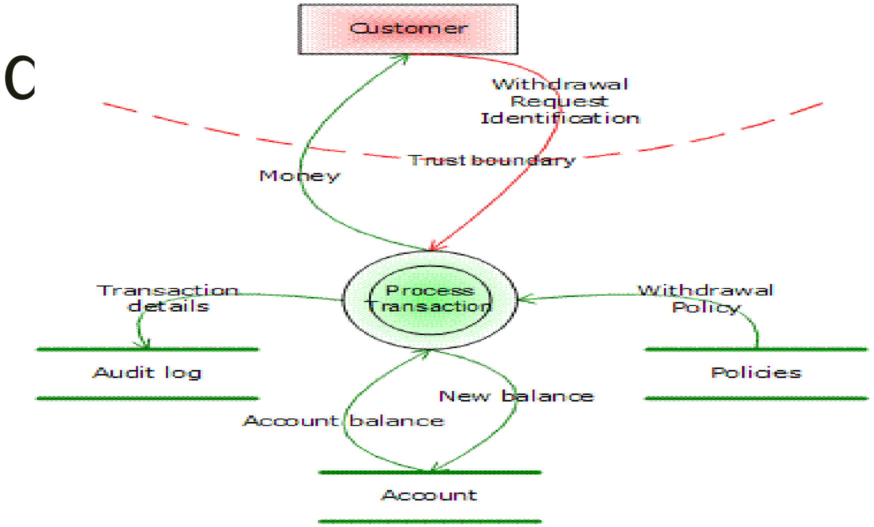
- Enable stakeholders to ask questions
  - *About the system / feature / diagram / threats / etc*
- Encourage questions
  - *Ego-free questioning*
- Demand questions and feedback
- “Assumptionless Diagramming”
- Keep asking:
  - *Until you have an answer or documented assumption*
  - *Then discover / validate / enforce / monitor*

Mitigation: Asking Questions

- Find assumptions using Socratic questioning
  - *Clarifying concepts*
  - *Probing assumptions*
  - *Requesting reasons and evidence*
  - *Alternate viewpoints and perspectives*
  - *Exploring implications and consequences*
  - *Questioning the question*

Mitigation: Invite Challenge

- Inviting Challenge is How We Learn
- Create mutually challenging and accepting culture
- Focus on learning and sharing knowledge
- Open ended questions vs “Redc
- Incomplete diagram



Threat: Passive Participation

- Crickets
- Minimal data
- Monosyllabic responses
- No active questions
- No volunteered information

Mitigation: Storytelling & Gamification

- Start by telling the story of the feature
- Invite participants to describe the next part
- Reward participation
- Ask directly by name
- Create rapport ahead of time
- Mind the local culture
- LISTEN and don’t retort negatively

Threat: Bullies and Dominators

- One loud one takes over the meeting
- “No need for others, I have all the information”
- Negative responses
- Escalating arguments and verbal violence
- Personal attacks
- Toxic culture

Mitigation: Print your resume

- Kidding!

Mitigation: Respectful Culture

- Respect everyone
- “The No A**hole Rule” (code of conduct)
- Model positive disagreements
- Stop escalation immediately
- Probe for root cause
- “Let’s take this offline”
- Mind the local culture

Summary of Social Techniques

- Focus on Stakeholders
- Trust and Communication
- Reduce Friction
- Ask Questions
- Invite Challenge
- Storytelling & Gamification
- Respectful Culture

Can We Do A Better Job

The Value Driven Approach

“All Threat Models are wrong,
some are useful”

- *George Box (kind of)*

Accept that it’s wrong,
focus on the usefulness

Bounce
SECURITY

Value Chain Analysis

- **Why** are we building this?
- **How** do we get the value from this?
- **What** do we do to ensure that happens?

Prioritize by Value Chain

- Focus on building the most useful controls
- Find the highest value
- What affects the revenue stream?

Security Expectations

"As a … I want … so that … WITHOUT … "

As a customer,
I want to complete an Order
so that a Product is added to my account
<u>WITHOUT my credit card being stolen</u>

Security Expectations

As a Customer with the “Social” addon,
I want to see all my friends in one place,
so that I can easily choose who to message
WITHOUT friends seeing each other OR changing my list

Sorry Points (aka Risk Categories)

