Notes:

- Log collector is a centralized device - Could be security onion
- There may be multiple IDSs in different locations in your network, like hospital, mod team, clinic
- Fire up a security onion ISO
- How to setup security onlin
    a. Double click on the setup
    b. Run ifconfig to find the subnet mask and static IP, put them in the dialob box of setup
    c. DNS server can be 127.0.0.1
    d. Interface can be eth1, interface you want to monitor
    e. Then restart, click again the setup button after there machine reboots
    f. Click on production mode
    g. Choose best practices
    h. Choose snort or suricata, whatever you like
    i. Set PF_RING_min_num_slots to… NIC interface max throughput, PF_RING sets up bucket size so that you do not drop packets if your in is faster than your out, leave it as is
    j. Select proper interface (eth1)
    k. HOME_NET: set it to the PROPER CIDR and home address
    l. Last screen: copy that into a notepad, these are useful services to check (sudo sostat quick …)