**Incident handler's journal**

| **Date:**  Tuesday, 09:00 | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | A ransomware attack on a healthcare facility compromised the systems and prevented employees from being able to perform their jobs. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: An organized group of hackers who are known for targeting small healthcare facilities caused this incident. * **What**: The attackers compromised the network using phishing emails and malicious email attachments, and encrypted several employee devices. * **When**: Tuesday at 09:00 * **Where**: The small healthcare office that provides primary care services. * **Why**: The attackers are seeking a ransom payment in order to restore the devices and network. | | |
| Additional notes | This incident highlights a ransomware attack, and indicates that a better security posture and more social engineering training is necessary for the organization to avoid this type of attack in the future. | | |

| **Date:**  7-20-2022 | **Entry:**  2 | | |
| --- | --- | --- | --- |
| Description | A phishing email with a malicious attachment was sent to an employee and the attachment may have been opened. | | |
| Tool(s) used | I used the alert ticket, along with the phishing playbook to escalate the incident. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: The incident was caused by a phishing scammer. * **What**: An employee received an email with malware and may have downloaded it. * **When**: The incident occurred on July 20, 2022 09:30:14 AM * **Where**: The company email server and employee’s device * **Why**: The employee was tricked into downloading the malicious file due to the phishing attempt. | | |
| Additional notes | This ticket has been escalated. The email contains a malicious file attachment that needs to be investigated further by the security team. | | |