DSS Visualizer Top Level Requirements

## Description.

The DSS Visualizer system is an application that can present evaluator information in a graphical and easy to understand manner to researchers. An evaluator is defined as an individual who is conducting a cyber security penetration test or exercise. The evaluator could be a student or a security professional. These graphical visualizations will allow researchers to gain better insight pertaining to the actions of evaluators during cyber security events. This system receives data from the ECEL system and is responsible for visualizing the data in an intuitive manner. Data generated by ECEL includes evaluator keypresses, mouse clicks, timed/manual screenshots, system function calls, and network traffic data (both throughput and packet information). This tool will allow researchers to better understand cyber security incidents from the evaluator point of view and will eventually be used in order to better train cyber security professionals and students.

## Top Level Requirement.

* The system shall be capable of functioning standalone or as a plugin for Intel Bucket.
* The system shall be capable of importing, exporting, and visualizing ECEL data including:
  + Keypress Data
  + Mouse Click Data
  + Screenshot Data
  + Traffic Throughput Data
  + Traffic Packet Data
  + System Function Call (Snoopy) Data
* The system shall be capable of visualizing ECEL data in multiple different ways. The following visualization types must be supported by the system:
  + Timeline Graphs
  + Frequency Graphs
* The system will have a plugin architecture.
  + The plugin architecture shall support the following types of plugins:
    - Visualization Plugins – Provide different ways to visualize ECEL data.
    - Library Plugins – Provide dependencies for other plugins.
    - Datasource Plugins – Provides a mechanism to change how a standalone configuration stores ECEL data on the host workstation.
* In a standalone configuration, the system shall be responsible to storing ECEL data. In a plugin configuration, the Intel Bucket shall be responsible for storing data.
* The system shall work cross platform. The following platforms must be supported by the system:
  + Kali Linux
  + Windows 7, Vista, and 10