4 Design

4.1 Design Context

4.1.1 Broader Context

Describe the broader context in which your design problem is situated. What communities are you designing for? What communities are affected by your design? What societal needs does your project address?

List relevant considerations related to your project in each of the following areas:

Area	Description
Public health, safety, and welfare	**Cybersecurity Training** - Increases security team's abilities in protecting corporate/personal information and critical infrastructure, and students are able to use CySim for training experiences and increase job opportunities
Global, cultural, and social	**Accurate/Similar to real life scenario** - Organizations are allowed to create scenarios for students that will be tailored to situations that happen in their work environment. These need to reflect their work environment's culture and show how they can improve their security posture.
Environmental	**Power Consumption** - Servers will be running on electricity, likely generated by some nonrenewable resources. **Server / Equipment Materials** - Servers and computing resources utilize rare earth metals
Economic	**Executive Response Training** - Executives will have the space to freely examine situations and be able to practice accurately reporting on the situations. In real life, these actions affect the company's trust and stock evaluation. **Cybersecurity Training** - Participants will be able to practice defending specific systems that are tailored to real situations. So, we will have people prepared in incident response able to lessen financial damages in cyber breaches.

4.1.2 Prior Work/Solutions

Include relevant background/literature review for the project

– If similar products exist in the market, describe what has already been done

  - **CDC competitions** - Students are able to secure a network of systems to the best of their ability. Red teams will attack these spaces and plant flags. The students are then required to look at logs and try and figure out how the red team got in and submit how. As this is going on, there are also mini challenges like decrypting a cipher text, buffer overflow attacks, and updating server software to get their team some more points.
  - **CTF** - Participants all around the world can participate. This is different from the CDC because it is more individual based rather than working in a team. It is also only a challenge, and you are not securing systems. You will be doing a task to get a flag, and then you can submit the flag to get yourself some points. A lot of these challenges will include buffer overflow, integer overflow and network problems
  - **Tabletop** - There is a multi-stage scenario on the system, and it is up to the participants to explain the actions they would take to be able to resolve the situation each step of the way.

– If you are following previous work, cite that and discuss the **advantages/shortcomings**

  - **CDCs** have a lot of what we need, like space for teams to be able to secure systems. Also, it has live scoring, and mini challenge space. What it does lack is the ability for corporations to get involved.
  - **CTFs** are great to practice utilizing exploits in order to capture data, and help give hands-on experience in identifying vulnerabilities. Much like the CDC, however, it's still not as accessible to team members without a basic level of vulnerability exploitation knowledge.
  - **Tabletops** are very accessible to all members, but require a lot more discussion time and debriefing in order to fully understand the impact of the exercise.

– Note that while you are not expected to "compete" with other existing products / research groups, you should be able to differentiate your project from what is available. Thus, provide a list of pros and cons of your target solution compared to all other related products/systems.

- Pros

  - CySim focuses on relating game scenarios to real world industry operations
  - CySim allow for corporate management to see incident response operations and understand a feel for time and impact of security breaches
  - CySim simulates financial impacts of security breaches, showing technical teams the importance of their positions
  - Depending on the players available, different styles of games are able to be played. These games incorporate many aspects from CDCs and Tabletops
  - CySim allows the ability to remotely connect where the CDC you have to physically be there

