# 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>2024-10-14 | **Entry:**<br>1 |
|---|---|
| Description | Documenting a ransomware attack on a small U.S. health care clinic, which falls under the Detection and Analysis phase of the NIST Lifecycle. This highlights the need for robust detection mechanisms and employee training. |
| Tool(s) used | None noted |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who caused the incident? An organized group of hackers.**<br>• **What happened? Employees were unable to access their computers due to ransomware, which encrypted files and displayed a ransom note.**<br>• **When did the incident occur? Tuesday morning at 9:00 a.m.**<br>• **Where did the incident happen? At a health care clinic.**<br>• **Why did the incident happen? The attackers used phishing emails with malicious attachments.** |
| Additional notes | This incident highlights the need for improved employee training on recognizing phishing attempts. |

| **Date:**<br>2024-10-14 | **Entry:**<br>2 |
|---|---|
| Description | Using Wireshark to capture network traffic during a suspected data breach incident, which is part of the Detection and Analysis phase. This helped identify unusual outbound traffic. |
| Tool(s) used | **Wireshark** |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who caused the incident? Unknown, under investigation.**<br>• **What happened? Network traffic analysis revealed unusual outbound connections indicating data exfiltration.**<br>• **When did the incident occur? Over the weekend, detected on Monday morning.**<br>• **Where did the incident happen? Company network.**<br>• **Why did the incident happen? Potential exploitation of unpatched vulnerabilities.** |
| Additional notes | Further investigation required to identify the root cause of the breach. |

---

| **Date:**<br>2024-10-14 | **Entry:**<br>3 |
|---|---|
| Description | Analyzing suspicious file hashes related to malware found on employee |

| | |
|---|---|
| | workstations. This falls under the Detection and Analysis phase of the NIST Lifecycle, facilitating rapid response to threats. |
| Tool(s) used | HashAnalyzer |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who caused the incident? Potentially a malicious insider or external actor.**<br>• **What happened? Several files with known malicious hashes were detected and flagged.**<br>• **When did the incident occur? Detection occurred on Thursday morning.**<br>• **Where did the incident happen? Employee workstations in the main office.**<br>• **Why did the incident happen? Likely downloaded from untrusted sources.** |
| Additional notes | Immediate action taken to quarantine affected workstations. |

---

| **Date:**<br>2024-10-14 | **Entry:**<br>4 |
|---|---|
| Description | Utilizing Splunk to perform a query on user access logs to identify unauthorized access attempts, a critical activity in the Detection and Analysis phase. It enhances monitoring of potential intrusions. |
| Tool(s) used | **Splunk** |

| | |
|---|---|
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who caused the incident? Unauthorized external actor.**<br>• **What happened? Query revealed multiple failed login attempts followed by a successful one.**<br>• **When did the incident occur? Friday night at 10:00 p.m.**<br>• **Where did the incident happen? Remote access to the company's server.**<br>• **Why did the incident happen? Password guessing or stolen credentials.** |
| Additional notes | Recommendations made for enhancing password policies and implementing multi-factor authentication. |

Reflections/Notes:

**Were there any specific activities that were challenging for you? Why or why not?**
Yes, analyzing packet captures with Wireshark was challenging due to the complexity of interpreting the data. Understanding the significance of different packets and filters required additional study and practice.

**Has your understanding of incident detection and response changed since taking this course?**
Absolutely. My understanding has deepened significantly, especially regarding the importance of the NIST Incident Response Lifecycle and the critical role of preparation in effectively managing incidents.

**Was there a specific tool or concept that you enjoyed the most? Why?**
I particularly enjoyed using Splunk for log analysis. Its user-friendly interface and powerful query capabilities made it easier to identify patterns and potential security incidents, enhancing my analytical skills.