Project Plan

1. Problem Definition

- 1.1 Problem to solve *(Which problem does the customer like to be solved?) - Brandie*
  - National Health Service (NHS) of the United Kingdom was the target of a ransomware attack in Spring 2017. Specifically, they were impacted by a ransomware known as WannaCry. WannaCry functions by encrypting all of a computer's files, and demanding bitcoin as payment to unlock them. It utilized an exploit in Windows known as EternalBlue. Most of the impacted devices were running outdated versions of Windows, such as Windows 7 and Windows XP. The ransomware also spread via the internet (but not from email).
  - As a result of the attack, NHS scheduling and payment systems were down for several days. Thousands of appointments and operations were cancelled, including those for emergencies.
  - Patient data was exposed, and the attackers even threatened to leak everything that they uncovered.
  - **SUMMARY:** NHS wants to address patient privacy, ransomware detection and prevention, and ransomware mitigation.

- 1.2 Goals *(What does the customer like you to do?) - Aleksandar*
  - Find a solution for ransomware prevention + detection

- 1.3 Scope *(What will be done by the group and what not?) - Thomas*
  - Data backup and recovery (can do by group)
  - Protecting the network (can do by group)
  - Analysis of the attack (can do by group)
  - How to protect sensitive data (can do by group)
  - Ransomware detection and mitigation (can do by group)

- 1.4 Research Questions and Sub questions *(including what security aspects are relevant in the chosen technology?)*
  - These questions will be given after our next meeting with the client.

- 1.5 Research Strategies to be used *(Refer to The Research Framework, see below) – Yasen*
  - DOT Framework: Known also as the development-oriented triangle framework is a way of organizing and defining research in ICT. It has

three main components: the "what", "why", and "how" of your research.

In the "what" phase, you focus on the specific use cases of your project and the available knowledge that can help. This includes understanding the context in which your IT project will be used and using existing theories and models.

In the "why" section, it is possible to clarify the purpose of your research. This may include creating a product that meets stakeholder needs or ensuring that appropriate standards are met. There is often a trade-off between having a broad overview and ensuring that you are certain about specific aspects of your business.

The "How to" section describes the methods and techniques to use in your research. This includes library research to analyze existing knowledge, field research to understand user needs, laboratory research to test aspects of your product, surveys a showroom to compare your ideas with existing work, and a workshop analysis to explore opportunities through sampling and design.

- 1.6 Deliverables *(What will be delivered the customer and to FHICT?) -*
    - Project Plan, etc

2. Team division of tasks *(Team members and sub-group division of the research questions, also see [Project Task] Develop Personal Leadership and [Project Task] Develop Interaction Skills)*

Work *division* of research questions

3. Activities and Scheduling (*make it specific for the coming weeks) - Brandie*

Week 4 – Client interview, new draft of project plan

Week 5 – Stakeholder interviews

Week 6 – Documentation of NIST requirements + additional requirements.

4. Test Environment *(What resources do you need in the seclab virtual environment?) -Al-waleed*

The secure solution will be implemented in the Seclab environment offered by Fontys. The exact needed resources will depend on the client requirements. However, according to our current information, we expect the environment to at least have a Pfsense firewall that has three VLANs and IDS configured. The first VLAN will contain an admin server that serves as a monitoring system, the second VLAN will contain the employees' computers, and the third VLAN will contain the server where backups will be stored. Whenever a ransomware gets launched, it will firstly get detected by the IDS installed in the Pfsense Firewall. Additionally, the monitoring server installed in the admin server will also be able to detect it. After the infection and cleaning the environment up, admins will be able to recover the environment using the backups stored in the third VLAN.

5. Risks *(Are there any risks concerning the project assignment, like legal, financial, organisational?)*

- Ransomware can laterally spread across a network. So, the test environment needs to be secure
- The workload for the group is spread evenly according to the demand of the project either software or infrastructure related. All members will have individual tasks but some tasks might require teamwork. If in the event a team member is sick, it could set back the progress of the project due to the low number of project members.
- The scope involves research behind a healthcare system for the UK. Detection should theoretically be able to detect malware from all the systems and should work, which means that any software or system created should be working for a large scale production environment.