**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  04/02/2025 | **Entry:**  04 |
| Description | This journal entry discusses an incident related to a **phishing attack** that led to unauthorized access to sensitive customer information. The incident was thoroughly investigated, and the findings were documented, including the use of specific tools for analysis and remediation. |
| Tool(s) used | VirusTotal (to analyze and verify malicious file hashes)  Web Application Logs (to trace attacker activities)  E-commerce Web Application Vulnerability Scanning Tools |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   **External attacker** who sent phishing emails and exploited a vulnerability in the web application to access customer data.   * **What** happened?   The attacker gained unauthorized access to **50,000 customer records** by exploiting a vulnerability in the e-commerce platform and performed a **forced browsing attack**.   * **When** did the incident occur?   **Initial phishing attempt**: **December 22, 2022**  **Confirmed breach and reporting**: **December 28, 2022**   * **Where** did the incident happen?   **Target organization**: **E-commerce company**  **Location**: Affected employees' devices and the company's web application server.   * **Why** did the incident happen?   A **vulnerability in the web application** allowed the attacker to exploit the system and access sensitive customer data by modifying the order numbers in the URL. |
| Additional notes | The **response and remediation** steps included **notifying affected customers**, offering **identity protection services**, and conducting a thorough investigation to identify the root cause.  The **organization's security posture** has been reviewed and strengthened, with a focus on **access control** and **vulnerability management** to prevent future incidents. |