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: 12-12-2023	**Entry:** 01
Description	**Security incident**: Severe disruption of business operations.
Tool(s) used	**Cybersecurity tools**: NA.
The 5 W's	Capture the 5 W's of an incident. • **Who**: An organized group of unethical hackers. • **What**: Ransomware attack. The company was unable to access critical patient data, causing major disruptions in their business operations. • **When**: Tuesday at 9:00 a.m. • **Where**: Small U.S. health care clinic. The attackers were able to gain access into the company's network. • **Why**: Several employees of the company received phishing emails that contained a malicious attachment that installed malware on the employee's computer once it was downloaded. Once the attackers gained access, they deployed their ransomware, which encrypted critical files. Their 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	The company was forced to shut down their computer systems and contact

	several organizations to report the incident and receive technical assistance. **Questions**: How could the health care company prevent an incident like this from occurring again? [Employee Training.]

Date: 12-13-2023	**Entry:** 02
Description	**Security incident**: Malware. Phishing.
Tool(s) used	**Cybersecurity tools**: Security operations center (SOC). SHA256 file hash. VirusTotal. Playbook
The 5 W's	Capture the 5 W's of an incident. • **Who**: Unkown. • **What**: Malware attack. • **When**: Wednesday at 1:11 p.m. • **Where**: Small financial services company. • **Why**: An employee received an email containing a file attachment, successfully downloaded and opened the file. The intrusion detection system detected the executable files that were created on the employee's computer and sent out an alert to the SOC. The motivation of the attacker appears to be unknown.
Additional notes	According to VirusTotal and the file hash, 57 security vendors and 2 sandboxes flagged this file as malicious. It has a negative community score, indicating it to be malicious. According to the playbook instructions, since the alert severity is Medium it was a good indication that the ticket required escalation. The sender details of the email reveal inconsistencies that indicated a phishing attempt. After

	analyzing the message body (and subject line) of the email and noticing a grammatical error in the subject line, it was a good indication of a phishing attempt as well. Plus, a file was attached to this email. I, following the playbook instructions , escalated the ticket and updated the ticket status to **Escalated** and notified the level-two SOC analyst via email and text. **Questions**: How could the company prevent an incident like this from occurring again? [Employee Training.]

Date: 01-03-2024	**Entry:** 03
Description	**Security incident**: Data Breach.
Tool(s) used	**Cybersecurity tools**: Security operations center (SOC). OWASP (Broken Access Control).
The 5 W's	Capture the 5 W's of an incident. • **Who**: Hacker. • **What**: Web application vulnerability. • **When**: December 28, 2023, at 7:20 p.m., PT. • **Where**: Mid-sized retail company. With both physical store locations and e-commerce operations. • **Why**: The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer

	data, which the attacker then collected and exfiltrated. The motivation of the attacker appears to be financial.
Additional notes	The organization collaborated with the public relations department to disclose the data breach to its customers. Additionally, the organization offered free identity protection services to customers affected by the incident. To prevent future recurrences, we are taking the following actions: • Perform routine vulnerability scans and penetration testing. • Implement better access control mechanisms. **Questions**: How could the company prevent an incident like this from occurring again? [Employee Training (SW team). OWASP Top Ten.]

Date: 12-15-2024	**Entry:** 04
Description	**Security incident**: NA. Training (Analyzing a packet capture file).
Tool(s) used	**Cybersecurity tools**: Wireshark.
The 5 W's	Capture the 5 W's of an incident. • **Who**: NA • **What**: NA • **When**: NA • **Where**: NA

	• **Why**: NA
Additional notes	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity. Although I previously used Wireshark, I simply scratched the surface of this powerful tool. This activity provided me a real world scenario that went into depth on the use of it.

Date: 12-15-2024	**Entry:** 05
Description	**Security incident**: NA. Training (Familiarizing with tcpdump and analyzing a packet capture file).
Tool(s) used	**Cybersecurity tools**: Linux. tcpdump.
The 5 W's	Capture the 5 W's of an incident. • **Who**: NA • **What**: NA • **When**: NA • **Where**: NA • **Why**: NA

Additional notes	For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that is accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic. Although I minimally used tcpdump, this lab provided me a real world scenario that went into depth on the use of it. The instructions in this lab were clear and straightforward that allowed me to press forward more easily.

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: Record additional notes.
Despite there being activities and labs that were challenging for me, the fact that the instructions in them were clear and straightforward allowed me to press forward more easily. My understanding of incident detection and response changed since taking this course because my previous experience with some of these technologies simply scratched the surface whereas the activities and labs in the course provided me real world scenarios that went into depth on the use of these tools (such as Wireshark, tcpdump, Suricata, and Spunk) in the cybersecurity field. These specific tools and concepts behind final reports, journals, and playbooks I enjoyed the most because they reinforce the importance of documentation and remind me how imperative are frameworks and teamwork in planning ahead for future security incidents.