An unknown device is connected to the company's internal network

**You are asked to investigate an alert related to an unknown device that is connected to the company's internal network.**

**After you complete your investigation, you follow company policies and procedures to implement preventative measures that will stop the potential threat posed by the device.**

We would start an investigation, taking into account the following assumptions.

* Review if that device really belongs the company inventory.
  + In case it does, then we can review if there is either an application or program that is trying to run when we connect that device.
  + In case it does not, then we can suspect and investigate about that device, where it came from.
* Review if there is any process or service that starts or stops running. We could identify that process/service using command lines such as Bash Scripting or Windows Batch Scripting. We can get a list of all the processes/services which are running in the operating system background.
* Review the current polices that the company is using to see if that devices belongs to the list of allowed devices by the company.
  + In case it does, then we can continue with the steps mentioned previously.
  + In case it does not, then we can investigate why that specific device was used when actually it should not be used by policy company.