## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | Write **2-3 sentences** about the types of information found on this device.   * *Are there files that can contain PII?* * *Are there sensitive work files?* * *Is it safe to store personal files with work files?*   The PII is present in several personal and work-related files (Wedding list, and JB\_Resume).  SPII of employees is also present in some other work files (Employee budget, and Shift schedules).  It isn’t safe storing personal and work files together. In the wrong hands, this would give a threat actor too much information to use on a wide attack surface through different vectors and tactics. |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.   * *Could the information be used against other employees?* * *Could the information be used against relatives?* * *Could the information provide access to the business?*   There is information that can also be used against relatives and other employees. For instance, with the provided information for new hires and the employee shift schedule, a threat actor could impersonate and gain access to the organization. |
| **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?*   On the wrong hands, the contents of the USB could be replaced by malicious software to infect the network or take control of the machine where it’s plugged. If this USB was discovered through USB baiting by another employee, there would be a high probability to trigger this malicious software.  The information found in the device could be used against JB and the organization. There is enough information, like PII, to proceed with brute force attacks through dictionaries. It would take less effort for a threat actor to impersonate the individual and gain access not only to the organization. |