# Plan of Action

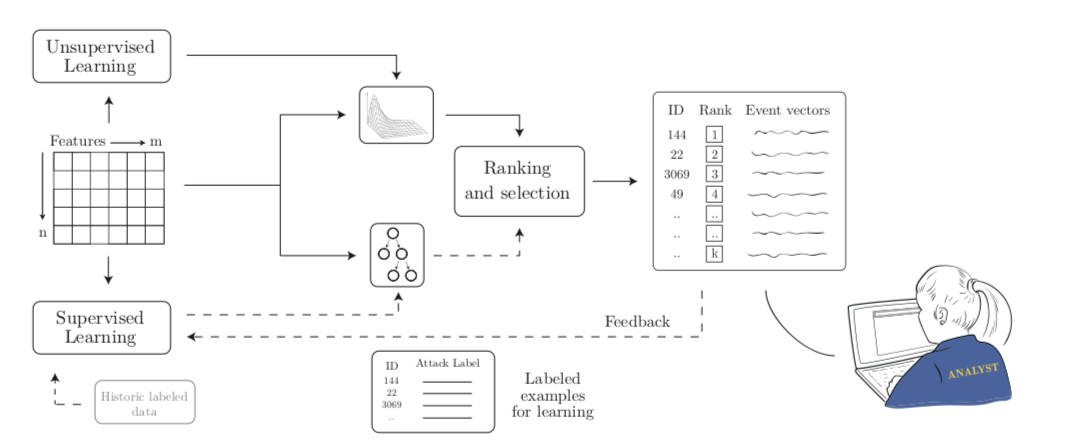
In this EPIC partnership, a close collaboration with two business, IT and management students from Saxion University is established. This collaboration is centred around the development of a plan of action, including topics like product development, idea generation, profitability and business planning. 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.

## Market research and idea generation

Machine learning systems like neural networks are often considered as the magic bullet to secure networking systems. Strategies like AI controlled anomaly detectors are widely used in today’s world of cybersecurity techniques, as a tool able to identify previously invisible attacks.[[1]](#footnote-1)

A system developed by researchers from MIT’s Computer Science and Artificial Intelligence laboratory (CSAIL) and the machine-learning startup company PatternEx, claims ability to not only detect but actually to predict 85% of cyber-attacks using supervised Deep Learning trained algorithms and unsupervised outlier detection. The core functionalities of this system can according to their published research, be divided into four main components[[2]](#footnote-2):

* Big data processing system
* Outlier detection system
* Feedback mechanism and continuous learning
* Supervised learning module



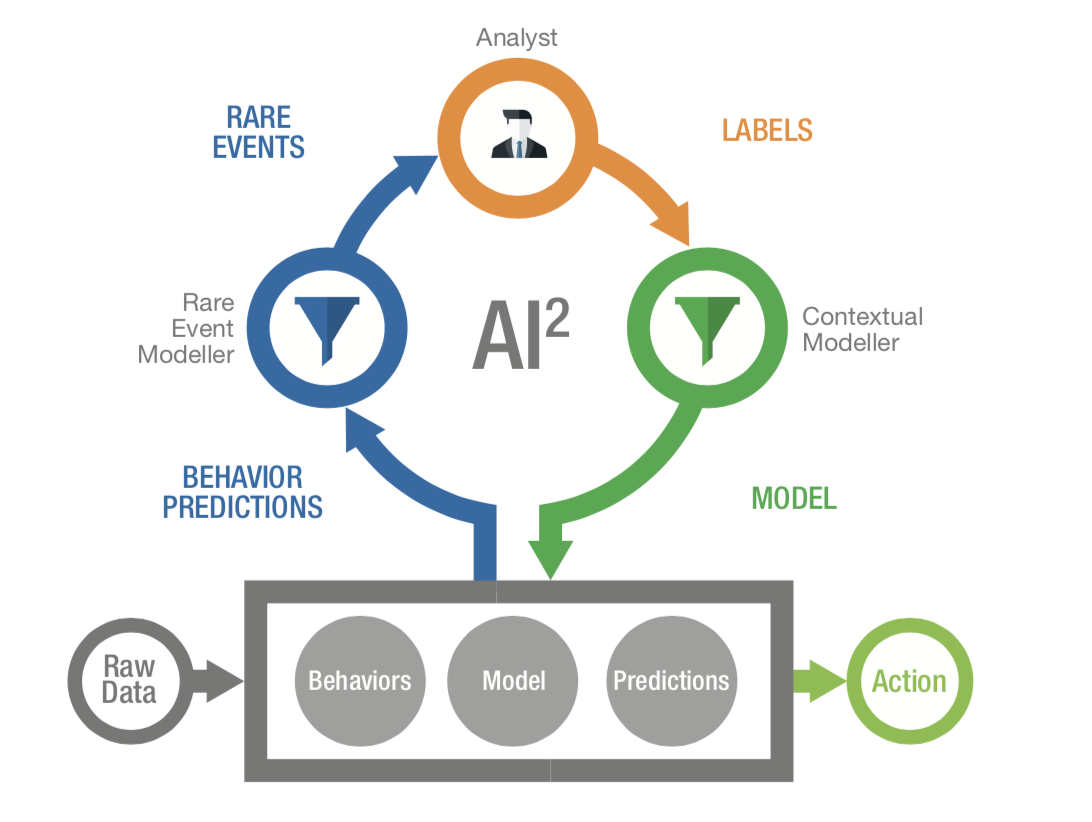
Figur 1 Illustration of the Ai2's core functionalities.

