Cyber-Protect: Reflection
Alexander Kellough

Scenario:
Cyber-Protect is a gamified exercise designed to demonstrate balancing budget and security allowing students to take the role of a security admin at a fictional corporation. Students participate in the exercise by purchasing and allocating security resources from a quarterly budget, and then being tested against simulated attacks. The exercise has been completed when an implementation gains a rating of 90%, meaning it is resistant against 90% of attacks.

Reflection;
I attempted this exercise three times before I completed it, and the two more afterwards in an attempt to maximize resilience. These were my takeaways:

Attempt 1;
My first instinct during this attempt was to try to harden the network interfaces as much as possible, as early as possible. While this seemed to work decently in the beginning, I quickly realized that internal threats would be a much bigger issue than I originally anticipated.

Attempt 2:
During this attempt I took a similar strategy to the first attempt, but applied it to the server. This found more success in general, especially when dealing with internal threats, but there were still some issues.

Attempt 3:
During this attempt, I focused on hybridizing the first two strategies, while also adding in an early focus on user training and redundant systems. Another observation that was made during the first 2 playthroughs is that you can upgrade deprecated systems. This means that it is arguably cheaper in the long run to upgrade a system rather than repair it, as it was likely to get upgraded anyway. Another realization that I made was that putting protections on employee computers was essentially wasted money. These “client-side” protections offered very little that the server couldn’t, while being much more expensive to deploy across all the systems.

Maximizing Attempts:
These attempts were made only to maximize the resilience of the strategy in the third attempt. During this attempt I had the most experience, as well as a good understanding of the pace of the game, and therefore the ability to make ideal choices.

Conclusion:
The main theme I found in this exercise was defense-in-depth. Poor quality protections could easily be made up for by breadth and layers, but lack of depth was a sure mistake. The second main theme I took away was the understanding that breaches are going to happen, so it is just as important to focus on damage mitigation, as it is damage prevention.