rsyslog setup (For Linux):

1. Install rsyslog with sudo apt install rsyslog
2. Check rsyslog is installed with rsyslogd -v (Should output version info)
3. Check the service is running with systemctl status rsyslog

* If not running, run it with sudo systemctl start rsyslog

1. Access rsyslog configuration file with sudo nano /etc/rsyslog.conf
2. Jump to around lines 16-22 (Should start with “# provides UDP syslog reception”) and uncomment the lines for module and input (imudp = UDP, imtcp = TCP)

* Both TCP and UDP can be configured by uncommenting both sets of 2 lines

1. Add these lines to the beginning of rsyslog.conf:

*$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"*

*\*.\* ?RemoteLogs*

*& ~*

* Make sure the service is enabled through the firewall (if using ufw, run sudo ufw allow 514/tcp; service enabled through rfw by running sudo ufw allow 514/udp)

1. Restart rsyslog after configuration changes by running sudo systemctl restart rsyslog.service

Windows Event Viewer (eventvwr in cmd) works for Windows, but the best approach is to use Splunk (works across the network)