## **Scenario**

## 

## Review the following scenario. Then complete the step-by-step instructions.

## You are part of the security team at Rhetorical Hospital and arrive to work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. There’s no one else around who might have dropped it, so you decide to pick it up out of curiosity.

## You bring the USB drive back to your office where the team has virtualization software installed on a workstation. Virtualization software can be used for this very purpose because it’s one of the only ways to safely investigate an unfamiliar USB stick. The software works by running a simulated instance of the computer on the same workstation. This simulation isn’t connected to other files or networks, so the USB drive can’t affect other systems if it happens to be infected with malicious software.

## 

## **Parking lot USB exercise**

| **Contents** | Write **2-3 sentences** about the types of information found on this device.  There are files which contain the PII in the USB stick.  There are some work files like shift schedules and employee schedules. It is not safe to store personal and work files together in any medium. |
| --- | --- |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.  The information could be used against the other employees as it contains PII. The information could also be used against the family members or the relatives of the employees.  The information could barely provide any access to the business. |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:  The first thing we should do after discovering any software like this is create a virtual environment to isolate it from the rest of the organization network.  If other employees have discovered any device like this then there are chances that the employee could have connected to his/her work computer to check its files which could have led to serious problems to the organization’s network and systems.  Threat actor could find sensitive information like the work timings of a particular employee  The sensitive information might be used against the employees or their relatives. |