Business Injects

Deliverables:

1. 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):

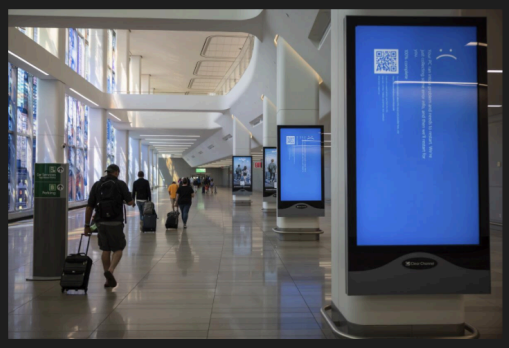
It's 2:00am... you just got paged...

Scenario

- You work in the SOC at a bank
- Crowdstrike update went wrong
- 200 Windows machines are bricked

Objectives

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



Submit: https://jessh.zip/week2-1

33

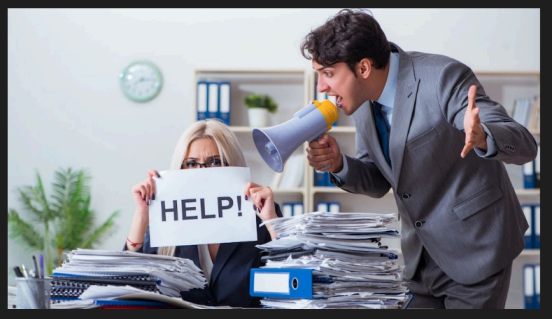
8:30am... your CEO is awake and angry

Scenario

- CEO wakes to frozen transactions and stoppage of business
- "Why are we paying for a tool that destroyed our business?!"

Objectives

- 1 page report
- 30 minutes
- Explain and justify the usage of an EDR **to your C-Suite**



Submit: https://jessh.zip/week2-2

34

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. ANOTHER INJECT (Now you are at a marine touring company, not a bank):

   Dear IT/Security Team,

   We've recently added EDR solutions to many of our company workstations and servers. I still don't really get what they do but I've been told they will make our computers more secure. I was recently talking with some CIOs of other companies at a business conference recently and one of them mentioned using a SIEM and how they are so great. I want you to look at at least 3 different SIEMs and get back to me on which one you think would be best for our company and why. Also, it would be nice if you could explain what a SIEM is, and the difference between a SIEM and an EDR.

   Thanks!
   Joe Marine
   Your Boss

PLEASE SAVE ALL RESPONSES IN SEPERATE PDFs, ZIP THEM, NAME THE ZIP FILE "firstinitialLastname-hw2ccdc.zip", AND SUBMIT THE ZIP FILE.