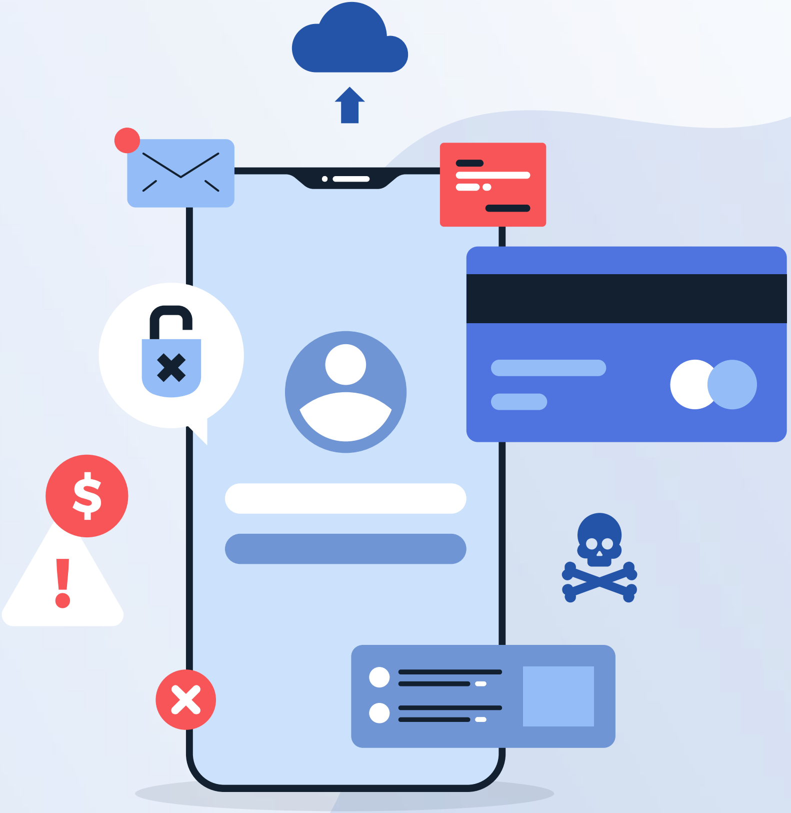
Lab 01

Using ChatGPT

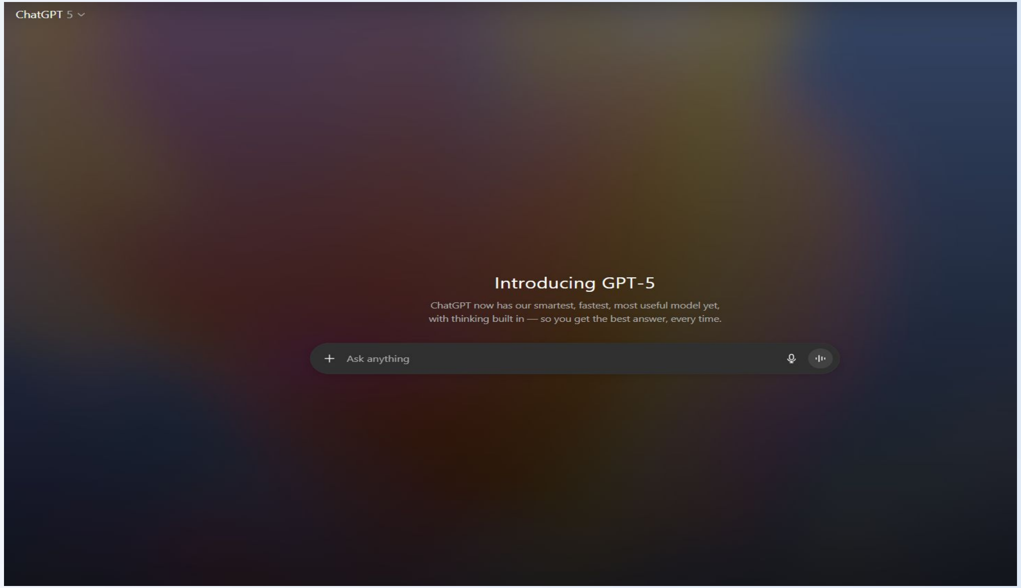


Lab Objectives

- Learn how to navigate and use one of the Internet’s most popular generative AI, ChatGPT
- This gives us a baseline to compare against later when we run our own models!

