**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

| **Date:**  Record the date of the journal entry. | **Entry: 1**  Sunday 8th of June | | |
| --- | --- | --- | --- |
| Description | We are going to analyze the following event:  A small U.S. healthcare clinic suffered a security incident on Tuesday at 9:00 a.m. that severely disrupted its business operations.  The cause of the security incident was a phishing email containing a malicious attachment. Once downloaded, ransomware was deployed, encrypting the organization's computer files.  An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanding money in exchange for the decryption key. | | |
| Tool(s) used | Using NIST Framework, to apply standards and prepare a response for the event, SIEM Tools, Wireshark to analyze network packets, Forensics tool to prevent encryption. Backup and recovery systems. | | |
| The 5 W's | * **Who** caused the incident?   The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files.   * **What** happened?   An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key.   * **When** did the incident occur?   Tuesday morning at 9:00 AM.   * **Where** did the incident happen?   Small U.S health care clinic.   * **Why** did the incident happen?   A phishing email served as the initial point of entry into the clinic's systems.  A successful **social engineering attack (phishing)** led to the deployment of **ransomware**. | | |
| Additional notes | 1. How could the health care company prevent an incident like this from  occurring again?  2. Should the company pay the ransom to retrieve the decryption key?  3. ¿Any phishing training for the employers?  4. ¿Principle of least privilege on users?  5. ¿Backup strategy? | | |