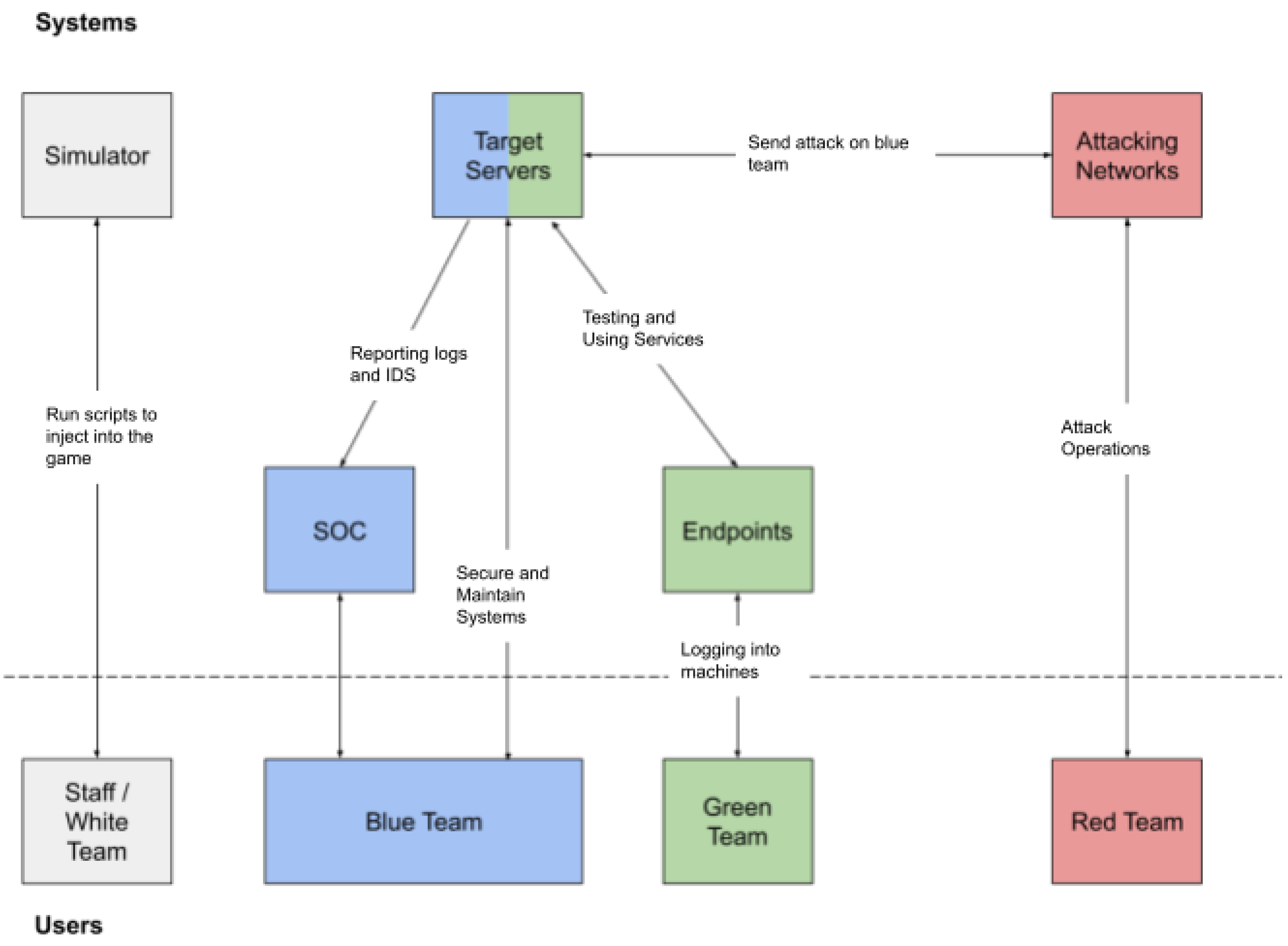
- Cons

  - CySim like a CDC, is a full day competition whereas CTFs and Tabletops are able to only be an hour to a few hour events
  - In order to maintain CySim you will need to rely on external sources to ensure funding

