**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:** 21st April 2025  Record the date of the journal entry. | **Entry: 1**  Record the journal entry number. **Tuesday 13:11** |
| Description | The SOC team received a phishing alert which was triggered by our IDS, an employee downloaded the file on thie computer |
| Tool(s) used | Virustotal.com |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   The incident was caused by a user when launching the file.   * **What** happened?   Once the file was launched this triggerd a malicious payload on the user's computer   * **When** did the incident occur?   It started today at13:11 the incident lasted until 13:20 from receiving / opening the file when the malware generated multiple executable files locally on the user's computer, the IDS triggered an alert to the SOC team of the incident.   * **Where** did the incident happen?   Onsite at the company's physial location.   * **Why** did the incident happen?   This happened due to user bad pratices this would have been avoided if the user scannd the file with the antivirus tool prior to executing. |
| Additional notes | A sha25 hash of the file was generated which is : 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b the ip address 114.114.114.114 is marked as suspicious according to virustotal, this is a harmful excutable file that uns a malware payload on the local computer of the user. |