|  |  |
| --- | --- |
|  |  |
|  | --- |
|  | ### 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? 249 |
|  |  |
|  | - In the last 24 hours, of the visitors from China, how many were using Mac OSX? 19.23% |
|  |  |
|  | - In the last 2 days, what percentage of visitors received 404 errors? 7.692% How about 503 errors? 0% |
|  | - In the last 7 days, what country produced the majority of the traffic on the website? CN China |
|  | - Of the traffic that's coming from that country, what time of day had the highest amount of activity? 13-14:00 |
|  | - 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). |
|  | Ccs- cascading style sheet- it’s used to format the contents of a webpage |
|  | Deb- debian- it’s a standard Unix archive that contains 2 biozipped archives, one for the installer and another for actual installable data. |
|  | gz- gzip- archive file compressed by the standard GNU zip compression algorithm |
|  | Rpm- Red Hat Package Manager- is a free and open-sourced package management system |
|  |  |
|  |  |
|  | 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). 91:55 |
|  | - In your own words, is there anything that seems potentially strange about this activity? They bytes are way high for one count |
|  |  |
|  | 4. Filter the data by this event. |
|  | - What is the timestamp for this event? 21:55 |
|  | - What kind of file was downloaded? Rmp file |
|  | - From what country did this activity originate? IN India |
|  | - What HTTP response codes were encountered by this visitor? 200 |
|  |  |
|  | 5. 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?win 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? Facebook |
|  |  |
|  | 6. Finish your investigation with a short overview of your insights. |
|  |  |
|  | - What do you think the user was doing? Getting packages |
|  | - Was the file they downloaded malicious? If not, what is the file used for? Yes |
|  | - Is there anything that seems suspicious about this activity? He is getting suspicious packages from facebook |
|  | - Is any of the traffic you inspected potentially outside of compliance guidlines? Noncompliant to facebook compliant |
|  |  |
|  | --- |
|  | © 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved. |