Main question:

# How can we dynamically improve security on android based devices with the focus on malware using the current Honeypot system while making it appealing for a target group?

It depends on what the target group is. But we can build security algorithms from the data we get from the system and defend the end users.

Part-questions:

# What is a Honeyjar-system and which information should it collect and generate?

## What is the current state of security on android based devices? (Saxion)

## What is the honeypot system in its current state? (AAU)

Right now it is a system that can start, stop and list VM, generate PCAP’s and scripts that can manage IPtables

## How do we improve the current Honeypot system? (AGU, AAU, UTP)

We can make a GUI to make it easy to access for users, implement it on a server and complete more aspects of the honey jar like the containment system

# Why and how should our target group use a Honeyjar-system?

## Who would benefit the most from android based security? (Saxion)

# What are the results of the Honeyjar-system and what does this mean from a business perspective?

## How do we create a product that can be profitable? (Saxion)