**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:**  July 20, 2025 | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | Documented a phishing incident that targeted employees of a mid-sized marketing firm. The suspicious email contained a link to a credential-stealing site. The SOC detected abnormal login attempts shortly after the email was opened, prompting an immediate investigation. Employee accounts were temporarily locked to prevent further compromise. | | |
| Tool(s) used | Email filtering logs and SIEM alerts helped identify the phishing source and timeline of events. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: An organized group of unethical hackers. * **What**: A ransomware security incident. * **When**: Tuesday morning at approximately 9:00 a.m. * **Where**: At a small healthcare clinic in the United States. * **Why**: The attackers exploited the organization’s security by using phishing emails to install malware. Once inside the network, they encrypted files and demanded a ransom payment. The motivation appears to be financial. | | |
| Additional notes | How could the healthcare company prevent an incident like this from occurring again?  Should the company pay the ransom to retrieve the decryption key? | | |

| **Date:**  August 3, 2025 | **Entry:**  2 | | |
| --- | --- | --- | --- |
| Description | Investigating an alert about a suspicious file being downloaded. | | |
| Tool(s) used | VIRUSTOTAL, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** : An organized group of unethical hackers. * **What** : Malicious file downloaded. * **When** : **1:11 p.m.:** An employee receives an email containing a file attachment.   **1:13 p.m.:** The employee successfully downloads and opens the file.  **1:15 p.m.:** Multiple unauthorized executable files are created on the employee's computer.  **1:20 p.m.:** An intrusion detection system detects the executable files and sends out an alert to the SOC.   * **Where** : A financial service company. * **Why** : Ignorance about cyber security. | | |
| Additional notes | This file contains various viruses. It steals credentials and valuable information. | | |

| **Date:**  August 6, 2025 | **Entry:**  3 | | |
| --- | --- | --- | --- |
| Description | Using a playbook to respond to a phishing incident. | | |
| Tool(s) used | NONE | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** : Malicious hacker. * **What** : Send a file with malware. * **When** : July 20, 2022 09:30:14 AM * **Where** : A financial service company. * **Why** : Downloading a file with malware. | | |
| Additional notes | Sender mail and name are not the same. Therefore I can say it is a mail sent by a malicious entity. | | |

| **Date:**  August 8, 2025 | **Entry:**  4 | | |
| --- | --- | --- | --- |
| Description | Used vulnerability scanning tools to assess a retail company’s web application security. The scan identified outdated plugins and misconfigured access controls. The results were documented to inform remediation and penetration testing. | | |
| Tool(s) used | Web server log analysis tools  Vulnerability scanning tools | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** : An unidentified attacker exploiting a web application vulnerability. * **What** : A forced browsing attack allowed unauthorized access to purchase confirmation pages, exposing and exfiltrating approximately 50,000 customer PII and financial records. * **When** : First suspicious email: December 22, 2022, 3:13 p.m. PT   Confirmed breach: December 28, 2022, 7:20 p.m. PT   * **Where** : E-commerce web application of the retail company. * **Why** : A vulnerability in the e-commerce web application allowed attackers to modify order numbers in the URL to access other customers’ purchase confirmation pages. | | |
| Additional notes | * The company disclosed breach to customers and provided free identity protection services. * Future prevention steps: routine vulnerability scans, penetration testing, and stricter access control mechanisms (allowlisting URLs, authenticated access only). | | |

| **Date:**  August 13, 2025 | **Entry:**  5 | | |
| --- | --- | --- | --- |
| Description | Explored the use of Suricata to analyze network traffic and create intrusion detection signatures. The activity focused on monitoring suspicious patterns and generating alerts for abnormal behavior. This practice helped understand signature creation and real-time threat detection. | | |
| Tool(s) used | * Suricata commands to analyze logs and generate signatures. * Monitored incoming and outgoing traffic to detect anomalies. * Learned to customize rules to trigger alerts for specific threats. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** N/A * **What** N/A * **When** N/A * **Where** N/A * **Why** N/A | | |
| Additional notes | Regular log review and signature updates are critical for keeping the IDS effective. | | |

| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

### Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

| Reflections/Notes:   * Documenting incidents systematically helps identify patterns and recurring threats, which improves overall cybersecurity readiness. * Using tools like VirusTotal, Suricata, and log analysis enhances the ability to detect, analyze, and respond to threats effectively. * Understanding the 5 W’s (Who, What, When, Where, Why) ensures a comprehensive view of each incident, aiding in faster mitigation and better reporting. * Prevention and awareness are key: phishing training, vulnerability management, and regular system monitoring significantly reduce risk. * Reviewing past incidents and final reports helps identify gaps in policies and procedures, guiding future security improvements. * Keeping detailed notes supports continuous learning and strengthens the incident response workflow. |
| --- |