Project Plan

AI-FANATICS

ACA-IT

<<
This template can be used for all projects, especially software engineering projects. Chapters or parts that are not applicable can be removed.

Text in italic is background information and must be removed in the definitive version of your project plan.

Note that this is a template and can be changed for own purposes, e.g., you can adapt the layout to the layouts as used at the company of your internship.

For your project name, think of a name that highlights the most relevant aspect of your project, and specify whether it is about graduation internship or third year internship.
>>

Date	**:**	**02/17/2023**
Version	**:**	**V0.1**
State	**:**	**In progress**
Author	**:**	**AI-FANATICS**

Version history

Version	Date	Author(s)	Changes	State
V0.1	02/17/2023			
V0.2	02/28/2023			

Distribution

Version	Date	Receivers

Contents

1. Project assignment

1.1 Context

An element of the Advanced Cybersecurity semester is participating in a group project for a company client. All members of the group chose this project because each of us was interested in integrating AI (Artificial Intelligence) technology in a cybersecurity context.

We are working on a project with ACA-IT, which is a company located in Eindhoven. They are an IT service provider for a plethora of clients. They distinguish themselves from their competitors by focussing on innovative business-related IT-solutions, continuity, availability and most importantly, security.

1.2 Goal of the project

We are living in the information era, which means data is increasingly valuable. Therefore, the threat of advisories trying to exfiltrate that data, becomes prominent. Blue teamers are tasked with safeguarding the security, confidentiality, and integrity of a system. As AI (Artificial Intelligence) evolves over the years, it is getting implemented in a lot of different fields, including blue teaming.

The usage of anomaly detection in monitoring software is to detect irregularities. On the other side, there are red teamers that try to remain undetected, and what better way than to fight fire with fire. The goal of the project is to research and develop an AI that can help red teams avoid detection, and in turn use that information to help ACA-IT bolster their defences.

1.3 Scope and preconditions

Inside scope:	**Outside scope:**
1 Writing documentation on how the client can deploy/test the solution	1 No maintenance of AI after the end of the project date
2 The AI is going to function on a test environment (NetLab)	2 Gathered data will not be used maliciously
3 Demo environment on NetLab	~~3 Developing a new algorithm to analyse data~~
4	4
5	5
6	7

1.4 Strategy

We are using the Scrum methodology unlike waterfall we have more flexibility when on comes to planning and execution based on the client's preferences/suggestions. The sprints will consist of 3 weeks, which means 6 sprints in total.

We have created a backlog in Trello, containing all known tasks and use cases.

1.5 Research

Pre-research

It's important to have some knowledge about the base fundamentals of machine learning before we're able to do relevant research and develop a meaningful solution. The following topics will be researched in the earliest stage of the project by all group-members.

- Machine learning
- Algorithms
    - Supervised learning
        - Decision trees, Naïve Bayes, Support vector machines, etc.
    - Unsupervised learning
        - K-nearest Clustering, Hierarchical Clustering, etc.
- Models
- Big data
- Tools
    - Google Collab

Main-Research

1.5.1 Main question

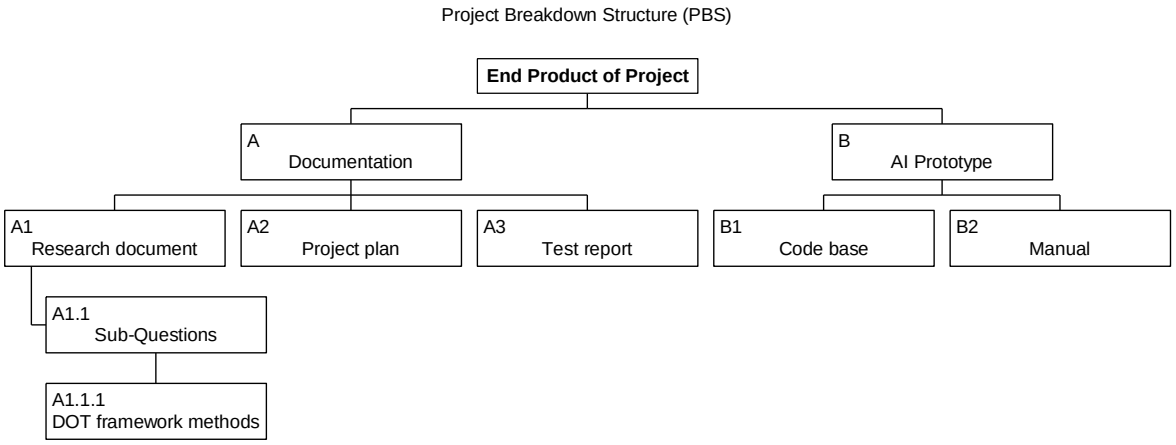
Suggetsion1: How can AI help avoid any detection by blue teams?
With this question, we want to answer how an Artificial Intelligence can help a red team avoid detection by a blue team/monitoring system. (Signature detection etc.)

