1 Introduction: Part 1

1.1 Problem Statement

What problem is your project trying to solve? Use non-technical jargon as much as possible. You may find the Problem Statement Worksheet helpful.

Who - Students or cybersecurity or enterprise professionals that want to improve their cybersecurity readiness. Corporations that want to scout the next generation of cybersecurity professionals.

What - Cybersecurity offense and defense practice. The cybersecurity and business fields need a way for people to learn and improve abilities in defending computer systems, exploiting vulnerabilities, and responding to cyber attack situations.

Where - Situation based, in workspaces when incidents occur and employees don't know how to accurately respond, students in their everyday life trying to prepare for after college, and they lack the real life attack prevention and response experience needed to fully be prepared.

When - A continuous and ongoing issue for corporations, employees, and students who need to keep and develop talent prepared for attacks.

Why - To help students and employees practice and learn techniques in response to cyberattacks. This helps prepare students and companies' abilities in the many fields of incident response.

How - Through the creation of a cybersecurity arena where individuals can learn, practice, and develop their skills for the cybersecurity industry.

Problem Statement: What is a good way to decide whether a candidate is fit for cybersecurity roles, and to train the next generation of cybersecurity professionals.

1.2 Intended Users and Uses

Who will use the product you create? Who benefits from or will be affected by the results of your project? Who cares that it exists? List as many users or user groups as are relevant to your project. For each user or user group, describe (1) key characteristics (e.g., a persona), (2) need(s) related to the project (e.g., a POV/needs statement), and (3) how they might use or benefit from the product you create. Please include any user research documentation, empathy maps, or other artifacts as appendices.

Students:

- **Demographics**: Likely a younger individual. Attempting to gain an undergraduate degree or maybe graduate degree. Might not have a lot of experience in real world cybersecurity applications.
- **Hobbies/Interests**: Probably quite busy with school work, but still enjoys computers and computer technology. An interest in offensive or defensive cybersecurity. May tinker, but lacks a place to put skills to use.
- **Motivation**: To earn a living doing something that they're interested in. To also gain valuable skills and expertise in their field.

- **Personality/emotions**: Likely overwhelmed and stressed with their schoolwork. Also stressed due to having to somehow get an internship or work after college. Might be more of an introvert who prefers to tinker with their devices.
- **Values:** Putting forth a good effort on schoolwork and succeeding in their field.

Students need a place to practice their cybersecurity skills as well as learn new ones because they want to have a successful career in cybersecurity.

Students will have a place to practice and learn new cybersecurity skills. They can also potentially prove their capabilities to professors and employers giving an even greater benefit.

Technical Corporation Employees:

- **Demographics**: Likely middle aged or older with some form of degree and certifications. Probably new to cybersecurity or already has gained quite a bit of experience.
- **Hobbies/Interests**: Probably busy with work, but still enjoys computers and computer technology. An interest in offensive or defensive cybersecurity. May tinker, but like students may lack a place to put their full range of skills to use. Likely tries to keep up with the evolving landscape the best they can by reading articles/news about cybersecurity.
- **Motivation**: To earn a living doing something that they're interested in and support a family which they've likely started.
- **Personality/emotions**: Likely overwhelmed and stressed with their work. Also stressed due to the shifting cyber security environment.
- **Values:** Keeping the company safe from cyberattacks. Probably starting a family and values their side projects. Likely values their free time and family time. Ensuring they do the best job possible to continue advancing.

Technical corporation employees need a way to efficiently practice their skills because it may have been a while since they've encountered certain scenarios or may not be prepared for a new cybersecurity threat.

The benefits besides improving their skills and gaining experience against new threats would be potentially showing their employer they deserve extra compensation or some sort of promotion.

Non-Technical Corporation Employees:

- **Demographics**: Likely older with very little experience in cybersecurity. Likely doesn't have much of an idea of the technical aspects and is more focused on running the company. May have a degree like an MBA. Probably quite wealthy overall as they take on more of a management role.
- **Hobbies/Interests**: Probably enjoys more free time outside of work. Might go on weekend trips or collect expensive items.
- **Motivation**: To make their company earn as much money as possible. Find the best talent and keep the company secure in the cyber realm.
- **Personality/emotions**: Likely outgoing and friendly. Maybe a bit boastful or may brag about their position.
- **Values:** Likely values company success and employee motivation. Likely values their free time and families.

Non-Technical employees need a way to be able to reach recruitable students and practice non technical skills such as media management during a cybersecurity attack. This is because in order to ensure their company remains profitable they have to maintain a high level of company security.

The benefits of this would be making it easier for recruiters to find new talent at student events. It would also allow for them to practice those skills outside of the technical ones that may be needed during a cyber attack.

Professors:

- **Demographics**: Likely a middle-aged or older individual. They likely have a higher level degree, such as a PhD. Probably has a lot of experience and knowledge relating to the field of cybersecurity.
- **Hobbies/Interests**: Likely spends a lot of their time writing new lessons, exams, and lab assignments. Likely runs CDC's and enjoys discussing cybersecurity related matters with students.
- **Motivation**: To teach and help students learn new cybersecurity skills while also helping them to practice old ones. To create the next generation of cybersecurity experts.
- **Personality/emotions**: Likely stressed with having to put together a lesson plan and teach. Likely enjoys putting on CDC's and seeing their students gain knowledge related to cybersecurity.
- **Values:** Challenging their students. Making sure that they gain knowledge related to cybersecurity.

Professors need a simple to use program or space to efficiently teach and help students to gain skills and experience since they are motivated by training the next generation of cybersecurity experts.

Professors can use CySim as a new way to engage with students in the field that they are teaching, and can treat it as a new way of administering curriculum or other academic, skills-based challenges. The other benefit is making this easier then now and giving them a good way to let students gain real world experience in a controlled environment.