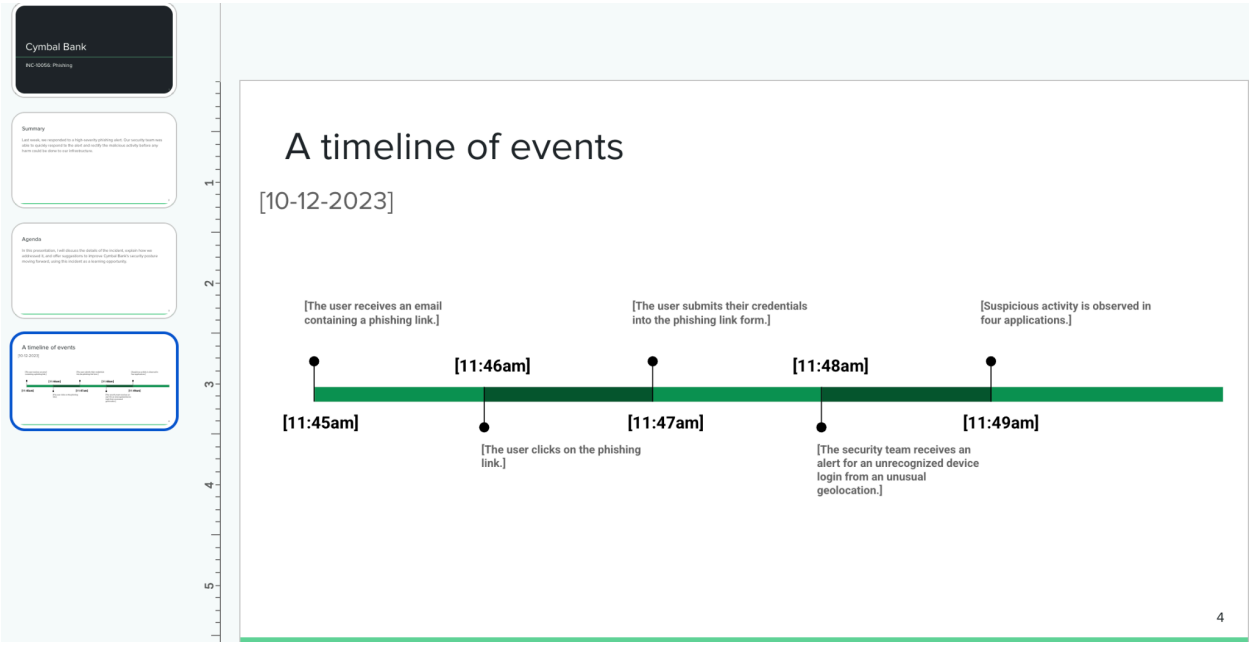
Course 4_Activity 1: Document a timeline of events

My Work:



My Assessment:

In this activity, the primary goal was to arrange a sequence of events related to an incident in order based on time of occurrence. The scenario highlights an individual that was not aware of a phishing attack by a threat actor attempting to obtain the user's login credentials. By clicking the link and sharing their credentials, the threat actor successfully gained unauthorized access to the system. In this case the specific vulnerability is rooted in employee training and development, which is related to a weak security posture. The security team should not only implement regular training and development, but they should also implement multi-factor authentication within their Identity and Access Management tool within their CSP (cloud service provider), instruct the user to change their credentials, while also reviewing SIEM logs for any suspicious login activity. In addition, the security team must report the attack, and the team should also consider implementing email security measures and contain any breaches if necessary.

Google Answer: