## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | *The information found on this device contains PII and sensitive work files. It is not safe to mix personal files with work files as it compromises the security of sensitive and private work information.* |
| **Attacker mindset** | *The information in the USB can be used to gain access to sensitive work schedules, private resumes, and a hiring letter (which may contain sensitive company information). Additionally, this information can be used against Jorge as a form of blackmail or a hacking bluff to scare Jorge into revealing more sensitive information. The USB drive could also contain malware, so by Jorge using the device personally and at work, he could be unknowingly compromising company assets.* |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:   * *What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?* * *What sensitive information could a threat actor find on a device like this?* * *How might that information be used against an individual or an organization?*   *Self-reproducing software as well as RATs can be hidden on these type of devices which, if connected, could provide access to sensitive company and employee data which could be used for malicious purposes. On top of that, a threat actor could find sensitive personal or professional information related to Jorge, or important company operations information like work schedules. This information could be used against the company in the form of a ransomware attack, or potentially against Jorge in the form of blackmail.* |