Instructions

1. Add the sample web log data to Kibana.

2. Answer the following questions:

    - In the last 7 days, how many unique visitors were located in India?
      245
    - In the last 24 hours, of the visitors from China, how many were using Mac OSX?
      10 25%
    - In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?
      0-404 errors 0-503 errors
    - In the last 7 days, what country produced the majority of the traffic on the website?
      US
    - Of the traffic that's coming from that country, what time of day had the highest amount of activity? 10am
    - List all the types of downloaded files that have been identified for the last 7 days. Css, deb, gz, rpm, and zip.

3. Now that you have a feel for the data, Let's dive a bit deeper. Look at the chart that shows Unique Visitors Vs. Average Bytes.

    - Locate the time frame in the last 7 days with the most amount of bytes (activity).
    - In your own words, is there anything that seems potentially strange about this activity?

      high amount of bytes and only 1 individual IP is creating alot of traffic.

4. Filter the data by this event.

    - What is the timestamp for this event? 2021-6-12 2157 hours
    - What kind of file was downloaded? Css files
    - From what country did this activity originate? Indonesia
    - What HTTP response codes were encountered by this visitor? 220 error code
5. Switch to the Kibana Discover page to see more details about this activity.

    - What is the source IP address of this activity?
    - What are the geo coordinates of this activity?
    - What OS was the source machine running? Windows 8
    - What is the full URL that was accessed?
    - From what website did the visitor's traffic originate?
6. Finish your investigation with a short overview of your insights.

    - What do you think the user was doing?
    - Was the file they downloaded malicious? If not, what is the file used for?
    - Is there anything that seems suspicious about this activity?
    - Is any of the traffic you inspected potentially outside of compliance guidlines?