WARNING: Save and close all Excel documents prior to running this script

Prerequisites: ACTIVATED version of Excel 2016

1. Install Powershell 7, leave all options default (Click next through everything)
2. Open Powershell 7-Preview (Can be found in the start menu under the powershell folder)
3. In the Powershell prompt navigate to the location of the script (output file will also show up here)
4. Run the script
5. Select spreadsheet with IOCs
6. Rename the output file (must be a .rules file/end in .rules)
7. Place file in /etc/suricata/rules on Suricata server (script uses SIDs in the 5 and 6 million range, if this conflicts with other rules in Suricata look for the comment in the script with \*\* at the end and change the 2 lines under it)
8. Run “suricata-update --local /etc/suricata/rules”
9. Check rules by running suricata -c /etc/suricata/suricata.yaml -i em1 (em1 is the sensor interface used in every dmss multi node build)

\*\*\*May have to change permissions on fast.log and eve.json to -rw-rw-rw- (666)