Nigel Adkins
February 18
CYSE 200T
Professor Duvall

Michael Morey, Three things that resonated with me

BLUF: Michael Morey talked about the importance of zero trust and how organizations have to assume that there is already a threat. He also explained that both penetration testing and red teaming both try to limit vulnerabilities. He also gave real life examples of how threats could exploit systems that are often thought of as a risk to exploit a system.

Zero trust

What resonated with me is when he talked about how there's zero trust given to anybody and how an organization assumes that there is already a threat in the network. He also talked about how everything is treated as hostile and then reviewed later. I found it interesting that he typed his pin 4 times while in the Navy to send an email. There are 7 pillars and 152 activities within zero trust. Least privilege, limiting access to the role of that person.

Red teaming and Penetration testing

He talked about how penetration testing and red teaming both try to limit vulnerabilities. They look to see how many ways there are to get into a system before the adversary and if they are already in they focus on how to limit their activity and get them out so that they can't do harm. He also said that there's a red teaming aspect to AI prompt inputs. There are a lot of different people and parts that can make up a village to raise a red team.

Example of threat

It was interesting when he gave an example of how someone could break into the heating system and how they could alter the temperature and make it say something that it's not so they could cause some sort of damage.

Conclusion; Michael Morey talked about some of the threats that networks often face and how Red teaming, penetration testing, and zero trust policies can limit the threats and vulnerabilities that a company can face and all the different ways that you can get involved.