Security by Design: Threat Modelling

Dr Rosanne English

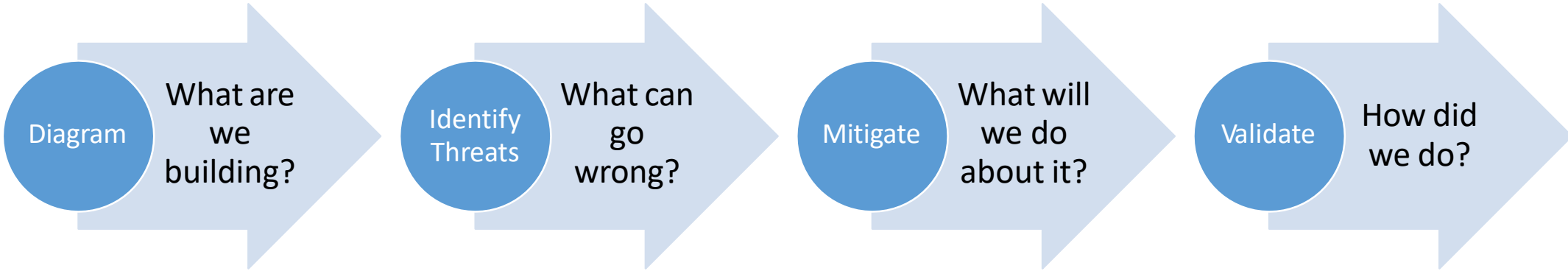
What is threat modelling?

A systematic and structured approach to determining the threat landscape for a given context

Why threat model?

- Increased data and connectivity results in increased attack space
- Threat actors need only locate one vulnerability
- Breaches in security can be costly for organisations

General Threat Modelling Process



[Threat modelling article - Goran Aviani]
[Agile Threat Modelling - Martin Fowler]

Activities and Outcomes

Question	Activity	Outcome
What are you working on?	Explain and explore	diagrams, e.g. components in software being built, points of entry, dependencies, sequence diagrams, data flow, state diagrams etc.
What can go wrong?	Brainstorm threats	A list of technical threats
What are you going to do?	Prioritise and fix	Prioritised fixes added to backlog
How did it go?	Reflection	Changes in procedure, policies, or mitigation mechanisms

e.g. using STRIDE, Cyber Kill Chains, Attack trees