## **Security Incident Report: Investigation of Found USB Drive in Hospital Parking Lot**

|  |  |
| --- | --- |
| **Contents** | The USB drive contains documents that include personal information which Jorge would prefer to keep private. These work files also contain personally identifiable information (PII) of other individuals, as well as details regarding the hospital’s operations. |
| **Attacker mindset** | Timesheets on the USB drive could provide an attacker with valuable information about the people Jorge works with. This personal or work-related information could be exploited to deceive the owner. For instance, a phishing email could be crafted to appear as if it is from a coworker or a family member. |
| **Risk analysis** | Raising employee awareness about these types of threats and advising on appropriate actions when encountering a suspicious USB drive is a managerial control that can mitigate the risk of a negative incident.  Implementing regular antivirus scans is an operational control that can be established. Additionally, a technical control, such as disabling AutoPlay on company computers, can serve as another layer of defense by preventing automatic execution of malicious code from a USB drive. |