Hi Morcel,  
  
You are asking very good questions, and I will try to answer them as good as possible in the following. I might not cover everything you would like to know, and maybe something is not clear - then please ask again. I am also happy to discuss it all during e.g. a Skype meeting. Next week I am quite available Wednesday-Friday between 10 and 12 in the morning (which between 6 and 8 morning in Brazil).  
  
1) Regarding the Honeyjar project in general.   
  
The Honeyjar project dates back to 2013 where a first architecture was developed as part of a master thesis project, and a first implementation was made.  
  
The motivation behind it was a need for good ground truth data to be used for research and training machine learning algorithms: We needed to collect network traffic traces, where we would be sure which applications created the traffic (and which of there were malicious and benign). There are surprisingly few such good traces available, and therefore many researchers still use very old (and in our opinion outdated) datasets such as the KDD’99 dataset from 1999. At the same time, we needed to record this traffic in a controlled and semi-closed environment to ensure that we do not cause harm to other people or organisations.  
  
The architecture was from the beginning based on the three parts you have already discussed in Riga, i.e.:  
- The test environment, which we try to create to “look as a real network”, based on a number of virtual machines that can be created and taken down again, with automatic installation of operating systems and software (malware and benign software) and an emulated Internet environment.  
- Containment, to ensure we can connect to the outside world, while not allowing harmful traffic.  
- The analysis part, where data are collected for analysis.  
  
None of these parts are trivial, each of them is in fact very complex - and even with working implementations it is always possible to further refine and improve. Based on this, we have been running a number of student projects since 2013, improving parts of the system. It has all been done based on the initial hardware “platform”, consisting of around 30 old PC’s. Some of the projects were actually quite succesful, i.e. some students received the Danish Tele Award in 2016 for their work where they analysed around 300.000 pieces of malware, and found patterns that differentiated malware from cleanware.  
  
While the implementation have been quite useful for our research, the hardware setup was far from optimal (performance was not so good, and sometimes one of the computers would break down and create problems for the experiments). So we were very happy when we last year received a grant from a Danish foundation to buy two new and very powerful Dell servers, which would allow us to streamline the setup and improve the performance. This is also why we have initiated the new Honeyjar projects. The hardware will be used for both Honeyjar (and hopefully many new student projects) and as a training platform for “white hacker training” - much of the architecture for these purposes are actually quite similar, since it is all about creating virtual machines and virtual networks. And we were lucky to win another grant for developing this training platform as part of a national training platform for cyber security. Also, with the new hardware in place we have gotten a much better (faster and separate) connection to the Danish research network.  
  
The two previous projects that the students did in the previous semester were related to the Honeyjar as they were exploring (1) a virtualisation setup for mobile devices, and (2) a setup for automatically setting up (and taking down) virtual machines on our new server-platform (based on a honeypot usecase).  
  
So as you can see the “Honeyjar” is more a platform which can host many different platforms than it is a single project in itself.   
  
So far I have mainly described the project as a place for running and monitoring malware in a closed environment (what Anna called Sandbox). In fact another application is to work as a honeypot, where we create something that from the outside looks like e.g. a company network and try to attract malware or attackers who think they are working their way into a real system: In this way, we can monitor their behaviour and how they work, in order to learn how to better protect real systems. This is something we have not explored much so far, but it could be interesting in the future. In connection with this, we have a good collaboration with our regional  representatives of the Danish National Cyber Crime Center (part of the police) - one of these guys is very active in the Honeynet project (googl it can you can learn much more..).  
  
So as you can see we have (as a university) had a mainly academic perspective on using the platform for education and research. I am very curious if you can see a way how this (or part of it) can be developed into a commercially viable product!  
  
  
2) Regarding the “Costs” question  
I think there are two answers to your question.  
  
One is the university perspective, where basically the current project is funded by 1) Donations from a Danish foundation (used to buy the hardware), and 2) A Danish research network project which provides us a limited amount (around 40.000 EUR) for developing a training platform. This is not much to develop a business from!  
  
The other reply (I am cc’ing Valentin as he might have different opinions) is the business perspective. Here I see what you are doing as an attempt to make a commercial product based on the Honeyjar design and functionality. As such, you would find no pre-allocated funds for the project, but rather an opportunity to “sell” the project to a company such as Talaia (or to other companies or investors).  
  
Here you would need to sketch one or more business cases: What is the required investments and what would be the potential return on investment? (and everything in-between: How? Which opportunities and threats? What is the timeframe? What is the strategy?)  
  
One approach that I would suggest could be to outline three different approaches:  
- The light version, which requires at least investment as possible, but still with a possible outlook  
- A “middle way”, representing a higher investment, of course with an ever better possible outlook than (1)  
- An “all in” approach, where a heavy investment could result in e.g. a globally leading market position within a short timeframe - a higher investment than (1) and (2), but with an outlook to match.  
  
I am not sure what should be the order of magnitude for investments in the different scenarios, I really think you need to clarify what size of investments would make sense given the project and its potentials. For the energy company where I am in the board, a small investment would be around 1 mio EUR, a medium but significant investment around 10 mio EUR, and a very large investment around 100 mio EUR - but of course this would be different from company to company.  
  
If you accept this reply the ball is really played back in your field, as you would need to define the magnitude of the investment, as well as your approach to the market:   
- Which segments and geographies do you see as your markets?   
- Is it a local/regional/national/European/International/Global scale?  
- How to start out in the different scenarios.  
  
Maybe Valentin has different opinions?   
  
And maybe I am now just a tech guy trying to respond to a business question, so if you have more qualified ideas (or maybe your supervisor has) then that is super fine with me.  
  
Kind Regards,  
  
Jens

Hi Morcel and Jens,

Nice discussion!  I'm also a tech guy, but let me share my opinion too. I would say that I would go with the light version of Jens or even less. I think that the other two options are rounds for companies in a more mature stage. As far as I understood from the project, the idea is to create something almost from scratch, and for getting those funds you need first to find out (and being able to demonstrate) whether your idea has traction in the market. It is very difficult that someone give you that much amount of money when you are just creating the company.  
  
Another approach would be the bottom up, you can do a business plan that uses the minimum resources possible in order to be able to create the company and find out if your idea has traction. So at the end of the project, you will be able to go to an investor and say: "We have this amazing idea and we need 500.000 € to bring it to the market".  
  
However, and as Jens said, this is just an opinion :)