1.5.2 Sub question

- Are there any existing solutions on avoiding blue team detection?
    - With the answer to this question, we want to research and conclude if there are any existing Artificial intelligence systems that can help a red team avoid detection by a blue team.
    - DOT-Framework Methods: Available product analysis,
- What methods do blue teamers implement to detect anomalies?
    - With the answer to this question, we want to determine what methods are used by blue teamers to detect possible anomalies.
    - DOT-Framework Methods: Design pattern research, Expert Interview
- What types of AI can be used for evasion of defences? (ML/DL/etc)?
    - With the answer to this question, we want to research and conclude what type of AI algorithm can be used/fits the best to evade the defences of a blue team.
    - DOT-Framework Methods: Literature study, Available product analysis, interview
- What data is relevant to train the AI to avoid blue team detection?
    - With the answer to this question, we want to determine what data is relevant to train the AI to avoid any blue team detection and what data we need from the company and what data we need to create for ourselves.
    - DOT-Framework Methods: Interview, data analytics
- How can the company benefit from the AI's output?

- With the answer to this question, we want to explain how ACA-IT benefits from our test results en how it can help the company improve the safeguarding, security, confidentiality, and integrity of their systems
- DOT-Framework Methods: Prototyping, security test

1.6 **End products**



The final product of our projects is divided into an AI Prototype, usage manual and detailed documentation about it. The final product will be able to avoid blue team detection techniques and learn their weaknesses as more data is being fed to it. The end deliverable will have a code-based files that we will personalize for the client company and the data will be their own.

The documentation deliverable is consisted with detailed explanation of our research process, project plan and test reports that we have executed. Based on the DOT framework methods, this document will answer all predefined research questions.

2. Project organisation

2.1 Stakeholders and team members

Name	Abbreviation	Role and functions	Availability
Michael Waterman	*M.Waterman*	*Client*	*Company is located near TQ, also available through e-mail.*
Martin Ederveen	*Ederveen,Martin M.W.*	*Semester coach*	*Tuesday morning, Friday afternoon*
Lazar Dimitrovski	*L.D.*	*Group member*	*Tuesday, Friday*
Koen Sanders	*K.S.*	*Scrum master (Rotates)*	*Tuesday, Friday*
Ahmed Alharthy	*Alharthy, Ahmed A.S.A*	*Team leader*	*Tuesday, Friday*
Lisa Koremans	*Koremans, Lisa L.*	*Group member*	*Tuesday, Friday*
Naomi Kollen	*Kollen, Naomi N.S.M.*	*Group member*	*Tuesday, Friday*
Rob de Voort	*Voort, Rob R. de*	*Group member*	*Tuesday, Friday*
Angel Angelov	*Angelov, Angel A.S.*	*Group member*	*Tuesday, Friday*

2.2 Communication

The communication with the stakeholders goes through the team leader of the group which is defined in the table above. The whole team is responsible for the communication, but the team leader is the face of the project group.

3. Activities and time plan

3.1 Phases of the project

As explained in the chapter strategy we are using the scrum methodology, this means that the separate phases are called sprints. Each sprint consists of a period of three weeks, at the end of every sprint there is an evaluation and sub-delivery to the company. During the delivery, the company is freely to give feedback which we as group can use in the upcoming sprints as well as validate the user stories as done for “definition of done.”

3.2 Time plan and milestones

Sprints	Start date	Finish date
0	06/02	03/03
1	06/03	24/03
2	27/03	14/04
3	17/04	12/05
4	15/05	02/06
5	05/06	23/06

Sprint 1
Research and develop a way to avoid signature detection by the blue team. In the meantime, we're going to research the fundamentals of machine learning. So, at the end of Sprint 1 we're going to demonstrate how to avoid signature detection.
(This is an example, and could change overtime)

Sprint 2
Research and develop a way to overload the monitoring system of a blue team with false positives. This results in the monitoring system misclassifying an actual attack. So, at the end of Sprint 2 we're going to demonstrate this type of attack on our own environment.

4. Testing strategy and configuration management

4.1 Testing strategies

We're going to need relevant data to test our solution with. Given that we have setup a test environment in netlab, we are either going to generate dummy traffic/data, or we are going to create our solution based on actual data from ACA-IT. This data is going to be used to test the accuracy/efficiency of our proof-of-concepts.

4.2 Test environment and required resources

One of our research questions covers the investigation of different techniques used by blue teams to defend against potential attacks. To answer this sub-question, we are going to setup a test environment in NetLab.

Regarding required resources needed for the project, we are planning to use Google Colab. This is a service provided by google that support students, data scientists and AI researchers with their projects (Free of charge). AI requires a lot of computer resources, so a service like Google Colab would be an ideal solution.

4.3 Configuration management

While using the Scrum methodology JIRA is the most fitting backlog tool and version issue-tracking software for the project.

It would contain all the tasks and use cases for the project, with story points on each field to enable the creation of burndown chart, a way to assess the progress of work as we go.

For the tooling related to the code base that we are tinkering/creating, will all be saved in either Google collab itself or GitLab.

5. Finances and risk

5.1 Project budget

We are going to be using Google Colab for AI purposes which is free so there will be no budget required for the project.

5.2 Risk and mitigation

Risk	Prevention activities	Mitigation activities
1 Expanding project scope		Clearly defined scope
2 Absent team members		Clear expectations Multiple involved team members
3 Lack of knowledge, especially in AI		Group efforts to study tough subjects