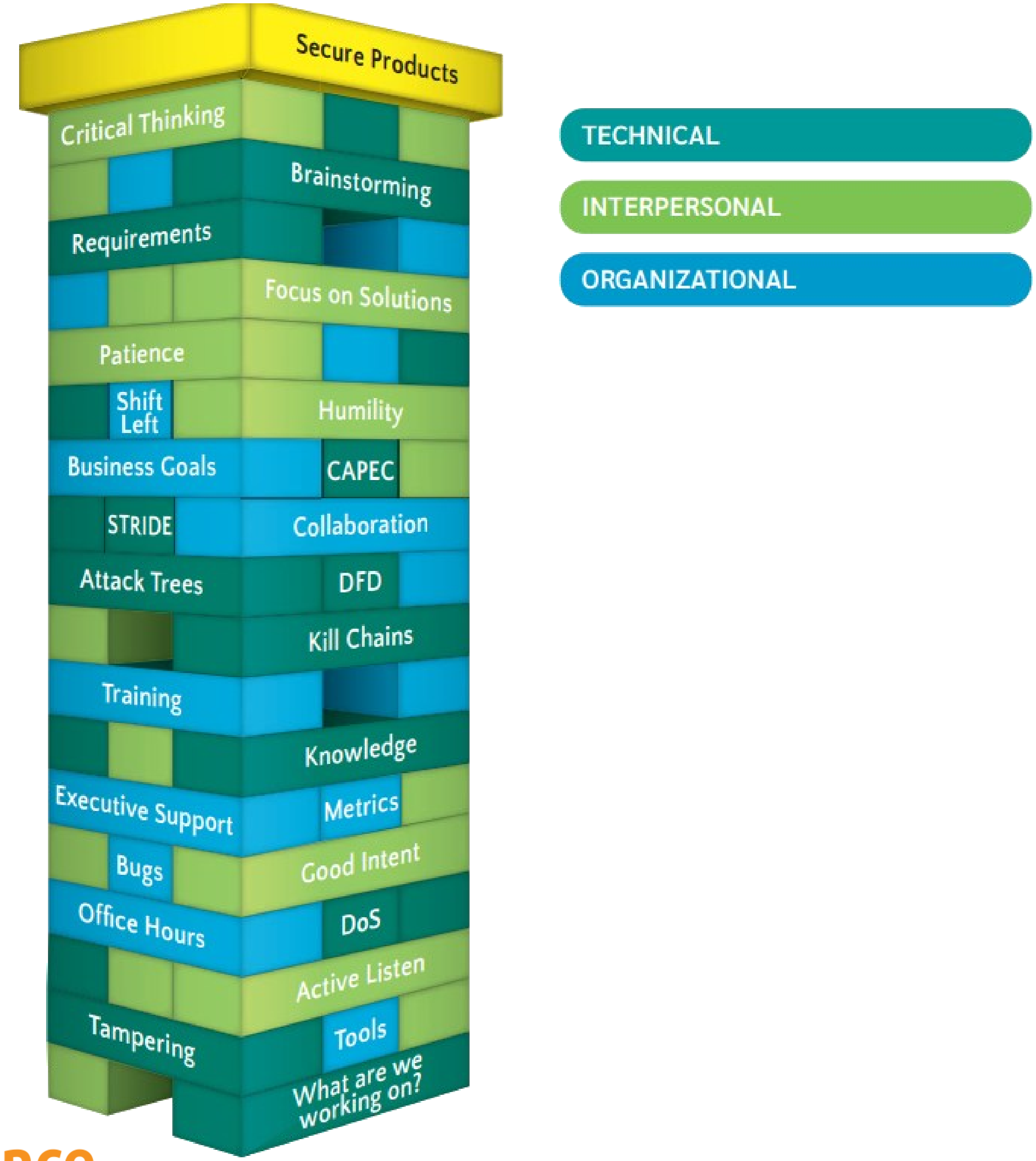
- Similar to Story Points
  - *Rough estimate relative to other stories*
- Measured in the same way
  - *Tshirt sizes, Fibonacci values, etc*
- “How sorry will you be if this breaks?”
  - *Value*
  - *Visibility*
  - *Side effects*

Sorry Points: Risk Context

- "T-Shirt" estimate
- Exposed externally / external users
- Cross-component or shared service
- All customers or limited subset
- Sensitive functionality
- Sensitive assets or PII
- High privileges
- Cloud or on-prem
- New technology / unusual complexity / other consideration

