Milestones:

1. Research Windows internals (API), Docker environment, and network protocols

   The application targets Windows systems, which requires an in-depth knowledge of Windows internals. Developing kernel modules requires knowledge of standards and subroutines. Similarly to Windows, in-depth knowledge is required to operate the Docker environment envisioned, in a secure manner. Finally, since we will be monitoring network traffic, we ought to understand network protocols.

2. Develop the network, host, and report modules in YAHOS

   Kernel drivers need to be developed for obtaining host information while a process is running. Components need to be developed.

3. Create and test a Docker container used to run and analyze new processes

   In order to test new processes that are chosen by the user to execute, we need to build a container first. That way if the user chooses to run a harmful process, their machine is protected.

4. Research Qt workflow

   Since Guillermo has no experience with Qt and Thomas hasn't used it in a while, they need to do research on Qt workflow to ensure future development using Qt runs smoothly.

5. Create UI components for all modules

   We want YAHOS to be easy to use, we need to create well designed UI components for each module in YAHOS. This will be done using C++ and Qt.

Timeline:

Task Number	Task	Task Timeline
1	Research Windows API calls	10/7/2024-10/21/2024
2	Research Windows Native API	10/21/2024-10/21/2024
3	Research Docker environment / Sandbox isolation	10/21/2024-11/4/2024
4	Research Network protocols / common packets for software	11/4/2024-11/18/2024
5	**Milestone 1: Research Windows internals (API), Docker environment, and network protocols**	**10/7/2024-11/18/2024**
6	Research how to attach to an existing process similarly to PROC MON	11/18/2024-12/2/2024
7	Develop Network Module	1/13/2025-1/27/2025
8	Develop Host Module	1/13/2025-2/3/2025

9	Research how to track process events through windows API	1/13/2025-2/3/2025
10	Develop a standard for data output	2/3/2025-2/10/2025
11	Develop report module	2/10/2025-2/17/2025
12	**Milestone 2: Develop the network, host, and report modules in YAHOS**	**11/18/2024-2/17/2025**
13	Create/Build Dockerfile for windows image	2/17/2025-2/24/2025
14	Create/Build Dockerfile for Linux image	2/17/2025-2/24/2025
15	Create docker-compose.yml file	2/24/2025-3/3/2025
16	Create mounted volume for data gathering	2/24/2025-3/10/2025
17	Research if this can backfire on host if loading suspicious software	3/3/2025-3/10/2025
18	Test images and containers	3/10/2025-3/17/2025
19	**Milestone 3: Create and test a Docker container used to run and analyze new processes**	**2/17/2025-3/17/2025**
20	Research QT workflow for C/C++ programming	3/24/2025-3/31/2025
21	**Milestone 4: Research Qt workflow**	**3/24/2025-3/31/2025**
22	Create UI components for each module	4/1/2025-4/15/2025
23	Compile components	4/1/2025-4/15/2025
24	**Milestone 5: Create UI components for all modules**	**4/1/2025-4/15/2025**

Effort Matrix:

Task Number	Task	Guillermo Effort	Thomas Effort
1	Research Windows API calls	50%	50%
2	Research Windows Native API	50%	50%
3	Research Docker environment / Sandbox isolation	50%	50%
4	Research Network protocols / common packets for software	50%	50%

5	**Milestone 1: Research Windows internals (API), Docker environment, and network protocols**	50%	50%
6	Research how to attach to an existing process similarly to PROC MON	75%	25%
7	Develop Network Module	0%	100%
8	Develop Host Module	100%	0%
9	Research how to track process events through windows API	50%	50%
10	Develop a standard for data output	50%	50%
11	Develop report module	50%	50%
12	**Milestone 2: Develop the network, host, and report modules in YAHOS**	**54.17%**	**45.83%**
13	Create/Build Dockerfile for windows image	85%	15%
14	Create/Build Dockerfile for Linux image	85%	15%
15	Create docker-compose.yml file	10%	90%
16	Create mounted volume for data gathering	85%	15%
17	Research if this can backfire on host if loading suspicious software	85%	15%
18	Test images and containers	0%	100%
19	**Milestone 3: Create and test a Docker container used to run and analyze new processes**	**58.33%**	**41.67%**
20	Research QT workflow for C/C++ programming	50%	50%
21	**Milestone 4: Research Qt workflow**	**50%**	**50%**
22	Create UI components for each module	50%	50%
23	Compile components	50%	50%
24	**Milestone 5: Create UI components for all modules**	**50%**	**50%**