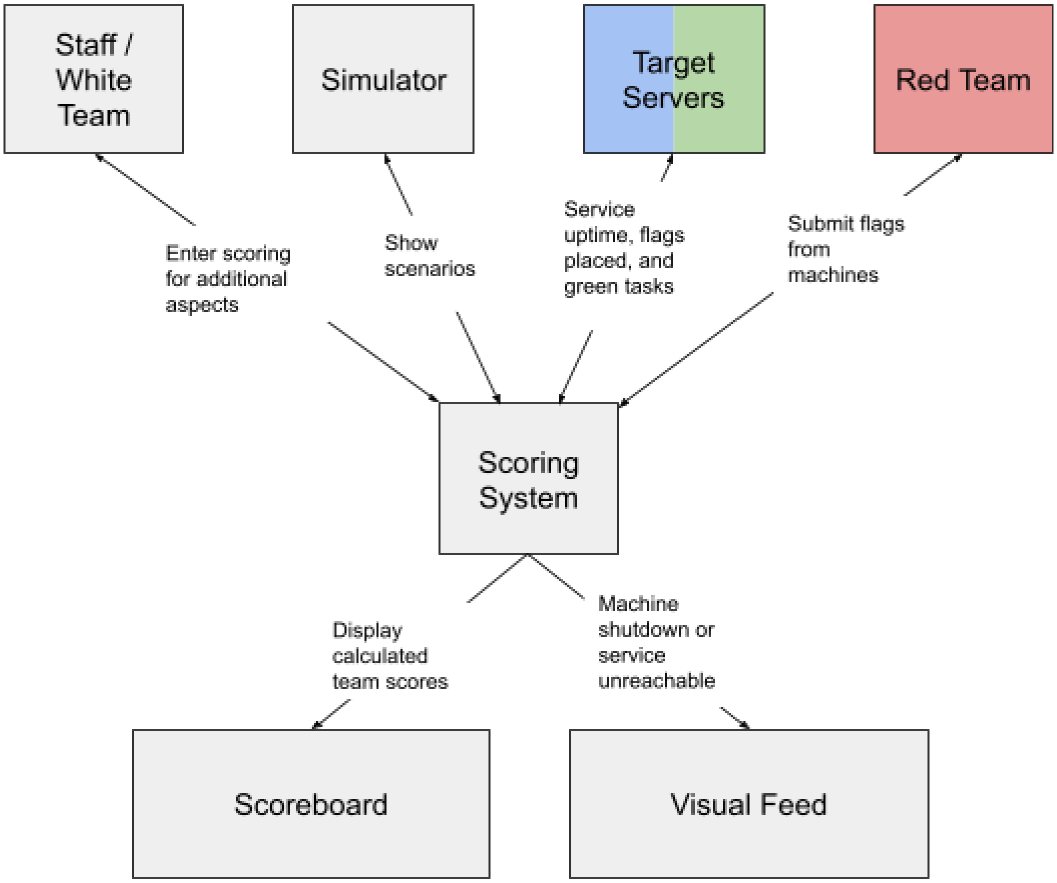
4.1.3 Technical Complexity

1. The design consists of multiple components/subsystems that each utilize distinct scientific, mathematical, or engineering principles –AND–
2. The problem scope contains multiple challenging requirements that match or exceed current solutions or industry standards.

Systems:



Scoreboard logic:


Staff / White Team
Simulator
Target Servers
Red Team
Enter scoring for additional aspects
Show scenarios
Service uptime, flags placed, and green tasks
Submit flags from machines
Scoring System
Display calculated team scores
Machine shutdown or service unreachable
Scoreboard
Visual Feed

