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: 12-09-2024.	**Entry:** #1
Description	Provide a brief description of the journal entry. A small U.S. healthcare clinic experienced a security incident on Tuesday at 9:00 a.m. disrupting their business operations. Employees could not use their computers to access files and software needed to work. 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. The cause of the security incident was a phishing email that contained a malicious attachment. Once downloaded, ransomware was deployed encrypting the organization's computer files. The clinic shut down its computer systems and contacted several organizations to report and receive support.
Tool(s) used	
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Group of unethical hackers. • **What** happened? Ransomware attacks on computer systems caused by email phishing. • **When** did the incident occur? Tuesday at 9:00 am.

	• **Where** did the incident happen? A small U.S. healthcare clinic. • **Why** did the incident happen? Hackers wanted to extort money from the clinic.
Additional notes	Include any additional thoughts, questions, or findings. One of the several employees clicked the email phishing link instead of ignoring it. Need to hold a cybersecurity meeting about email phishing for the employees. Also, add security filtering to the business emails to reduce this risk.

Date: 12-12-2024	**Entry:**#2
Description	Received an alert that an employee had downloaded a suspicious file. The employee had downloaded a password-protected spreadsheet from a phishing email. When the password was entered a malicious payload was executed on the computer. I analyzed the file's SHA256 hash number to identify the malware using VirusTotal. The file was found to be malicious.
Tool(s) used	• VirusTotal • Pyramid of Pain • Module 3 Indicators of Compromise Reading
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A phishing email hacker. • **What** happened? An unsuspecting employee downloaded a malicious file from a phishing email. • **When** did the incident occur? At 1:15 pm that day. • **Where** did the incident happen? The employee's company computer.

	• **Why** did the incident happen? A hacker wanted to extract data from the company using the trojan horse method.
Additional notes	Include any additional thoughts, questions, or findings. Meetings must be held to inform employees of phishing emails and other social engineering attacks.

Date: 12-13-2024	**Entry:** #3
Description	Reviewing the alert ticket about a suspected phishing email attack. I analyzed the email to find clues on whether it was malicious or not. There were many IoCs like grammatical errors, a mismatch of the sender's identity, and a suspicious link. I decided to escalate the ticket to a level two SOC to handle.
Tool(s) used	• IDS • Security ticketing system • Phishing incident response playbook
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A phishing email hacker. • **What** happened? The employee alerted us of a possible phishing email attack. • **When** did the incident occur? July 20, 2022, at 1:15 pm. • **Where** did the incident happen? The employee's email and computer. • **Why** did the incident happen? The hacker disguised the malware as a resume to trick the employee.
Additional notes	The alert severity on the ticket was medium which means it might be escalated. The sender's email doesn't match the name at the end of the message. There

	are a lot of grammatical errors in the subject line and message. There was a download link to a file in the email.

Date: 12-14-2024	**Entry:** #4
Description	Reviewing the final report of a major incident before I was hired. A hacker had found a vulnerability in the e-commerce website and exfiltrated customer transaction data. They emailed the company on Dec 22 and 28, 2022 demanding money in exchange for not releasing the data on public forms. The security collaborated with public relations to notify affected customers and offer free identity protection. Then, I found the data breach and added a URL allow list to data requests with routine vulnerability scans and pen tests.
Tool(s) used	• Final report
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A hacker that used a possible injection attack. • **What** happened? The hacker exploited a web application vulnerability to exfiltrate customer data. • **When** did the incident occur? On Dec 22 - 28, 2022. • **Where** did the incident happen? Company's website and database. • **Why** did the incident happen? Hackers wanted to extort money from the business in exchange for not releasing the data to the public.
Additional notes	How did the IDS not alert higher traffic volume on the single log source?

Date: 12-18-2024	**Entry:** #5
Description	Beginner experience with Splunk. I am a security analyst with the e-commerce store Buttercup Games. My task is to investigate a possible security issue with the mail server's failed SSH logins for the root account. A basic search of the host as the mail server shows over 9,000 events with most being failed login attempts. I narrowed my search to failed root account logins by adding elements fail* and root into the search statement. I found over 300 failed login attempts from multiple IP addresses.
Tool(s) used	• Splunk
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A hacker from multiple IP addresses. • **What** happened? The hacker tried to log into the root account of the mail server with a brute force attack. • **When** did the incident occur? Multiple days, Feb 27 - Mar 7. • **Where** did the incident happen? Buttercup Games mail server login page. • **Why** did the incident happen? The hacker probably wanted to control the server to steal data or demand money in exchange for control.
Additional notes	Why was the IP address not put on a block list? Why didn't an IDS/IPS system not alert the security team beforehand?

Date: 12-18-2024	**Entry:** #6
Description	Beginner experience with Chronicle. I am a security analyst at a financial security company that received an alert from an employee receiving a phishing email. I reviewed the alert and investigated the domain in the email body; `signin.office365x24.com`, to see if any other employees had a similar experience or visited the website. In chronicle, I viewed the VT context of the website and its parent domain and found that they had low scores. This means it is not malicious but the site is still suspicious. Looking at the asset and timeline tabs, there are 7 different user accesses to the domain with both get and post requests from the login page, except for “roger-spencer-pc”. I checked if the resolved IPs are connected to multiple sites to ensure the site is malicious. Investigating the IP address; 40.100.174.34, I found that this site and another site resolve to this IP. New user access was found in the asset and timeline tabs, “warren-morris-pc”. This evidence confirms that this is a phishing email attack by most likely “roger-spencer-pc”.
Tool(s) used	• Chronicle
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The employee or hacker using “roger-spencer-pc” • **What** happened? A phishing email is stealing login info from employees. • **When** did the incident occur? On Jul 9, 2023. • **Where** did the incident happen? The phishing sites and employees’ email. • **Why** did the incident happen? The hacker probably wants to use the login info to steal data from other company sites. Use employee accounts to steal data.
Additional notes	The VirusTotal scores could be wrong. There is 7 different user accesses to the domain: ashton-davidson-pc,

	bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc “Roger-spence-pc” is the only account that doesn’t have a post request when logging in to the website. This site and its sibling site resolves to the IP address 40.100.174.34. A new user access, “warren-morris-pc” was found in the 40.100.174.34 asset tab. The third domain is “signin.accounts-gooqle.com”, it is misspelled.

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:

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

Of the activities in this journal, the Splunk and Chronicle activities were the most challenging since it was my first time using these SIEM tools. However, the video examples, readings, and step-by-step guide before the activities made learning and finishing the activities easier.

Has your understanding of incident detection and response changed after taking this course?

I gained more knowledge and experience with the incident and response lifecycle with this course than I did in my cybersecurity class in university. In university, I learned only the basics of each stage of the cycle rather than applying them. This section’s activities helped me better understand and apply the cycle with each real-world inspired scenario.

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

I enjoyed that each activity simulated real-world scenarios that I could encounter as a future security analyst in a comfortable and self-paced environment. I got to use popular industry tools like Splunk, Chronicle, and Suricata for the first time in this section and that will serve as a good foundation to keep learning them.