Red Canary Endpoint Assignment

**Introduction**:

This document is to describe the project that I’ve put together for the assignment that I’ve received from Red Canary toward endpoints. Below you’ll find description of how it works.

**Architect**:

I’ve written this program in Python (since that’s the language I’m more familiar with). There are five classes each doing a specific purpose:

LoggerProvider.py: This class is to create & set the logging mechanism

PlatformEndpoint.py: This is for platform specific actions. For example, in windows calling a process might be different than in Linux.

DataTransmitter.py: This class is use to create the socket & transmit the data to specific destination and port.

ArgParseProvider.py: This class is used to get the arguments passed in with the main program. I wanted to use the argparse module provided with python, but I had some issues modifying some custom fields.

Endpoin.py: This is the main program. This is the class that calls all the other classes as needed.

**How it works**:

* User can run python Endpoint.py help to get a list of actions that they can perform. There are examples at the bottom of this print statement.
* Here are some of the actions that can be performed:
  + to start a process:
    - python Endpoint.py process [processPath] [processCmdArgs]
  + to create a file:
    - python Endpoint.py file create /usr/local/bin/test.txt
  + to modify an existing file:
    - python Endpoint.py file modify /usr/local/bin/test.txt "hello world"
  + to delete a file:
    - python Endpoint.py file delete /usr/local/bin/test.txt
  + to transmit data:
  + python Endpoint.py transmit 192.168.1.23 443 [b'data1 to send']
* Logging:
  + When a user requests a specific action other than help:
    - It’ll create a file.log
    - Each action performed will be added to the file.log following the instructions from the assignment.

**Improvement**: There are always room for improvements☺.