# Implementation of PoA

In this EPIC partnership, a close collaboration with two business, IT and management students from Saxion University is established. This collaboration is centered around the development of a plan of action, including topics like product development, idea generation, profitability and business planning. By implementing the PoA into a problem analysis, it is secured that the technical visions of the project are carefully combined with up to date market research and product development strategies, to determine the requirement specification of the system.

## Idea generation and product development

Alternative products - What products with similar intentions/functionality exist in the current market? (E.g. Ai2) - How can we be inspired by the features of these already existing products into something new? (Use already located malicious behavior to train machine learning algorithm, Product type/profitable solutions, etc.)

What does the costumer want? To determine what product our target group desires, an interview with possible customers could be conducted. (Alex & Morcel) Examples of questions for interview: - What type of interface design would you prefer? (Operating system, Interface structure, Most important functionality, Things you definitely don’t want to have included in the program) - What products do you currently use for cybersecurity purposes? - What types of malware are you most likely to be attacked by? ...

## Turning the idea into something profitable

Market field research - How does other companies create profitable solutions from similar systems? - How would these structures fit with the visions of the HoneyJar system? (Visualize) - What method of profitable solutions is most relevant for HoneyJar?

- Status on project funding and costs associated with the system - Sketch of expected costs and required funds for product development

# Stakeholder analysis

## Actions for us to take:

### Monitor (Low Power, Low Interest):

- Stakeholders in this category are not that important. They don’t bring a lot to the table, but it’s worth monitoring them as they might influence the product in the future. We’re not going to inform or ask them anything.

### Manage closely (High Power, High Interest):

- Stakeholders in this category, are the most important. They bring knowledge to us, regarding what they expect from our product which helps develop something more relevant. Because these stakeholders are also interested in the final product, they want to tell us exactly what they need so we can adapt. We have to manage closely with these stakeholders to keep them interested and to keep getting information. (e.g. a company could tell us they need a design that makes it possible to turn the system on/off remotely, so we know our product has to have this as a feature.)

### Keep satisfied (High Power, Low Interest):

- Stakeholders in this category also bring knowledge. These stakeholders function as supporters. They help with every part of the project we’re having trouble with. Doesn’t matter if it’s regarding machine learning, business approach, overall collaboration or help with the server. These stakeholders don’t really have an interest in the final product, so we should try to keep them satisfied so they can continue guiding us.

### Keep informed (Low Power, High Interest):

-

## Explaining our stakeholders

### Android developer

-

### Jan:

- Jan has high power and low interest in this project. He will bring knowledge about Machine Learning and have a say in how we develop our Machine Learning.

### Server guys:

- Server guys also have high power and low interest. They are going to make it possible to setup the server as needed. They will make the server available and tell us what is possible or not.

### Jens:

- Jens have a high power and low interest in this project, he is our supervisor. He is important in how we work together. He helps us get the overview of the overall approach to the project.

### Valentine:

- Valentine have high power and low interest. Almost as Jens, he functions as a supervisor. He helps us get a clearer business approach. Teaching us how to design a product relevant for companies and what companies are looking for. (also bring some technical knowledge maybe as Taliyah?)

### Cypersecurity (competitors):

- Antivirus companies are low power but high interest in this project. They will want to buy the algorithm in order to improve their own algorithm.

### Companies wanting our algorithm:

- Companies could want our algorithm for a couple of reasons. They could want to buy the algorithm that we have created in order to make analysis on malware on which we have a lot of information on, or maybe it is an up and coming antivirus company how wants to improve their firewall and antivirus searching technology.

### Talaia:

### Users of devices connected to the internet:

### Operator setting up own honeyjar:

### Cybersecurity (Collaborator):

- Having other Cypersecurity (Companies?) as a collaborator would be greatly beneficial if they would be willing to share their findings with us in order to improve our algorithm at a more rapid pace.

# GUI features

## Dashboard:

**Statuses:**

* Server / connection status
* Test Status
* Security alerts

**More in depth statuses:**

**Server status**

* Connection status
* CPU, RAM and HDD utilization
* Server uptime
* Network bandwidth utilization

**Test Status**

* Running / not running / fault
* Amount of VM´s running
* Type of malware running
* Recap of chosen settings
* Time left in current test

**Security alerts**

* In depth alerts. TBD

## Test:

**Status**

* Running / not running / fault
* Amount of VM´s running
* Recap of chosen settings
* Time left in current test

**Customization**

* Type of OS (operating system) to use
* Amount of VMs to run
* Time for the test
* Preload selected malware?
* More? TBD

**Run / don´t run**

* Start / abort buttons
* Delay function? (TBD)

**Log**

* Last X amount of experiments and if some of their results? (amount found?) TBD.

## Security

**Status:**

* Amount of alerts, with short description of alert type
* TBD: What is an alert, what types of alerts to input? How to implement disciption?

**IP-Tables + bandwidth**

* Clear rules
* Delete rule
* Accept IP
* Accept Port
* Block IP
* Block Port
* Set Chain policy
* Show Current traffic
* Limit Bandwidth

**Ruleset overview:**

* Overview of current IP rules

## Settings:

* TBD (Discuss today)

**Last log:**

* Amount of malicious software indicators found
* Date / time done
* Type of OS used
* Amount of VMs used
* Average server utilization (CPU, RAM, HDD)

**Previous logs:**

* List of previous logs, click to open to get into the “last log” field, to get basic data from said log.

**Work in progress concept of GUI interface…**

