

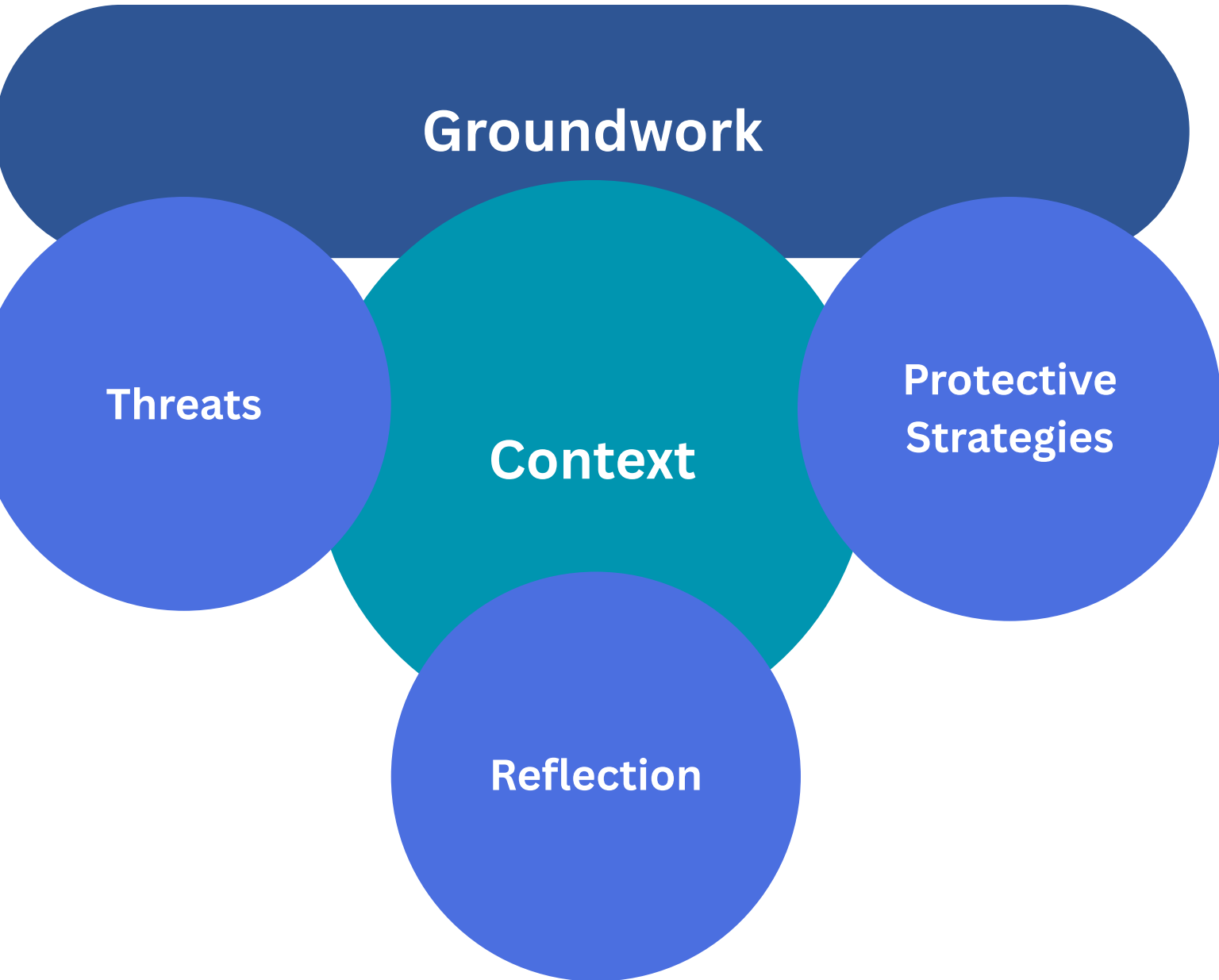
Human-Centered Threat Modeling: Framework, Guidelines, Lessons Learned

Warda Usman, Yixin Zou, Daniel Zappala

SoK (IEEE S&P 2025) + Interviews with researchers (IEEE S&P 2026)

Human-Centered Threat Modeling

a process to identify how people perceive and respond to security, privacy, and safety risks to themselves



Groundwork

understanding – developing connections and trust – ethical considerations

Context

risk factors – unique challenges – culture – personal identity and perception – technology background and usage

Guidelines and Considerations

1. Start with groundwork
2. Understand the centrality of context
3. Threat modeling is a broad process of discovery
4. Threat modeling is a non-linear and connected process
5. Customize the framework
6. Consider offline threats and non-technical considerations
7. Work toward a complete threat model
8. Use the framework at different stages of the research process

Threats

concerns – harms – actors – trade-offs – threat appraisal

Protective Strategies

recovery – information seeking – defenses – mapping threats to defenses – perceived cost – coping appraisal

Reflection

efficacy – barriers – advice – visioning

Lessons Learned

Groundwork is a continuous responsibility



“We end up buying a bunch of smart home devices to see how they actually behave ... A lot of the info online is either outdated or very superficial, so testing things ourselves is the only way to really understand what’s going on.”

Relationships with communities are both necessary and complicated



“And so when you recruit through an organization, there can be this feeling of like, well, we helped you, therefore we were hoping that your results are what we wanted to hear.”

Values are embedded in the work



“I would see the world as sort of fundamentally a place with a lot of inequities ... a lot of security, privacy, safety problems are a result of systems that value some people over others.”

Threat elicitation should start broad and stay participant-centered



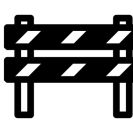
“We got much more rich data when we talked to them about specific issues that their community was facing, and their behaviors in response to those issues.”

HCTM should be a collaborative process between researchers and participants



“I never want to parachute in and be like, “Aha, I think you have a problem”, and they’re like, “No, this is not a problem. Why are you here? Go away.”

Structural barriers limit impact



“I think that's a big tension we have in academia, which is, like, it would be great if someone [followed through on future work for a research project], but, you know, this student wants to graduate and go, so probably not them.”