Exploring Kibana

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?

231

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

14 (28%)

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

404: 0% | 503: 7.143%

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

China

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

12pm (38)

* + 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).

CSS - this is a programming language usually used for writing webpage elements and design

DEB - compressed Linux software package, used by debian-based distros like ubuntu

GZ - compressed archive using the gzip compression algorithm

RPM - similar to deb files, these are compressed linux software packages used in Red Hat Enterprise based distributions

ZIP - compressed archive similar to tarball or gz 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).

Chart, bubble chart

Description automatically generated

* + In your own words, is there anything that seems potentially strange about this activity?

Yes, for such high activity, the number of unique visitors was very low especially compared to other timeframes when the bytes/activity was lower.

1. Filter the data by this event.
   * What is the timestamp for this event? 2022-02-19 06:00
   * What kind of file was downloaded? deb, gz
   * From what country did this activity originate? China
   * What HTTP response codes were encountered by this visitor? 200
2. Switch to the Kibana Discover page to see more details about this activity.
   * What is the source IP address of this activity? 243.233.91.124
   * What are the geo coordinates of this activity? lat: 38.66187028, lon: -90.65123
   * What OS was the source machine running? iOS
   * What is the full URL that was accessed? https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.3.2.deb
   * From what website did the visitor's traffic originate? http://www.elastic-elastic-elastic.com/warning/taylor-wang
3. Finish your investigation with a short overview of your insights.
   * What do you think the user was doing? Downloading a software
   * Was the file they downloaded malicious? If not, what is the file used for?

Without looking at the file or the software that is being downloaded/updated, it doesn’t seem malacious.

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

No?

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

No?