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: 06/09/2023	**Entry: #1**
Description	Ransomware attack on a small US based Health Clinic.
Tool(s) used	None

The 5 W's	• **Who** caused the incident?
	  ○ A group of hackers known for attacking healthcare and transportation industries.
	• **What** happened?
	  ○ All data on affected computers was encrypted, and a ransom note demanded for a large sum of money for the decryption key.
	• **When** did the incident occur?
	  ○ The incident occurred at approximately 9am.
	• **Where** did the incident happen?
	  ○ Inside the organization itself.
	• **Why** did the incident happen?

	○ The hackers were able to get a foothold on the organization's network through the use of social engineering techniques on employees that involved the use of phishing emails with a malicious attachment.
Additional notes	The malware in question might be a popular strain that is being used by APTs to target specific industries. Maybe further research on the malware or related APTs might provide a means for remediation.

Date: 13/09/2023	**Entry: #2**
Description	Investigating a suspicious file
Tool(s) used	VirusTotal
The 5 W's	● **Who** caused the incident? ○ An unknown malicious actor ● **What** happened? ○ The attachment was a password-protected spreadsheet file. ○ The spreadsheet's password was provided in the email with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ○ The employee downloaded the file, then entered the password to open the file.

	○ This led to the creation of multiple unauthorized executable on the employee's computer. ● **When** did the incident occur? ○ The incident occurred at 1:15 p.m ● **Where** did the incident happen? ○ Inside the company on an employee's computer. ● **Why** did the incident happen? ○ The employee must've thought the attachment was safe to open.
Additional notes	The employee was a victim of a phishing attempt. Further investigation of the email received might provide clues on why the employee decided to open the file. After creating a hash of the executable and passing it through VirusTotal, several metrics revealed that the file is indeed malicious. This file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech.

Date: 15/09/2023	**Entry: #3**
Description	Responding to a phishing email with a malicious attachment.
Tool(s) used	None
The 5 W's	● **Who** caused the incident? ○ An employee that received an email containing a file attachment. ● **What** happened?

	○ A phishing alert was received about a suspicious file being downloaded and opened on an employee's computer ● **When** did the incident occur? ○ The incident occurred at 1:15 p.m ● **Where** did the incident happen? ○ On an employees computer. ● **Why** did the incident happen? ○ The employee was tricked into downloading and opening the malicious attachment.
Additional notes	The email was confirmed to be malicious by passing the file hash through VirusTotal. Next, an alert ticket was created following the steps outlined in the phishing incident response playbook. Finally the ticket was escalated to a level-two SOC analyst to take further action.

Date: 16/09/2023	**Entry: #4**
Description	Identifying failed login attempts on a mail server.
Tool(s) used	Splunk
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ Explore any failed SSH logins for the root account. ● **What** happened? ○ Uploaded data that contains log and event information from Buttercup Games' mail servers and web accounts to identify any potential unauthorized access to the server through failed log in attempts.

	• **When** did the incident occur?
	  ○ After narrowing search results, the earliest failed login occurred around 01:39:51 am from the following IP address, 194.8.74.23 on port 3768.
	• **Where** did the incident happen?
	  ○ On Buttercup games mail servers.
	• **Why** did the incident happen?
	  ○ The frequency of failed login attempts might be an indication of malicious actors trying to access the root account via SSH.

Additional notes	After narrowing down the search for failed login attempts on the mail server's root account, this reduced the number of events to just over 300. It was observed that the server experienced a large number of failed login attempts from the root account via SSH on Thursday at approximately 01:39:51 am. Seeing as the attempts were coming from different IP addresses. This might indicate a targeted brute force attack on Buttercup games mail server. The malicious actor might be using a VPN to cover their tracks hence the different IP addresses or it might be a coordinated attack involving a number of diiferent malicious devices working in unison. Further investigation is required to identify the root cause of the logins.

Date: 17/09/2023	**Entry: #5**
Description	Using Chronicle to identify phishing emails from a suspicious domain.
Tool(s) used	Chronicle

The 5 W's	**None**
Additional notes	The suspicious domain has been involved in phishing campaigns. 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. Finally, two additional domains related to the suspicious domain were identified by examining the resolved IP address.

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.

Reflections/Notes:

After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response.