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: 08/19/2023	**Entry:** 1
Description	Security Incident Event at a small U.S. Health Care Clinic
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? - An organized group of unethical hackers who are known to target organizations in healthcare and transportation industries ● **What** happened? - A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations. The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key

	● **When** did the incident occur? - The incident occurred on a Tuesday morning at 9am ● **Where** did the incident happen? - At a small U.S. healthcare clinic ● **Why** did the incident happen? - The incident happened because of a phishing email sent to employees of the company. Once the phishing email is opened, malicious code is downloaded onto employees computers.
Additional notes	Include any additional thoughts, questions, or findings.

Date: 8/27/2023	**Entry:** 2
Description	Provide a brief description about the journal entry.
Tool(s) used	VirusTotal Website, Pyramid of Pain
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? - Unknown ● **What** happened? - I received a security alert about a suspicious file being downloaded on an employee's computer. The 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. ● **When** did the incident occur? - 8/26/2023 ● **Where** did the incident happen? - At a company on an employee’s computer ● **Why** did the incident happen? - This incident happened because the employee downloaded a file from a suspicious email.
Additional notes	If the employee would have not downloaded the attachment attached to the suspicious file, this incident would not have occurred. It’s interesting, however, that by putting the hash form of the suspicious file into VirusTotal, I was able to gain information on if the suspicious file was malicious or not.

Date: 8/29/23	**Entry:** 3
Description	Previously, I received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash using VirusTotal, the attachment has been verified as malicious. I have to take the next steps in resolving this matter.
Tool(s) used	Phishing playbook, VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident?

	- An attacker by the name of Clyde West, who claims they are from a company called Def Communications. ● **What** happened? - The user opened a phishing email and opened an attachment. The attachment contained malicious code. Some of the noticeable indicators of this email being a phishing email are the subject line which contains a word spelled incorrectly. In addition, the beginning of the email contains a grammatical error. Also, the sender's information is inconsistent being that it was spelled incorrectly as well. ● **When** did the incident occur? - July 20, 2022 at 9:30:14am ● **Where** did the incident happen? - The incident happened on an employee's computer ● **Why** did the incident happen? - This incident happened because the employee clicked on the phishing email and clicked on the attachment that was attached to the email.
Additional notes	Employees need to pay attention to indicators of compromise. Looking at the subject line and email body are some of the simple things employees can do to determine a phishing email.

Date: 9/3/2023	**Entry:** 4
Description	Using Splunk to create effective search techniques to efficiently identify

	patterns, trends, and anomalies within data
Tool(s) used	Splunk
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ● **What** happened? - I am working as a security analyst at the e-commerce store Buttercup Games. I've been tasked with identifying whether there are any possible security issues with the mail server. To do so, I must explore any failed SSH logins for the root account using Splunk. ● **When** did the incident occur? - March 6, 2023 at approximately 1:39am ● **Where** did the incident happen? - Buttercup Games “mailsv” host network. ● **Why** did the incident happen? - N/A
Additional notes	In the Splunk search function, I used the following search query: index=main host=mailsv fail* root This search term allowed me to search through the data for the keyword fail*. The wildcard tells Splunk to expand the search term to find other terms that contain the word fail such as failure, failed, etc. Lastly, the keyword root searches for any event that contains the term root. This search gave the following results: There are over 300 failed failed SSH logins for the root account on the mail server.