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 to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 06/31/2023	**Entry:** 1
Description	Healthcare company ransom ware attack
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? - A group of unethical hackers who target organizations in healthcare and transportation industries. • **What** happened? - A phishing email that contained malicious software was opened releasing the malicious code. That code created a backdoor that allowed the hackers to gain access, encrypt sensitive data, and leave a ransom letter demanding payment or the victims will not be able to decrypt the encrypted data. • **When** did the incident occur? - The incident occurred on a Tuesday at 9:00 a.m. in the morning. • **Where** did the incident happen? - The incident occurred at a small U.S. health care clinic specializing in delivering primary-care services. • **Why** did the incident happen? - The incident occurred because an employee opened the malicious email, releasing the malicious code.
Additional notes	I am hoping there was backup of sensitive data before the attack. So, we don't have to pay the ransom and resume normal business operation after a system restore is complete. We also need to address the phishing attack immediately, so this does not happen again.

Date: 06/31/2023	**Entry:** 2
Description	Threat actor was able to gain unauthorized access to customer personal identifiable information (PII) and financial information through a vulnerability in the e-commerce web application.

Tool(s) used	Web application access logs were reviewed.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? – Financially motivated threat actor. ● **What** happened? – A threat actor was able gain access to customer PII and financial data by performing a forced browser attack. ● **When** did the incident occur? – First email, approximately 3:13 p.m. on December 22, 2022. Second email, on December 28, 2022. These emails indicated a ransom. ● **Where** did the incident happen? – On the e-commerce web application of this company. ● **Why** did the incident happen? – This happened because there was an unknown vulnerability in the e-commerce application that the threat actor took advantage of.
Additional notes	The company worked with the public relations department to mitigate the situation. Free identity protection services were offered to impacted customers. Action have been taken to remedy the situation. Regular vulnerability scans and penetration testing will occur. Control measures will also be implemented to limit access to specific URLs and to ensure authorized users are the only ones that have access to the e-commerce application.

Date: 7/26/2023	**Entry:** 3
Description	I am a level one security operations center (SOC) analyst at a financial services company. A suspicious file has been downloaded on an employee's computer.
Tool(s) used	SHA256 hash function, VirusTotal report, Pyramid of Pain
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An employee was responsible for the security incident. ● **What** happened? The employee received an email with a password-protected spreadsheet file and a password. The employee then proceeded to open the file which executed and released the malicious code on the employees computer. ● **When** did the incident occur? The employee received the email at 1:11 p.m. and 1:15 p.m. the unauthorized malicious code it released onto the employee's computer. ● **Where** did the incident happen? The incident occurred on the company computer. However, no physical location was provided in the material for this activity.

	● **Why** did the incident happen? The incident occurred because the employee opened the file attached in the email they received.
Additional notes	It appears that training might be needed if employees are just opening files without due diligence. However, the file might have looked legit, training is still needed. We will have to contain the employee's computer and do forensic work to determine the extent of the damage. Disciplinary actions might have to been taken depending on the damage.

Date: 7/26/2023	**Entry:** 4
Description	I am a security analyst at a financial services company. An employee received a phishing email. I need to determine if any other employees received the same email and if they visited the domain.
Tool(s) used	Chronicle SIEM
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? A threat actor trying to gain access to the company's systems. ● **What** happened? The company received a phishing email from a suspicious domain name. ● **When** did the incident occur? Not sure, was not provide that information in activity material. ● **Where** did the incident happen? The incident occurred on a company computer but could be multiple computers. Not sure of the exact location because the information was not provided in the activity. ● **Why** did the incident happen? Not sure, the company might have been the target of a phishing campaign, with the hopes of gaining access to customer financial information.
Additional notes	I will need to review the log files in Chronicle SIEM to determine if any other employees received this email, visited the suspicious domain name, and triage if any systems have been compromised. Additionally, I really enjoyed using Chronicle to gain hands on experience with a SIEM.

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.

I really did not have a problem with any of the activities. However, I will need to spend more time learning about the SIEM systems and gain more experience using them. Also, my views on incident detection and response have changed since I started this course. I am more aware of details and attentive to notifications. I say that because each notification I get could be an attack so I will review each alert diligently. Finally, I really enjoyed the idea of creating your own documentation. I say that because in the beginning I was lost but I believed in the process and kept going. In the end, I learned that no documentation is perfect, what matters is how you use it to collect evidence and not how it looks.