What Else Can We Do

Social Techniques



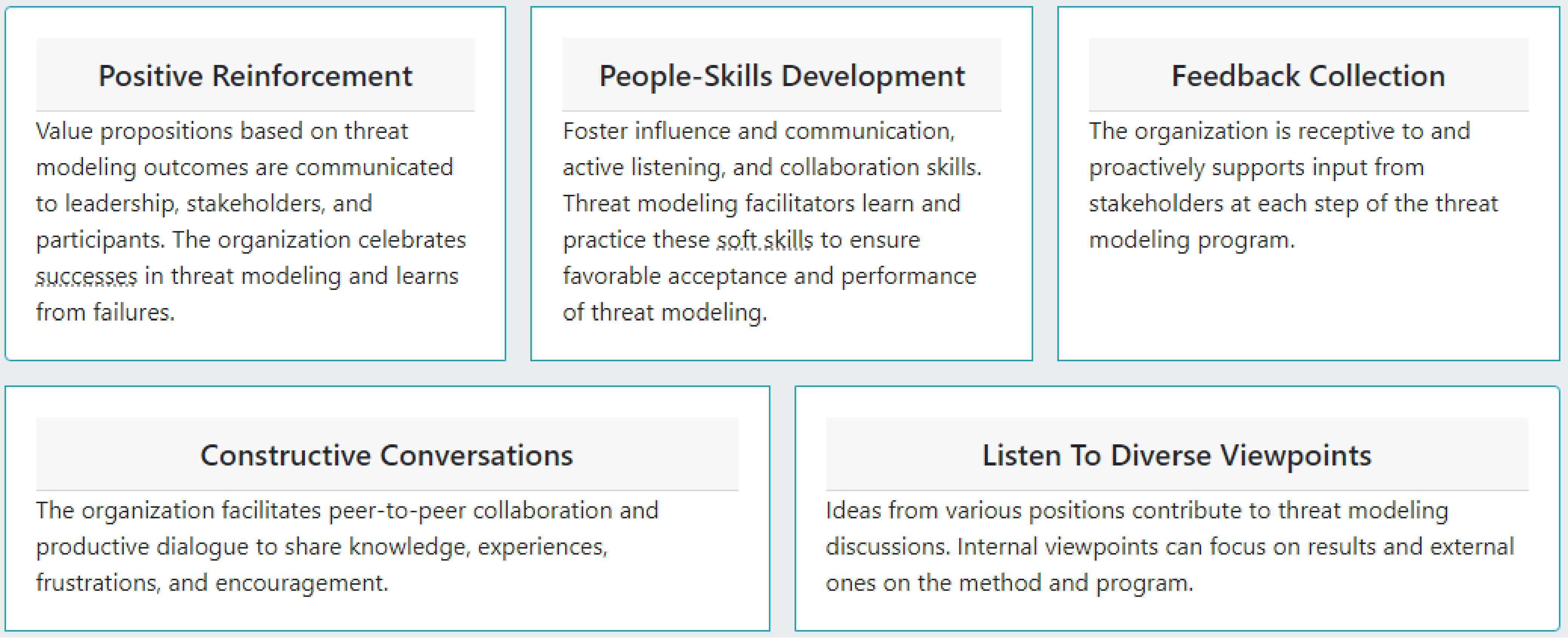
https://shostack.org/files/papers/The_Jenga_View_of_Threat_Modeling.pdf

- Critical thinking
- Knowledge of a repertoire of attacks
- General technical knowledge of the systems being used
- Understanding of software delivery models including DevOps, agile, Scrum and the local customizations to these models
- Teaching (especially around security)
- Agile approaches to work, including small incremental delivery, testing, and improvement.

- **Active listening**
- **Focus on solutions**
- **Patience**
- **Humility**
- **Respect**
- **Assumption of good intent**
- **Moderation and facilitation**
- **Understanding the working culture**
- **Working the organization**[2]
- **Developing a support network**
- **Commitments and predictability**

- **Clear goals**
- **Executive support**
- **Defined stakeholders and accountability**
- **Definitions, monitoring, and optimization**

Empowering Communication



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.

People-Skills Development

Foster influence and communication, active listening, and collaboration skills. Threat modeling facilitators learn and practice these soft skills to ensure favorable acceptance and performance of threat modeling.

Feedback Collection

The organization is receptive to and proactively supports input from stakeholders at each step of the threat modeling program.

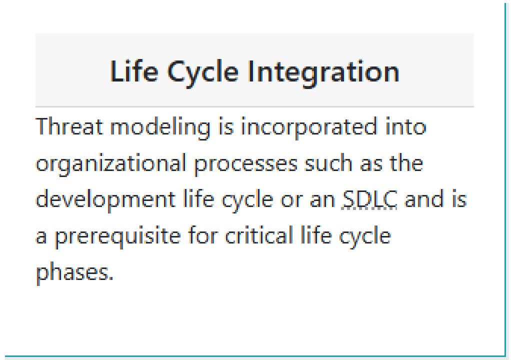
Constructive Conversations

The organization facilitates peer-to-peer collaboration and productive dialogue to share knowledge, experiences, frustrations, and encouragement.

