# Fremium datasharing / database model:

The honeypot system generates labelled data both trough an internal operator as well as trough people / companies who have downloaded the honeypot for their use. The honeypot is free of charge as long as all labelled data is shared with us. This labelled data is stored in a database allowing our machine learning to be trained.

As the business guy at talia suggested. Accsess to this database can also be a point of income by providing 2 database options.

1. Get data from the database from the last short while (free)
2. Get data from the database from an extended period of time ( premium, paid)

So one is buying accsess to a larger amount of data to do with whatever they so please. For example creating their own ML systems. Of course not ALL data will be shared, as the internal system has to be among the best. Therefore 2 times, say the last week (free) and the last 3 months (paid) is a solution. You should talk to talia about realistic time-frames.

# ML based locally deployed real time protection

A relatively simple business prospect:

We provide a server they need to setup with their network. We keep this server updated with the latest version of our machine learning algorithm. It scans the network in real time WITHOUT sending any data back to us. When it finds something malicious it detects and protects against it and then passes the now labelled data back to us.

Some challenges with EU law not withstanding, this should be relatively simple to do.