View the "Lab 2 Opensource Intelligence" video within the "Video Playlist: Penetration Testing and Risk Management," located in the topic Resources.  
The use of the Maltego tool allows for the gathering of passive data across various platforms in order to better prepare an attacker to exploit a system. Utilizing this tool, as well as the OSINT framework, do the following:

* Research a Fortune 500 Company and one of its C-suite officers to extract as much passive data as possible in order to prepare your team to carry out a pending pen test of their systems.
* Present the findings of your attack surface discovery to your team through a video or streaming service 3-5 minutes in length. Define the stage of cyber operations in which you are currently operating. Your video should include screenshots and an examination of attack vectors that you will use to proceed with active recon.
* Once you have identified your prospective target, create a Spear Phishing Email to target someone within the organization you have researched, utilizing the information you gained. Present your attack in your video presentation, describing why and how you believe it would be effective. (**DO NOT SEND** this attack. It is a violation of the code conduct at GCU.)
* Explain, from a Christian perspective, the legal authorities and ethical considerations that must be taken into account when conducting such an attack as part of a penetration test.

APA style is not required, but solid academic writing is expected.

This assignment uses a rubric. Please review the rubric prior to beginning the assignment to become familiar with the expectations for successful completion.

You are not required to submit this assignment to LopesWrite.