# Cyber Security Questions/Flags:

1. Complete the setup of the sensors via the documentation provided by AQL

   _____

2. Once you are on the qomodo platform, you will now see a string of alerts on the qomodo platform which look to be some kind of ‘suspicious’ or ‘malicious’ network connection. What IP address is related to the malicious connection?

   _____

3. Look at the IP address above and identify the malware OR campaign to which this IP address is related to. Question: What nation-state do we think could be behind the attack?

   _____

4. When a device is connected to a ‘command and control’ (c2) server, this is typically initiated by a payload that has compromised the device. A payload, whether malicious or benign, is given a unique ID or a hash. The hash is like a digital fingerprint, created automatically by special software, to help identify and track files. What is the device ID of the infected device in this campaign?

   _____

5. A payload, or malicious activity is usually carried out first by actually gaining access to the device, typically through a vulnerability. Now you know the malware name, the nation-state involved and you have some of the indicators of compromise - what was the likely vulnerability that was exploited in the compromised device? Provide the CVE number.

   _____