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: 30/11/2023	**Entry: #1**
Description	Documenting a security Incident.
Tool(s) used	None.
The 5 W's	● **Who:** An organized group of unethical hackers ● **What:** A ransomware security incident. ● **Where:** At a small U.S. health care clinic ● **When:** Incident on Tuesday at 9:00 a.m. ● **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? 2. Should the company pay the ransom to retrieve the decryption key?

Date: 1/12/2023	**Entry: #2**
Description	Document a Security incident
Tool(s) used	Input Capture
The 5 W's	Capture the 5 W's of an incident. ● **Who:** An advanced threat actor BlackTech. ● **What:** An intrusion detection system detects the executable files and sends out an alert to the SOC. ● **When:** Incident at 1:11 p.m. ● **Where:** at a financial services company. ● **Why:** The incident happened because unethical hackers were able to successfully carry out a Phishing attack. An employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.
Additional notes	1. How could the financial services company prevent an incident like this from occurring again? 2. Should the company retrain the employees on Phishing attacks and other vulnerability attacks.

Date: 12/2/2023	**Entry: #3**

Description	Documenting a security Incident
Tool(s) used	Input capture
The 5 W's	Capture the 5 W's of an incident. ● **Who**: An advanced threat actor BlackTech ● **What**: An intrusion detection system detects the executable files and sends out an alert to the SOC. ● **When**: Incident on Wednesday, July 20, 2022, 09:30:14 AM. ● **Where**: at a financial services company. ● **Why**: The incident happened because unethical hackers were able to successfully carry out a Phishing attack. An employee received an email containing an attachment. The attachment was a password-protected executable file. The executable's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.
Additional notes	There is an inconsistency between the sender's email address "76tguy6hh6tgftrt7tg.su'" the name used in the email body "Clyde West," and the sender's name, "Def Communications." The email body and subject line contained grammatical errors. The email's body also contained a password-protected attachment, "bfsvc.exe," which was downloaded and opened on the affected machine. Having previously investigated the file hash, it is confirmed to be a known malicious file.

Date: 12/2/2023	**Entry: #4**
Description	Documenting a security incident

Tool(s) used	Forced browsing
The 5 W's	Capture the 5 W's of an incident. ● **Who**: An advanced threat actor. ● **What**: a vulnerability in the e-commerce web application. ● **When**: on December 28, 2022, at 7:20 p.m., PT ● **Where** at an E-commerce **Why**: 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 purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated.
Additional notes	To prevent future recurrences, we are taking the following actions: ● Perform routine vulnerability scans and penetration testing. ● Implement the following access control mechanisms: ○ Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range. ○ Ensure that only authenticated users are authorized access to content.

Date: 12/3/2023	**Entry: #5**

Description	Documenting a security incident
Tool(s) used	Drop site for logs or stolen credentials
The 5 W's	Capture the 5 W's of an incident. ● **Who** signin.office365x24.com ● **What** a phishing attack was performed by a malicious actor ● **When** 2023-01-31 18:40:45 ● **Where**: at a financial services company ● **Why**: The incident happened because unethical hackers were able to successfully carry out a Phishing attack. Multiple employees got phishing emails on 2023-01-31. Multiple assets might have been impacted by the phishing campaign as logs showed that login information was submitted to the suspicious domain via POST requests the login was performed using url=http://signin.office365x24.com/login.php.
Additional notes	A total of three POST requests were made to the suspicious domain. This is an Advanced persistent threat (APT) since the attacker gained access in January and performed a phishing attack again on July 9th, 2023. By examining further, it is determined that two additional domains related to the suspicious domain are login.office365x24.com and office365x24.com.

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.

1. Were there any specific activities that were challenging for you? Why or why not?
2. Has your understanding of incident detection and response changed since taking this course?
3. Was there a specific tool or concept that you enjoyed the most? Why?