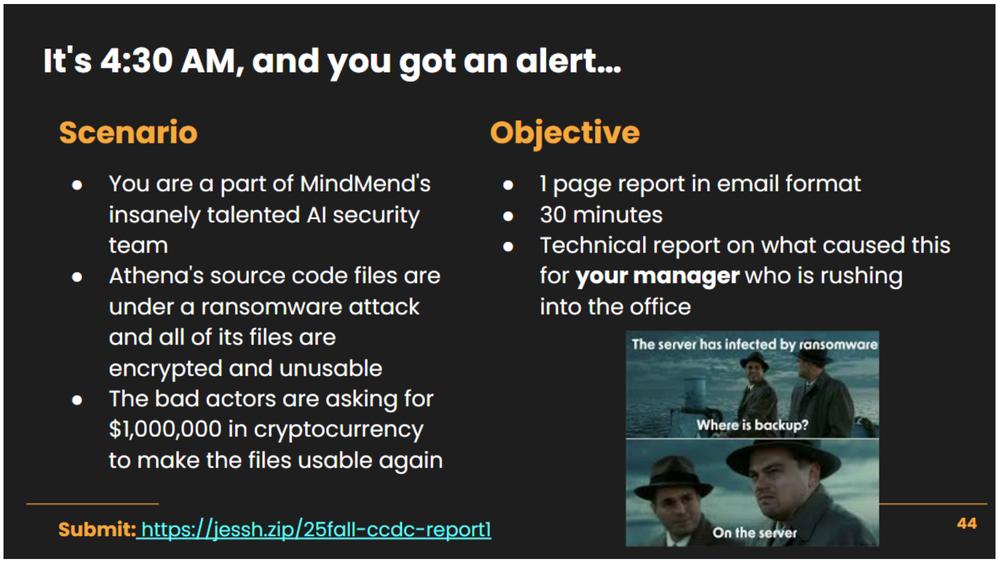
Homework 1

Business (50 points)

1. (25 points) Your inject responses for the two given during the week 2 meeting. If you missed the meeting or haven't otherwise done them, here they are (no need to submit to links in slides):



It's 4:30 AM, and you got an alert...

Scenario

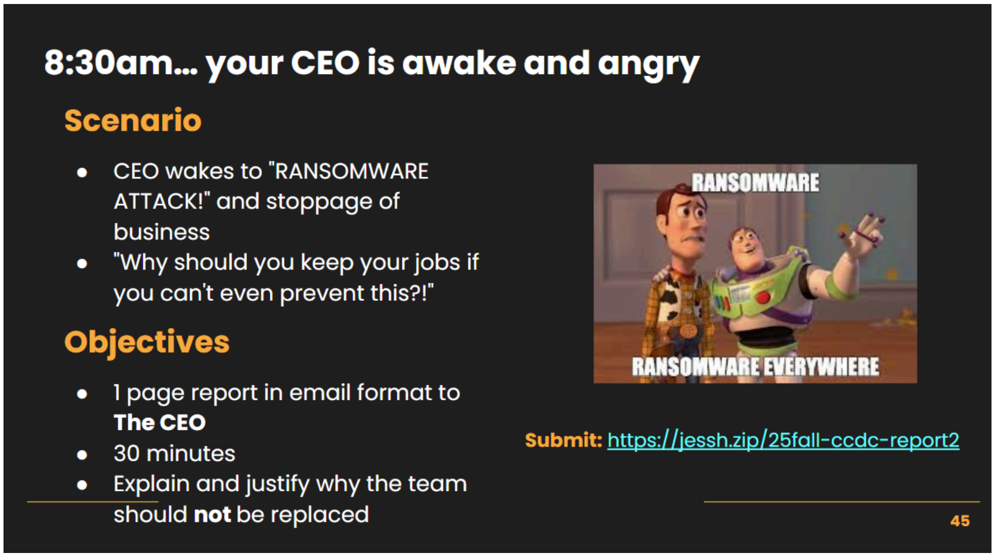
- You are a part of MindMend's insanely talented AI security team
- Athena's source code files are under a ransomware attack and all of its files are encrypted and unusable
- The bad actors are asking for $1,000,000 in cryptocurrency to make the files usable again

Objective

- 1 page report in email format
- 30 minutes
- Technical report on what caused this for **your manager** who is rushing into the office

Submit: https://jessh.zip/25fall-ccdc-report1

44



8:30am... your CEO is awake and angry

Scenario

- CEO wakes to "RANSOMWARE ATTACK!" and stoppage of business
- "Why should you keep your jobs if you can't even prevent this?!"

Objectives

- 1 page report in email format to **The CEO**
- 30 minutes
- Explain and justify why the team should **not** be replaced

RANSOMWARE
RANSOMWARE EVERYWHERE

Submit: https://jessh.zip/25fall-ccdc-report2

45

Remember the important aspects of a good inject response: Good formatting, professional language, answer all parts of the inject, provide evidence (sources, screenshots, graphics)

2. (25 points) ANOTHER INJECT

Greetings freshmeat intern,

Our cybersecurity team has recently set up something called a SentinelOne EDR solution on many of the company's workstations and servers as a result of the devastating ransomware attack on our beloved Athena. Something about "Ending Disruption and Reacting" or something. An attack like that better not happen again or you dimwits all are fired. I need to have an actually good security team. They told me that this will improve the security of our computers, but an actual explanation as to why this will protect us from another ransomware attack would be nice.

Additionally, I want to know if this is the best security response software for our company. You guys need to make our systems more secure. That's literally why you nerds were hired. Please look into at least two of these EDR solutions and compare them to our current one. Tell me which one is best and why.

In the process of getting our company back under control and Athena safely back into our hands, one of your coworkers also mentioned something called a SIEM. Can you explain what this is and how is it different from an EDR?

Give me all of this information in the next hour. I have a meeting with my CEO friend and I need to impress them with my knowledge.

Athena Johnson
Your CEO

Networking (50 points)

Please show documentation where needed.

1. Go to kamino.sdc.cpp and clone CCDC_Fall_Networking.
2. There are three VMs in your pod:
   a. **pfsense router: 1-1NAT-pfsense**
   b. **Windows 2016: Hippocampus**
      i. Creds - Administrator : CCDC2025!
   c. **Windows 10: Client**
      i. Creds - Administrator : Password123
   d. Ensure they are all on.
3. (5 points) Change the IP address of the Hippocampus to 192.168.1.37.
4. (5 points) Find the IP address of the Client.
5. (20 points) On Hippocampus, there are two websites that host a file each. Access the websites from the Client. Take a screen of the websites; be sure to include the URLs.
6. (20 points) One of those websites is not meant for business purposes.
   a. Use Powershell to enable all the windows firewall profiles, set the default inbound policy to block, and add an allow exception for the business web server's port. Submit screenshots of (1) the firewall commands used, along with (2) a screenshot showing you are no longer able to connect to the blocked website from the Client.

Deliverables:

PLEASE SAVE ALL INJECT RESPONSES IN SEPARATE PDFs.
SAVE THE NETWORKING HOMEWORK IN A SEPARATE PDF.
ZIP ALL OF THE PDFs AND NAME THE ZIP FILE "firstinitialLastname-hw1ccdc.zip", AND SUBMIT THE ZIP FILE.