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: Record the date of the journal entry.	**Entry: 1** 12/24/24
Description	Ransomware attack disrupts clinic operations, demands payment
Tool(s) used	● Splunk: Splunk aggregates and analyze log data from various sources, enabling real-time detection of phishing emails and malware activity. It also supports forensic analysis to trace the attack timeline and identify the root cause ● VirusTotal: Virus Total is an online service that analyzes files and URLs for viruses, worms, trojans, and other malicious content by aggregating results from over 70 antivirus scanners and URL/domain blacklisting services . It provides a comprehensive overview of potential threats, allowing cybersecurity professionals, researchers, and users to quickly identify and understand the nature of suspicious files and links

The 5 W's	Capture the 5 W's of an incident. - **Who** Attacker/Hacker - **What** Ransomware attack - **When** Tuesday December 12 at 9am - **Where** US healthcare clinic - **Why** Employe clicked a malicious linked allowing the attacker to encrypt data for financial gain
Additional notes	- More employee training on phishing emails - Can data be recovered or pay ransom? - Are there backups of the data?

Date: Record the date of the journal entry.	**Entry: 2** December 22, 2022
Description	VirusTotal is a free online service that analyzes files and URLs for viruses, worms, trojans, and other malicious content by aggregating results from over 70 antivirus scanners and URL/domain blacklisting services[13]. It provides a comprehensive overview of potential threats, allowing cybersecurity professionals, researchers, and users to quickly identify and understand the nature of suspicious files and links
Tool(s) used	- Splunk: This SIEM tool is ideal for aggregating and analyzing log data to detect anomalies, such as malicious file downloads or unauthorized access. It provides real-time monitoring, threat intelligence integration, and customizable dashboards to track the attack timeline and

	understand its scope. ● Wireshark: Wireshark is a network protocol analyzer that can capture and analyze network traffic in real-time. It allows analysts to inspect communication between systems, identify suspicious traffic patterns, and trace the ransomware's network activity, such as command-and-control communication or file encryption triggers
The 5 W's	Capture the 5 W's of an incident. ● **Who** Malicious actor ● **What** Ransomware data theft ● **When** 3:13 p.m., PT, on December 22, 2022 ● **Where** an organization ● **Why** Vulnerability in e-commerce web app allowed forced browsing attack by modifying order numbers in URLs. Attacker accessed thousands of purchase confirmation pages, exposing customer PII and financial data. Inadequate access controls and authentication led to this breach. Attacker's motive was financial gain, attempting to extort the company for cryptocurrency payment in exchange for not releasing the stolen data publicly.
Additional notes	● The forced browsing attack exploited a critical vulnerability in the e-commerce platform, highlighting the need for more robust input validation and access controls. ● Web application access logs were crucial in determining the scope of the breach, emphasizing the importance of comprehensive logging and monitoring practices.

INCIDENT FINAL REPORT

Executive Report

The organization experienced a security incident on December 28, 2022, at 7:20 p.m., PT, during which an individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information. Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential loss of revenue. The incident is now closed and a thorough investigation has been conducted.

Timeline

At approximately 3:13 p.m., PT, on December 22, 2022, an employee received an email from an external email address. The email sender claimed that they had successfully stolen customer data. In exchange for not releasing the data to public forums, the sender requested a $25,000 cryptocurrency payment. The employee assumed the email was spam and deleted it. On December 28, 2022, the same employee received another email from the same sender. This email included a sample of the stolen customer data and an increased payment demand of $50,000. On the same day, the employee notified the security team, who began their investigation into the incident. Between December 28 and December 31, 2022, the security team concentrated on determining how the data was stolen and the extent of the theft.

Investigation

The security team received the alert and traveled on-site to begin the investigation. 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

---

Date:	**Entry: 3**
Record the date of the journal entry.	January 15th 2025

Description	Password-protected spreadsheet in phishing email delivered malware to employee's computer, compromising network security.
Tool(s) used	Virus Total Sha256 Khali Linux
The 5 W's	Capture the 5 W's of an incident. ● **Who** Malicious actor ● **What** A malicious payload was executed on the employee's computer after opening a password-protected spreadsheet attachment received via email ● **When** 1:11pm ● **Where** financial service company ● **Why** The employee opened a suspicious email attachment, likely part of a phishing attack designed to infiltrate the company's network.
Additional notes	● Identify additional IoCs and potential malware connections ● Consider company-wide phishing awareness training

---

Date: 7/20/2022	**Entry: 4** Record the journal entry number.
Description	Malicious file downloaded on employee computer
Tool(s) used	Splunk Virus Total

The 5 W's	Capture the 5 W's of an incident. - **Who** Malicious actor - **What** Malicious file downloaded on employee computer - **When** 09:30:14am - **Where** Financial Service Company - **Why** Employee clicked malicious link
Additional notes	- Block the sender's email address and any associated malicious URLs or domains - Reset the targeted user's credentials

---

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.

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.