# Incident handler's journal

| | |
|---|---|
| **Date:** Oct 15, 2025 | **Entry: #1** |
| Description | Documenting a cybersecurity incident<br><br>This incident occurred in the two phases:<br>1. **Detection and Analysis**: The scenario outlines how the organization first detected the ransomware incident. For the analysis step, the organization contacted several organizations for technical assistance.<br>2. **Containment, Eradication, and Recovery**: The scenario details some steps that the organization took to contain the incident. For example, the company shut down their computer systems. However, since they could not work to eradicate and recover from the incident alone, they contacted several other organizations for assistance. |
| Tool(s) used | None |
| The 5 W's | ● **Who**: An organized group of unethical hackers<br>● **What**: A ransomware security incident<br>● **Where**: At a health care company<br>● **When**: Tuesday 9:00 a.m.<br>● **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key. |
| Additional notes | 1. How could the health care company prevent an incident like this from occurring again?<br>2. Should the company pay the ransom to retrieve the decryption key? |

| | |
|---|---|
| **Date:** Oct 17, 2025 | **Entry: #2** |
| Description | Analyzing a packet capture file |
| Tool(s) used | I used Wireshark to analyze a packet capture file. |
| The 5 W's | ● **Who**: N/A<br>● **What**: N/A<br>● **Where**: N/A<br>● **When**: N/A<br>● **Why**: N/A |
| Additional notes | I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic. |

---

| | |
|---|---|
| **Date:** Oct 17, 2025 | **Entry: #3** |
| Description | Capturing my first packet |
| Tool(s) used | I used tcpdump to capture and analyze network traffic. |
| The 5 W's | ● **Who**: N/A<br>● **What**: N/A<br>● **Where**: N/A<br>● **When**: N/A<br>● **Why**: N/A |
| Additional notes | I'm still new to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times because I used the wrong commands. But after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic. |

---

| | |
|---|---|
| **Date:** Oct 20, 2025 | **Entry: #4** |
| Description | Investigate a suspicious file hash |
| Tool(s) used | For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious.<br>This incident occurred in the **Detection and Analysis** phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat. |
| The 5 W's | ● **Who**: An unknown malicious actor<br>● **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of **54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b**<br>● **Where**: An employee's computer at a financial services company<br>● **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file<br>● **Why**: An employee was able to download and execute a malicious file attachment via e-mail. |
| Additional notes | How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on? |