4.2 Design Exploration

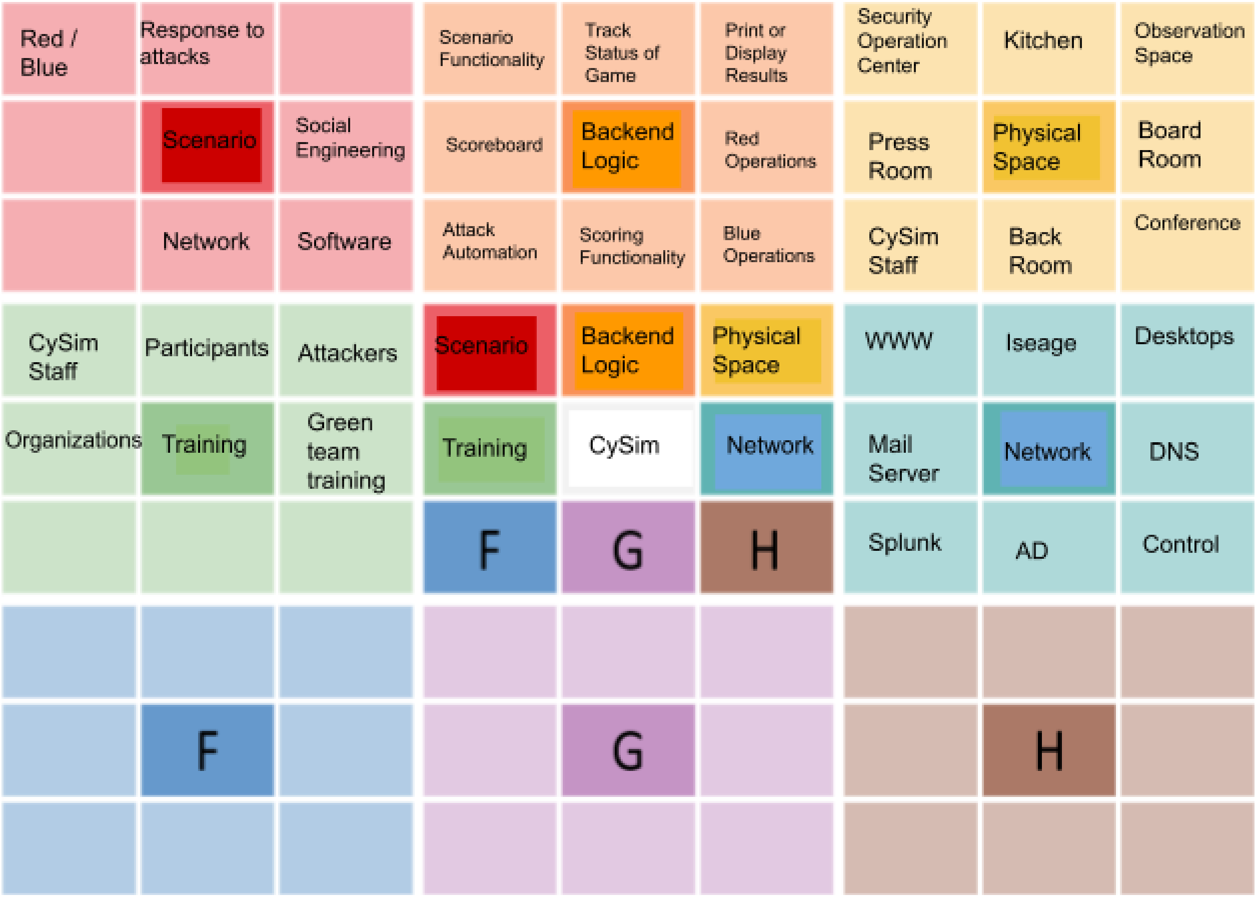
4.2.1 Design Decisions

List key design decisions (at least three) that you have made or will need to make in relation to your proposed solution. These can include, but are not limited to, materials, subsystems, physical components, sensors/chips/devices, physical layout, features, etc. Describe why these decisions are important to project success.

- **How are we going to automate (script) the games?**
    - One game mode that will be a part of CySim is the scripted games and events that will occur throughout the simulation. Because of this, we need to figure out how these will be scripted. This includes automating red team attacks and attack logs, as well as scripted events based off of blue team actions.
- **How/when will simulation feedback to the participants be triggered?**
    - Simulated feedback to give participants a feeling of real world effect based on events and actions that occur during the gameplay. We need to research and decide how and when these will take place in order to provide this experience to participants.
- **Will scripted feedback be part of only the CDC's, only scripted games, or both?**
    - Along with the previous question, we need to decide whether this simulated feedback system will be universal among all game types or reserved for specific ones such as scripted events. This is important, as simulated feedback is a large part of what makes CySim special as a cybersecurity training tool.
- **How will staff central control be handled? Webapp, program, etc.**
    - One important requirement is for the game master to have complete control over the cyber games, especially for scripted events. Because of this, we need to decide how they will interact with the game and control its flow in order to properly run the games.

4.2.2 Ideation

For at least one design decision, describe how you ideated or identified potential options (e.g., lotus blossom technique). Describe at least five options that you considered.



Red / Blue	Response to attacks		Scenario Functionality	Track Status of Game	Print or Display Results	Security Operation Center	Kitchen	Observation Space
	Scenario	Social Engineering	Scoreboard	Backend Logic	Red Operations	Press Room	Physical Space	Board Room
	Network	Software	Attack Automation	Scoring Functionality	Blue Operations	CySim Staff	Back Room	Conference
CySim Staff	Participants	Attackers	Scenario	Backend Logic	Physical Space	WWW	Iseage	Desktops
Organizations	Training	Green team training	Training	CySim	Network	Mail Server	Network	DNS
			F	G	H	Splunk	AD	Control
	F			G			H	

4.2.3 Decision-Making and Trade-Off

Demonstrate the process you used to identify the pros and cons or trade-offs between each of your ideated options. You may wish you include a weighted decision matrix or other relevant tool. Describe the option you chose and why you chose it.

For our Decision-Making and Trade-Off portion, we decided to use a weighted decision matrix

<table>
<tr><th></th><th></th><th colspan="4">Network Structure Options</th></tr>
<tr><th>Criteria</th><th>Weighting (Less 1-5 More)</th><th>ISEAGE Instance</th><th>Regular VMs</th><th>Physical Hosts</th><th>Participants Just Roleplay the Whole Time</th></tr>
<tr><td></td><td></td><td>Score | Total</td><td>Score | Total</td><td>Score | Total</td><td>Score | Total</td></tr>
<tr><td>Ease of Implementation</td><td>2</td><td>4 | 8</td><td>3 | 6</td><td>2 | 4</td><td>1 | 2</td></tr>
<tr><td>Resources Required</td><td>4</td><td>4 | 16</td><td>3 | 12</td><td>2 | 8</td><td>2 | 8</td></tr>
<tr><td>Maintainability</td><td>4</td><td>4 | 16</td><td>4 | 16</td><td>4 | 16</td><td>5 | 20</td></tr>
<tr><td>Ease of Automation</td><td>3</td><td>4 | 12</td><td>2 | 6</td><td>2 | 6</td><td>1 | 3</td></tr>
<tr><td>Scalability</td><td>2</td><td>5 | 10</td><td>2 | 4</td><td>1 | 2</td><td>5 | 10</td></tr>
<tr><td>Avoids Obsolescence</td><td>4</td><td>4 | 16</td><td>4 | 16</td><td>2 | 8</td><td>5 | 20</td></tr>
<tr><td></td><td>TOTAL:</td><td>78</td><td>60</td><td>44</td><td>63</td></tr>
</table>