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: 03/24/2024	**Entry:** # 1
Description	A small U.S. health care clinic experienced a ransomware attack by an organized group of unethical hackers. The hackers encrypted essential business files, which disrupting normal business operations and demanding a ransom.
Tool(s) used	- **N/A**
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? - An organized group of unethical hackers ● **What** happened? – The hackers deployed a ransomware to encrypt the organization's computer files. ● **When** did the incident occur? – Tuesday at 9:00 AM ● **Where** did the incident happen? At a small U.S. health care clinic ● **Why** did the incident happen? The attackers demand a ransom.
Additional notes	Include any additional thoughts, questions, or findings. - How could the clinic prevent any further attacks like this? - If the clinic pays the ransom, will they get the decryption key? - Employees need more security awareness training.

Date: 03/30/2024	**Entry:** # 2
Description	A SOC analyst at a financial services company received an alert about a suspicious file being downloaded on an employee's computer. The analyst created a SHA256 hash of the file and used VirusTotal to uncover additional IoCs that are associated with the file.
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? - An employee ● **What** happened? – A suspicious file was downloaded to the employee’s computer. ● **When** did the incident occur? - at 1:13 p.m. ● **Where** did the incident happen? – In the financial services company. ● **Why** did the incident happen? - An employee received an email containing a file attachment, and he/she successfully downloaded and opened the file; Then, a malicious payload was executed on his/her computer.
Additional notes	Include any additional thoughts, questions, or findings. - Is there anyone else opened the email and downloaded the file? - Is there any other computer infected? - Employees need more security awareness training.

Date: 03/31/2024	**Entry:** # 3
Description	Follow playbook instructions to investigate and resolve the incident's alert ticket.
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? - Clyde West (The name mentioned in email body) ● **What** happened? – An email with attachment was sent to the employee of the inergy company. ● **When** did the incident occur? 07/20/2022 at 09:30 AM ● **Where** did the incident happen? Ingery company ● **Why** did the incident happen? The malicious actor was trying to trick employee to open the malicious attachment in the email.
Additional notes	Include any additional thoughts, questions, or findings. - There are several spelling and grammar errors in the email. Did the employee notice? - The attachment is an executable file.

Date: 04/01/2024	**Entry:** # 4
Description	Review a final report
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An attacker ● **What** happened? An attacker accessed and collected the information of customers and requested a payment of $50k for not releasing data to public. ● **When** did the incident occur? December 28, 2022 ● **Where** did the incident happen? Company website. ● **Why** did the incident happen? The attacker was trying to request a payment for not releasing customers' data to public.
Additional notes	Include any additional thoughts, questions, or findings. - Did the company pay the ransom? - Did the attacker release any customer's information? - If the employee notified the security team when she/he first received the email, will the security team find out the vulnerability earlier?

Date: 04/05/2024	**Entry:** # 5
Description	Upload sample log data from Buttercup Games’ mail severs and web accounts to Splunk cloud and write queries to locate failed SSH login(s) for the root account.
Tool(s) used	Splunk cloud
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Unknown ● **What** happened? Failed SSH logins for the root account ● **When** did the incident occur? 02/27/2023 - 03/06/2023 ● **Where** did the incident happen? Mailsv, www1, www2, www3 (Buttercup Game mail server and web application) ● **Why** did the incident happen? Someone attempts to log in to an SSH server using the **root** account but fails to authenticate successfully.
Additional notes	- Using wildcard * can expand search results

Date: 04/05/2024	**Entry:** # 6
Description	Using Chronicle to investigate domain that contained in the phishing email to see if it’s malicious, and determine if there are any other employees have received phishing emails containing this domain.
Tool(s) used	Chronicle
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Unknown phishing email sender ● **What** happened? An employee received a phishing email and visited the domain. ● **When** did the incident occur? 01/31/2023 ● **Where** did the incident happen? At a financial services company ● **Why** did the incident happen? To steal login information
Additional notes	Include any additional thoughts, questions, or findings. - After clicked IP address 40.100.174.34 under RESOLVED IPS, I found signin.office365x24.com uses another domain signin.accounts-google.com - Affected assets are: amir-david-pc, ashton-davidson-pc, bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc, warren-morris-pc. - Three POST requests were made from ashton-davidson-pc, emil-palmer-pc, and warren-morris-pc to the IP address 40.100.174.34 - Malicious actor sent out phishing emails to trick employees to visit suspicious domain and submit login information via POST requests.

Reflections/Notes: Record additional notes.

1. Were there any specific activities that were challenging for you? Why or why not?

   Using Chronicle to investigate suspicious domain was a little bit challenging since I didn’t have any experience using Chronicle before. But the instructions for using it is very detailed and easy to follow.

2. Has your understanding of incident detection and response changed since taking this course?

   Before this course, I thought incident detection and response were linear processes, but it turns out that it’s a cyclical process. For example, there are four stages in the NIST incident response cycle framework: Preparation, detection & analysis, containment, eradication & recovery, and post-incident activity. To effectively manage incidents, the second and third phases may occur multiple times during incident handling. Furthermore, to prevent future incidents from occurring, the final phase may provide more insights into how to better protect and prepare for the next incident.

3. Was there a specific tool or concept that you enjoyed the most? Why?

   I enjoyed Splunk Cloud the most because it’s more straightforward to use and the interface is user-friendly.