

Capture the flags

1

Set up sensors and access

Follow Instructions to get the sensors set up, and your qomodo platform access

2

Something bad is going on

There are frequent alerts that have occurred due to the traffic from the sensors you have set up. Let's investigate - what is the malicious IP address in question?

3

Who could be targeting us?

What nation-state or country could be behind this attack on us?

4

How did this happen?

When a device is compromised, control is typically gained through a malicious payload. Search the platform for this payload and confirm the device-ID

5

How did they get in?

What vulnerability was used to exploit this device? We want a CVE number.

**Any questions,
raise your hand!**