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: 2024/04/18	**Entry:** 1
Description	This entry is about a ransomware attack that occurred to a small U.S. health care clinic. The business operations were down because employees were unable to access the files and software needed to do their job.
Tool(s) used	NA
The 5 W's	Capture the 5 W's of an incident. • **Who:** Organised group of unethical hackers • **What:** Ransomware attack • **When:** Approximately 9:00 a.m. • **Where:** A U.S. health care clinic • **Why:** The attackers sent several phishing emails to the company's employees. The phishing emails contained a malicious attachment that installed malware on the employee's computer once downloaded. Once the attacker gained access, they deployed their ransomware, encrypting critical files. The motive is likely financial due to them asking for a large sum of money to decrypt the files.
Additional notes	• What security controls are in place to deal with phishing emails?

	• What security training have the employees been trained on?

Date: 2024/04/22	**Entry:** 2
Description	This entry is about a trojan horse attack that occurred on an employee's computer of a financial services company. The employee received a job application email with an attachment.
Tool(s) used	TotalVirus
The 5 W's	Capture the 5 W's of an incident. • **Who**: Threat actor BlackTech • **What**: Phishing email with trojan attached • **When**: 1:11 p.m. • **Where**: A financial services company • **Why**: The attacker sent an employee of the company a job application email containing a password protected resume and the password. The employee downloaded the file, then entered the password to open the file. A malicious payload was then executed on their computer. Due to the malware having input capture, it is likely it is designed to obtain credentials.
Additional notes	• The malware is a trojan under the name Flagpro commonly used by threat actor BlackTech • What is the best way to prevent similar attack in the future

---

Date: 2024/04/23	**Entry:** 3
Description	An individual gained unauthorised access to customer 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.
Tool(s) used	NA
The 5 W's	Capture the 5 W's of an incident. ● **Who**: Threat actor ● **What**: A major data breach ● **When**: 3:13 p.m. December 22, 2022 ● **Where**: A retail company ● **Why**: The attacker took advantage of a vulnerability in the e-commerce web application. They performed a forced browsing attack and accessed customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. The attacker was able to access customer purchase confirmation pages, which they then collected and exfiltrated. The motivation seems to be monetary as they demanded payment in exchange for not releasing the data.
Additional notes	● How much has the incident affected the company's public standing? ● What other controls should be in place to keep customers' data safe

---

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.

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.