### **Instructions**

**Note: Performed this activity on 11/2, so answers may differ due to updated sample log data.**

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?

**There were 249 unique visitors located in India.**

* + In the last 24 hours, of the visitors from China, how many were using Mac OSX?

**There were 7 visitors from China in the last 24 hours who were Mac OSX users.**

* + In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?

**Over the last 2 days, 6.667% of visitors received 404 errors, while 0 percent received 503 errors.**

* + In the last 7 days, what country produced the majority of the traffic on the website?

**Over the last 7 days, China produced the majority of the traffic on the website.**

* + Of the traffic that's coming from that country, what time of day had the highest amount of activity?

**Out of the traffic from China, the 1300 hour (or 1pm) had the highest amount of activity.**

* + List all the types of downloaded files that have been identified for the last 7 days, along with a short description of each file type (use Google if you aren't sure about a particular file type).
    1. **css file type - stands for cascading style sheet, and is used to format web pages**
    2. **deb file type - debian software package**
    3. **gz file type - compressed archives created by the GNU zip (or gzip) compression algorithm.**
    4. **rpm file type - Red Hat Package Manager file**
    5. **zip file type - .zip compression archive**

1. 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?

**One visitor generated a large amount of traffic within a short period of time.**

1. Filter the data by this event.  
   * What is the timestamp for this event?

**Oct 24, 2021 at 22:57:28 hours**.

* + What kind of file was downloaded?

**The visitor downloaded an RPM file.**

* + From what country did this activity originate?

**The United States.**

* + What HTTP response codes were encountered by this visitor?

**This user encountered an HTTP 200 OK response code**

1. Switch to the Kibana Discover page to see more details about this activity.  
   * What is the source IP address of this activity?

**Source IP was 35.143.166.159**

* + What are the geo coordinates of this activity?

**"lat": 43.34121, "lon": -73.6103075**

* + What OS was the source machine running?

**The source machine was running Windows 8**

* + What is the full URL that was accessed?

**https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm**

* + From what website did the visitor's traffic originate?

**The visitor’s traffic originated from Facebook.**

1. Finish your investigation with a short overview of your insights.  
   * What do you think the user was doing?

**The user was downloading an metricbeat install package for a distribution of Red Hat Linux.**

* + Was the file they downloaded malicious? If not, what is the file used for?

**The file is not malicious, metricbeat is used to collect metric data from servers.**

* + Is there anything that seems suspicious about this activity?

**No, because metricbeat is a tool used by cybersecurity professionals to monitor the health of servers.**

* + Is any of the traffic you inspected potentially outside of compliance guidlines?

**No.**