1. Add the sample web log data to Kibana.

Graphical user interface, application

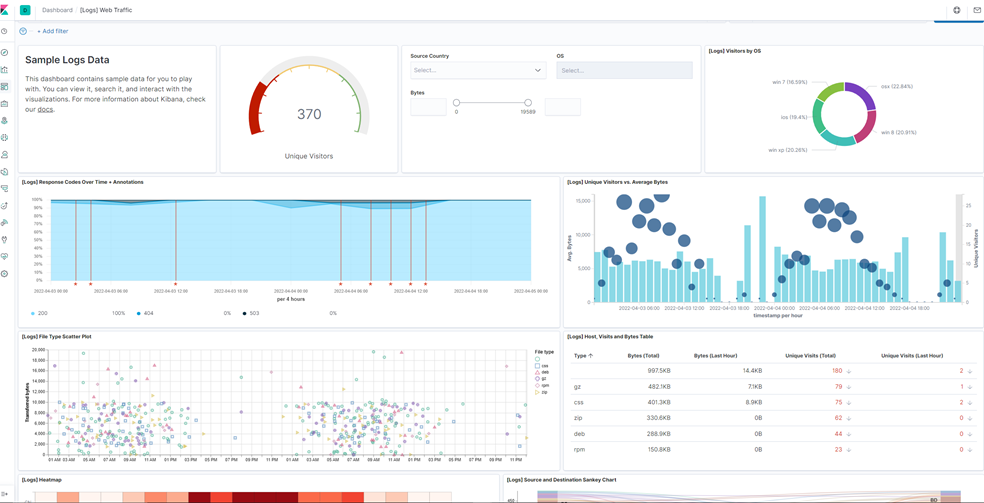
Description automatically generated

1. Answer the following questions:
   * In the last 7 days, how many unique visitors were located in India?

Chart

Description automatically generated with medium confidence

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



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

404 errors: 0%

503 error: 7.143%

A picture containing graphical user interface

Description automatically generated

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

China

A picture containing background pattern

Description automatically generated

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

10AM

Chart, bar chart

Description automatically generated

* + 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: a programming language that is used for writing webpage elements and design

Deb – a compressed linux software package that is used by Debian-based distros

Gz – a compressed archive using the gzip compression algorithm

Rpm – a compressed linux software package that’s used in red hat enterprise-based distributions

Zip – a compressed archive

Chart, scatter chart

Description automatically generated

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).

Avg bytes is 15,709 and 1 unique visitor

Chart

Description automatically generated with medium confidence

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

Something that is strange about this activity is that the number of unique users is unusually low unlike other times

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

22:50

* + What kind of file was downloaded?

rpm

* + From what country did this activity originate?

India

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

200

Graphical user interface, application

Description automatically generated

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

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?

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?

http://facebook.com/success/jay-c-buckey

Text

Description automatically generated with medium confidence

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

User was downloading rpm file

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

There’s a high possibility that it is not malicious as the file they used (eleastic.co) to download was related to designing websites

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

No, there is nothing suspicious about this activity. The person visiting the webpage might just be a regular user visiting a webpage.

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

No, this seems normal.