Listen To Diverse Viewpoints

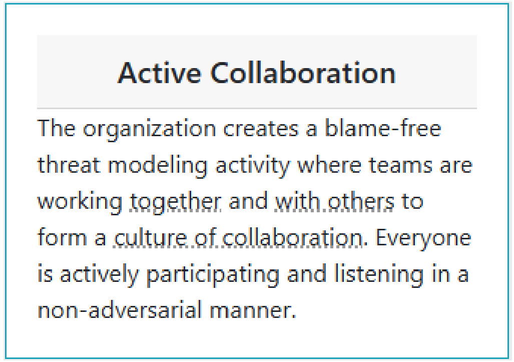
Ideas from various positions contribute to threat modeling discussions. Internal viewpoints can focus on results and external ones on the method and program.

Empowering Communication



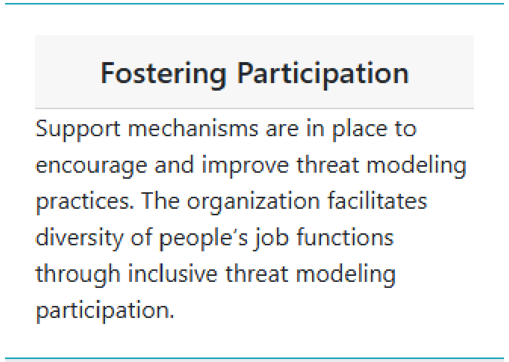
Life Cycle Integration

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.



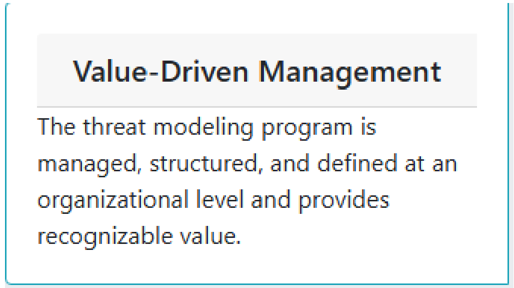
Active Collaboration

The organization creates a blame-free threat modeling activity where teams are working together and with others to form a culture of collaboration. Everyone is actively participating and listening in a non-adversarial manner.



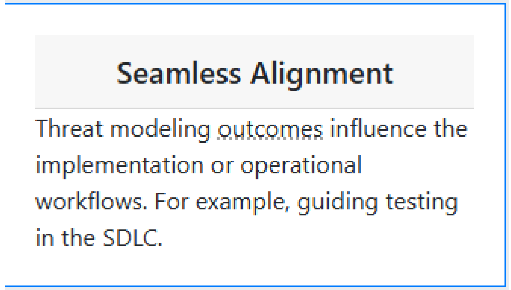
Fostering Participation

Support mechanisms are in place to encourage and improve threat modeling practices. The organization facilitates diversity of people's job functions through inclusive threat modeling participation.



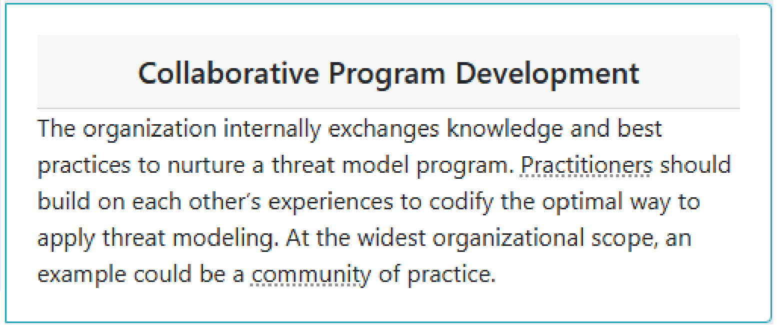
Value-Driven Management

The threat modeling program is managed, structured, and defined at an organizational level and provides recognizable value.



Seamless Alignment

Threat modeling outcomes influence the implementation or operational workflows. For example, guiding testing in the SDLC.



Collaborative Program Development

The organization internally exchanges knowledge and best practices to nurture a threat model program. Practitioners should build on each other's experiences to codify the optimal way to apply threat modeling. At the widest organizational scope, an example could be a community of practice.

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

Threat Modeling as Communication

- Focus for team discussions
- Guiding implementation
- Recording consensus
- Sharing with others
- Capturing rationale for future us

Readability and usability of output is critical!

“Security at the Expense of Usability Comes at the Expense of Security”

- *Me, really*

Takeaways

- Design with Empathy – it's a superpower
- Focus on the humans
- Be inclusive
- Work together as a team
- Be mindful of UX always
- Write for the reader
- Output is static, thought process is dynamic

THANKS FOR LISTENING!

Avi Douglen

Bounce Security

🐦 @sec_tigger