Security canvas workshop
What are you building?  
(customer input)

- Model system
- Business goal

What can go wrong with your product?  
(working session with analyst)

- Define assets
- Define attacker model
- Threat modelling

Security Requirements
Action points
(Report-back by Security Analyst)
Outline of the Security Canvas approach

1. What are you building?
   • To answer that question, we focus on two aspects:
     • [Business goal] Determine what is the business goal of the system /device/software/../ to be analyzed
     • [System Model] Create a model of the system to be analyzed, which includes an overview of the attack surface and trust boundaries.

2. What can go wrong with your product?
   • To answer this question, we guide you during the workshop to:
     • Define the assets: what does the assumed attacker want, what the customer want to protect, and stepping stones for either of these
     • Define the attacker model (from a typical list of attacker models)
     • Threat modeling (e.g. using attack trees)

Outputs:
• Comprehensive engagement on security at the start of development (during the workshop)
• A report comprising a set of security requirements and action points summarized by our Security Analyst, which can be used as input at the start/early stage of innovation development