September Community Meetup

THREAT MODELING CONNECT

# Scoping for Threat Modeling

September 22nd | 11:00 - 12:00 ET

Hosted by:

**Robert Hurlbut**
Principal Application Security Architect / Threat Modeling Lead
Aquia

# About the Community Meetup

- **Our Goal**
  Exchange real-world experience, share practical knowledge, validate ideas to improve our own practice.

- **Chatham House Rule**
  *Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.*

- **Video is optional but highly recommended :)**

## 📆 Agenda of Today

| | |
|---|---|
| 11:00 | Welcome and intro |
| 11:05 | Photo |
| 11:07 | Presentation |
| 11:25 | Discussion |
| 11:55 | Closing & Announcements |

# About me

**Robert Hurlbut**

*Principal Application Security Architect / Threat Modeling Lead*

Aquia Inc

- Started and led Threat Modeling Program for 5 years at Bank of America with 40,000 developers and 10,000+ products (seeing 1,500+ threat models created)
- Currently leading a Threat Modeling Program for a major government agency
- Co-author of Threat Modeling Manifesto (2020)
- Co-host of Application Security Podcast (2016+)

# Scoping for Threat Modeling

# Threat Modeling

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

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 Manifesto (TMM, 2020) - https://threatmodelingmanifesto.org

**Many times, the focus of "scoping" is on Item #1 above - *What are we working on?***

**Do we need a threat model of a large system or a single sprint change?**

# Avoid “boiling the ocean”

- “Boiling the ocean”: Undertaking an impossible task or making a task unnecessarily difficult (i.e. it’s literally <u>impossible</u> to boil the “whole” ocean)
    - Variously attributed to Will Rogers, Mark Twain, or Lewis Carroll

- Tendency to scope too large for a threat model
    - Ex: One front-end application with 1000+ microservices or 1000s of applications - “We’ve got to threat model them all!”
        - Admiration of the Problem anti-pattern: “Go beyond just analyzing the problem; reach for practical and relevant solutions.” (TMM, 2020)

# Scoping for Value

*“Very few organizations will have the time or resources to* ***threat model*** *their entire ecosystem. Assuming you do not have that luxury, you still can realize quite a bit of* ***value*** *just by adopting the mindset of looking for* <u>*blind spots and questioning assumptions*</u>*.”* *

* “‘Invisible’ Technologies: What You Can’t See Can Hurt You”, Ed Moyle (2017)

# Existing products vs new development

- Existing products
  - What products have the most exposure?
  - Are there external dependencies? (Diagrams can help)
  - Has some level of risk been determined for certain products (i.e. high risk / critical vs. medium risk vs. low risk)?
- New development
  - Review new features
  - Review big security decisions
  - For APIs, consider Mozilla's Rapid Risk Assessment (RRA) approach
  - Use Agile or Incremental Threat Modeling approaches
- TMM Patterns: Systematic Approach, Varied Viewpoints, Useful Tookit

# Versioning and Deltas for Threat Models

- Versioning threat models
  - Threat models are not static
  - Start with a base threat model (v1.0)
  - Create new versions by major features or large changes
- Deltas
  - Determine what's new in the system versus last time a threat model was created
  - Could we create a smaller threat model of the change(s)?
    - Perfect Representation (anti-pattern): "It is better to create multiple threat modeling representations because there is no single ideal view … may illuminate different problems." (TMM, 2020)

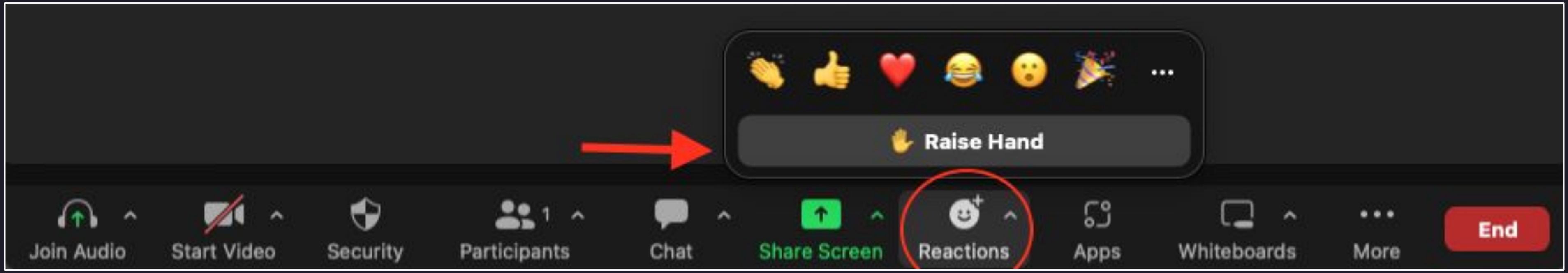
# Conclusion

- Don’t be afraid of scoping - threat modeling is too important not to do it
- Find ways to break down a larger scope of work into smaller, more manageable slices of work
- Take your time - threat models evolve and continue to improve

# Discussion

- **Question 1:** What are the challenges you have faced in scoping?
- **Question 2:** Any success stories in scoping?
- **Question 3:**  Any questions/guidance/takeaways?

Use "✋ Raise Hand" feature to let the hosts know you have something to share.



# Next Meetup

**Topic:** ThreatModCon 2023 Retrospective

**Date:** November 15, 2023

**Register:** threatmodelingconnect.com/events

THREAT MODELING | LAB

# Continuous Security

## Leverage incremental threat modeling

November 9th | 11:00am-12:30pm ET

**Irene Michlin**

Application Security Lead, Neo4j

OCT 29 | Washington, DC

# THREAT MODCON 2023

Join the **first Threat Modeling Conference** and meet the community.

Limited spots available. Secure yours today.
Use code **CONNECT** to receive $20 off.
**threatmodelingconnect.com/events**