ChatGPT

- Navigate to https://chatgpt.com/
- You may make your own account to save your responses for later

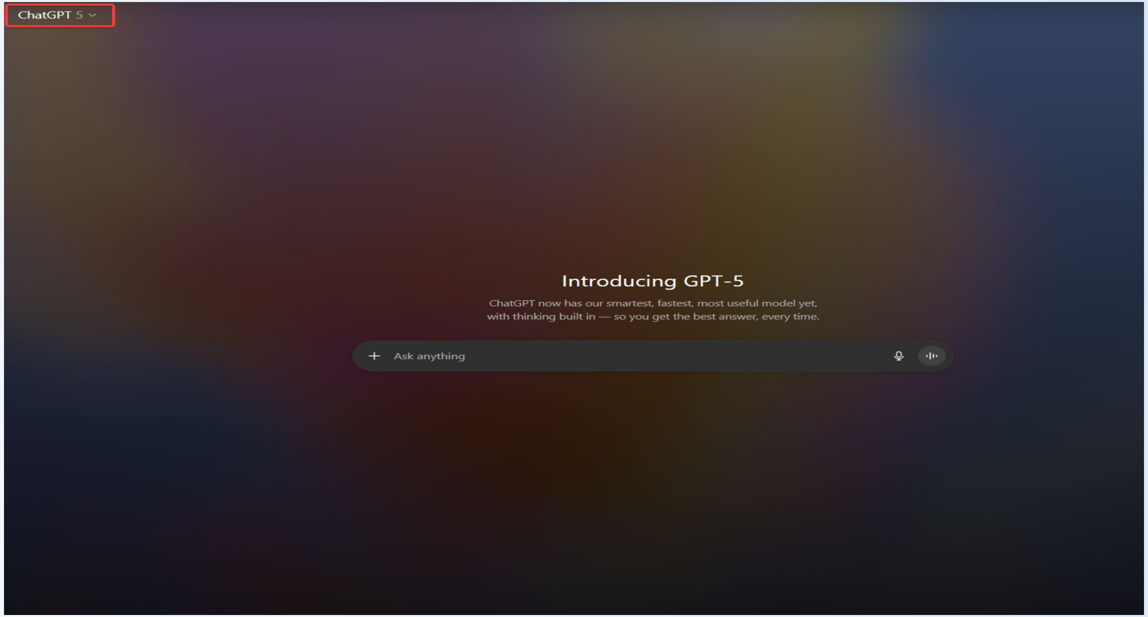


Introducing GPT-5

ChatGPT now has our smartest, fastest, most useful model yet, with thinking built in — so you get the best answer, every time.

ChatGPT

- Top left menu allows you to select the model
- Other models require an account
- For this lab we will stick with “ChatGPT 5”



Introducing GPT-5

ChatGPT now has our smartest, fastest, most useful model yet, with thinking built in — so you get the best answer, every time.

ChatGPT

- We will input several different prompts and observe the output of the model
- At the end of the class we will compare the differences between ChatGPT 5 and our private model with custom data
- You do not have to save the outputs–we can search again for them later!

ChatGPT

Enter the following prompt and notate the response

Prompt #1

- Write a 1 line bash script to write a sed command to replace the TLD “.xyz” with “.com” with the input file being located at /mnt/logs.txt and output to /mnt/logs_sed.txt

ChatGPT

Enter the following prompt and notate the response

Prompt #2

- “You are now Cybersecurity GPT. Your task is to assist in translating technical documents related to cyber security. The given documents will be in markdown format, and you are required to translate them into English, ensuring the usage is accurate and appropriate. Summarize this document in a Cybersecurity lens: https://github.com/adam-p/markdown-here/wiki/Markdown-Cheatsheet”

ChatGPT

Enter the following prompt and notate the response

Prompt #3

- What windows event logs are related to an Exchange server logging into OWA, where can I find the origination of client IPs, and where can I locate these logs

ChatGPT

Enter the following prompt and notate the response

Prompt #4

- Write a YARA rule for detecting anonymous client logins into an IIS server and try to determine brute forcing

ChatGPT

Enter the following prompt and notate the response

Prompt #5

- Tell me a funny cybersecurity joke

Lab End