Network Isolation Procedure

1) Create a virtual network with a static IP address and configure DHCP
2) MAYBE enable static routing to have a route to communicate with the internet. Only do if necessary to install tools, pull repo, etc.
3) Deny inbound traffic on all the ports apart from the “Mandatory Ports **(SSH (only allow inbound connections, not outbound), Scoring Engine)”**
4) SOC will keep looking at the logs to understand the attack vector and we could work on bringing the machine back up (Cleaning the machine by deleting any changes the attacker would’ve made etc)
5) Take account as to WHO is connected to the machine using the “who” command on Linux. Check these logs to see who is SSH’d into the machine.
6) Make a machine-network snapshot script
    a) Who is logged in
    b) Use netstat with tulpn to check for which ports were opened in the case of a reverse shell
        i) Can also just see if there’s some port that we missed.

Docker Containers

1) Create a private docker network and move the container to that network to keep working on it and fixing the machine