# 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:**<br>06/11/2025 | **Entry:**<br>1 |
|---|---|
| Description | Review of a ransomware incident where attackers exploited phishing emails to gain access and encrypt critical healthcare company data, demanding a ransom. This entry aligns with the Detection and Analysis phase, as the incident was identified and initial information gathered for further investigation. |
| Tool(s) used | None |
| The 5 W's | • **Who:** An organized group of unethical hackers (suspected ransomware threat actors)<br>• **What:** A ransomware security incident where the attackers successfully encrypted critical company data and demanded a significant ransom payment for decryption.<br>• **Where:** The targeted organization is a healthcare company, impacting its IT systems and sensitive data.<br>• **When:** The incident was first detected on Tuesday at 9:00 AM. |
| Additional notes | • The company should enhance its employee security awareness training to reduce phishing risks.<br>• Consider deploying advanced email filtering and endpoint protection to prevent similar incidents. |

| **Date:**<br>06/15/2025 | **Entry:**<br>2 |
|---|---|
| Description | Investigation of a phishing alert where an employee received and interacted with a suspicious email attachment. This occurred during the Detection and Analysis phase, as suspicious activity was identified and validated using VirusTotal. |
| Tool(s) used | VirusTotal (used to analyze the suspicious file) |
| The 5 W's | • **Who:** Malicious actor (phishing attacker)<br>• **What:** An employee received a phishing email containing a malicious file attachment. The employee opened the email and downloaded the file, introducing malware onto their computer.<br>• **When:** The incident occurred at 1:11 p.m.<br>• **Where:** A financial services company<br>• **Why:** The incident happened because the employee interacted with a phishing email, failing to identify it as malicious and unknowingly downloading malware. |
| Additional notes | • Recommend implementing security awareness training for employees to improve phishing detection skills.<br>• Consider enhancing email filtering and anti-phishing tools to reduce exposure to such attacks. |

| **Date:**<br>06/16/2025. | **Entry:**<br>3 |
|---|---|
| Description | Documentation of a phishing attack where an employee unknowingly downloaded malware via a phishing email. This corresponds to the Detection and Analysis phase, with escalation to SOC Level 2 for Containment planning. |
| Tool(s) used | Phishing email |
| The 5 W's | • **Who:** An employee who unintentionally opened a phishing email and downloaded malware.<br>• **What:** The downloaded malware installed unauthorized software on the employee's computer.<br>• **Where:** A financial services company<br>• **When:** The incident occurred today at 1:11 p.m.<br>• **Why:** The employee was unaware that the email was malicious and acted automatically, opening and downloading the file. |
| Additional notes | • The incident has been confirmed as a phishing attack and escalated to SOC Analyst Level 2 for further investigation and response.<br>• Recommend reinforcing phishing awareness training and reviewing email security controls. |

---

| **Date:**<br>06/17/2025 | **Entry:**<br>4 |
|---|---|
| Description | Review of a forced browsing and data exfiltration incident at a retail company, resulting in financial loss. The entry reflects both Detection and Analysis and Containment, Eradication, and Recovery phases as the incident was detected late and required mitigation actions. |
| Tool(s) used | Forced browsing (unauthorized URL access and enumeration) |
| The 5 W's | • **Who:** An anonymous malicious hacker<br>• **What:** The attacker exploited the company's web application through a forced browsing attack, gaining unauthorized access and exfiltrating customer purchase data and transaction records.<br>• **Where:** A retail company<br>• **When:** First signs of the incident: December 22, 2022 at 3:13 p.m.<br>- Security team notified: December 28, 2022<br>- Investigation period: December 28 – December 31, 2022<br>• **Why:** The company's web application had a vulnerability — a single log source revealed an unusually high volume of sequentially listed customer orders. The attacker identified and exploited this flaw to access data without proper authorization. |
| Additional notes | • Perform routine vulnerability scans and penetration testing to identify and remediate web application weaknesses.<br>• Strengthen access control mechanisms:<br>- Implement allowlisting to restrict access to approved URLs and block all other requests.<br>- Ensure only authenticated and authorized users can access sensitive content. |

Reflections/Notes:

**Were there any specific activities that were challenging for you? Why or why not?**

Some activities involving interpreting complex phishing indicators and correlating log data were challenging because they required close attention to subtle details. It took practice to identify patterns quickly and confidently.

**Has your understanding of incident detection and response changed since taking this course?**

Yes — my understanding has deepened significantly. I now see incident response as a structured lifecycle where preparation, detection, containment, and recovery are tightly connected rather than isolated steps.

**Was there a specific tool or concept that you enjoyed the most? Why?**

I especially enjoyed working with VirusTotal because it provided fast, actionable intelligence on suspicious files and URLs. It made threat analysis feel more manageable and practical.