**Log Analysis Take-Home Technical**

1. Download Splunk for free from <https://www.splunk.com> by creating a new account and using the software download option.
2. Once Splunk is installed, add the logs provided to it and use the available options to see the raw log data.
3. Determine what, if any, information is atypical or might indicate an attack occurred. Some examples (these MAY or MAY NOT be present):
   1. an external IP address attempting to communicate with the firewall that comes back as malicious when using open source intelligence (OSINT) tools like VirusTotal or AbuseIPDB
   2. a user attempting and failing to authenticate many times in a short timeframe
   3. signs of data being exfiltrated
4. Prepare a summary of the results of your investigation to present to the team. Things to include: investigation findings, steps taken to find information, and any conclusions the information allows you to draw. This presentation will be in either document or slideshow format (i.e. Word, PowerPoint). You will need to demonstrate what you found, how you found it, AND what it means in terms of cybersecurity. An example:
   1. If you were to find 5 failed authentications spread out over about a minute, you would show us how you found the failures. Then, put it into context of cybersecurity. In this example, 5 failures over a minute looks like a forgotten password and without further evidence of anything malicious, wouldn’t suggest any compromise.
   2. If you were to find 5 failed authentications spread out over a minute but that the login attempts came from outside the network and on an administrator account, you would show us that information and then draw the conclusion that the activity may show some sign of compromise and should be investigated further.

Use any resources at your disposal to learn how to use Splunk and gain relevant information from the logs provided! Splunk’s website has resources, but there are also YouTube videos, articles, etc. that will provide valuable insight into this tool.

For your presentation, please do not include definitions for any terms used. Keep the presentation concise but make sure it adequately covers everything you find and presents in an organized manner. You can include screenshots or use the live Splunk instance if you would like to draw emphasis towards any specific searches or data found. You will be displaying this to the team via screen sharing in Teams!