Why is the Hero Threat Modeler Detrimental in Group Work

The *Threat Modeling Manifesto* was developed to help anyone wanting to identify "what can go wrong in a system" (Shostack et al., 2020). The text is meant to be used as a guide, thanks to values and principles, to help develop secure solutions. The article lists some benefits from following the manifesto: systematic approach, informed creativity, varied viewpoints, useful toolkit, and theory into practice. According to the authors, this methodology prevents some problematic patterns when conduction a threat modelling. Amongst those anti-patterns, there is the 'hero threat modeler' which consists of a unique individual imposing his mindset while taking over threat modelling.

In the context of a university's group work, the ideal is obviously to meet regularly and discuss the assignment as a team. However, the reality of full-time work and part time study implies that time is valuable and limited. In this context, it is natural that, as a group, assignments are planned and divided per individual, putting pressure on ensuring the parts are done in a certain deadline. This way of doing creates silo work which is discouraged according to *Threat Modeling Manifesto.* Most groups proceeding like that, meet and show their work to each other to ensure varied viewpoints.

During my Module on Security and Risk Management, at University of Essex Online, the first team assignment was to prepare a risk identification report based on a fictive company. Two of the teammates were project managers and one was pentester consultant with 10 years of experience. Due to the restricted timeline, we decided to divide the workload according to our strengths. Our expert in IT took the most technical part, whereas the two project managers separate amongst themselves what was left. Throughout this assignment, the pentester did not show his part to the group as he only provided his work 24h before the deadline. As he is an expert, he did not perceive the need to share with us his threat modelling prior to that point. Considering that I had watched all the seminars, I know which model what supposes to be used for the risk assessment, however the IT specialist had decided to apply a different threat methodology. The academic grade for this assignment was the lower I had during my postgraduate certificate, and the main reason was the part from the pentester, which remained hidden and isolate too long from the rest of the team input.

I'm a project manager and it is routine to close projects with an exercise called lessons learned (Guide, 2001). So here are my lessons learned from this experience:

1) Trust yourself if you have done the readings, the works, and the seminars
2) Meet regularly, ideally weekly
3) Determine an early schedule for work to be done, one week before the final deadline
4) Ask the teammates to put their parts to a shared platform for all to see
5) Challenge the teammates on their parts
6) Participate in brainstorm for developing threat modelling or similar activities
7) Ensure the implementation of a dialogue with expert teammates

References

Guide, A. (2001). Project management body of knowledge (pmbok® guide). In *Project Management Institute* (Vol. 11, pp. 7-8).

Shostack et al (2020) *The Threat Modelling Manifesto.* Available from: https://www.threatmodelingmanifesto.org/ [Accessed 14 October, 2022].