By combining the unsupervised learning module with a complex supervised neural network, this system allows for effective anomaly detection. The relations between the main components of the system, is illustrated by the directional arrows in *Figure 1*. The first component of the system, the unsupervised learning module, actively processes big data datasets by quantifying the traffic data into behavioral patterns (features) of different entities. By using mathematical and statistical data modelling, the data is sorted by an algorithm created from the identified features and ranked by recognized malicious pattern striking as anomalies.

This representation of the network traffic data ranked by its possibility of being malicious, is then analyzed by human network analysis experts, to confirm whether the top ranked anomalies is of actual malicious character and transform the data into labeled data. The result is then fed to the supervised learning module, that predicts whether a new incoming network traffic data dump is normal or malicious. As new feedback is constantly generated by the active system, this module will constantly be refined. The data generated by the supervised learning model is additionally used to identify and extract new features for training of the unsupervised learning module.

To simplify the concept of the AI2 system to its absolute core functionality:

* 1st module, automatically extracts behaviors from raw data
* 2nd module, models the data to detect anomalies
* 3rd module, has a human analyst label the anomalies as either malicious or normal
* 4th module, adjusts the supervised models based on the analyst’s labels



Figur Illustration of core functionalities

### Productizing the AI2 system

* InfoSec complete security system
* Method of sale – how do they make profit?
  + E-mail questionnaire/interview

This section will include a discussion of how to effectively productize a machine learning based system like the Ai2, and transform it into a marketable product. We imagine this to be a close collaboration between Saxion and AAU.

The company selling the technology of the Ai2 system in collaboration with the researchers from MIT, is called PatternEx and we picture a collaboration with them as well if they’re interested. At the current stage, we imagine something along the lines of us asking them some questions via e-mail about:

* the technical circumstances of creating a system using human intelligence as analytical power combined with unsupervised and supervised learning modules to create a powerful malware detection/prediction system (Forming the questions in close collaboration with Ahmet)
* how they turned this AI based analytical system into a marketable product and what type of sale techniques/marketing strategies they are using (Forming these questions in close collaboration with Alex and Morcel)

This idea of reaching out for PatternEx is currently being discussed with Jens.

## From idea to profitable solution

**-**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?   
- Current status on project funding and costs associated with the system   
- Sketch of expected costs and required funds for product development

## Possible customer interview (Alex and Morcel) To determine what product our target group desires, an interview with possible customers could be conducted in close collaboration with Alex and Morcel. Examples of questions for such 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?

Questions for interview with Alex and Morcel

* From your conducted field research, what can you tell about competitors of similar systems available on the current market?
* If you were to identify a few of the most important market factors, that should influence the decisions within the technical aspects of the system development, what would those be?
* Is it possible to create a “longer sighted” business plan for this project?
* Can you elaborate on how an idealistic subscription based system would be structured? (Would be nice with some visualization)
* Can you present some alternative methods to monetization of our end product?
* Can you very precisely from your perspective, form the three most important requirements for the collaboration between Saxion and AAU in this project?

1. <https://securityintelligence.com/with-ai2-machine-learning-and-analysts-come-together-to-impress-part-1-an-introduction/> [↑](#footnote-ref-1)
2. <https://people.csail.mit.edu/kalyan/AI2_Paper.pdf> [↑](#footnote-ref-2)