Incident handler's journal

Date: December the 19th, 2023	**Entry:** #1
Description	This entry documents the pharmacy security incident.
Tool(s) used	Network activity logs.
The 5 W's	Capture the 5 W's of an incident. ● **Who:** An organized group of unethical hackers. ● **What:** Ransomware was deployed encrypting the organization's computer files. ● **When:** Tuesday at 9:00 a.m. ● **Where:** A healthcare company. ● **Why:** Malicious actors gained access through a phishing e-mail with a malicious attachment that an employee opened.
Additional notes	Urgent training is necessary. All employees should be made aware that security is a culture and a discipline.

Date: December 20th, 2023	**Entry:** #2
Description	A trojan virus infected an employee’s computer.

Tool(s) used	VirusTotal website.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: Malicious attacker sent an e-mail with a malicious attachment. ● **What**: Trojan virus infected an employee's computer. ● **When**: Wednesday December 20, 2023, at 2:30 a.m. ● **Where**: Financial services company. ● **Why**: An employee was tricked into downloading and installing a malicious file through phishing e-mail.
Additional notes	Training is required. All employees should understand the risks of downloading and executing files received via e-mail from unauthorized senders.

Date: December 21st, 2023	**Entry: #3**
Description	Employees might have fallen victim to a phishing attack.
Tool(s) used	Chronicle SIEM, VirusTotal.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: Seven compromised assets: ashton-davidson-pc, bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc, warren-morris-pc. ● **What**: A malicious domain was accessed from company's network. ● **When**: July 08, 2023 from 05:02:47 to 14:51:45. ● **Where**: Finance company premises.

	● **Why**: Several company computers accessed a malicious website (signin.office365x24.com) most likely after executing files attached to a phishing e-mail.
Additional notes	The intelligence report in Chronicle shows that this domain has been identified as malicious and categorized as “drop site for logs or stolen credentials”. The timeline shows HTTP POST requests from company’s computers to said malicious domain.

Date: December 21st, 2023	**Entry: #4**
Description	An individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information.
Tool(s) used	Incident final report.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: External malicious actor that gained access to company’s information. ● **What**: Personal and financial customer data was exfiltrated. ● **When**: 3:13 p.m., PT, on December 22, 2022, an employee received an e-mail with the claim that data had been stolen. ● **Where**: Retail company. ● **Why**: A hacker or group of hackers exploited a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page.
Additional notes	To prevent future recurrences, it is recommended to take the following actions: perform routine vulnerability scans and penetration testing, implement access control

	mechanisms like blocking requests outside of a set URL range and ensuring that only authenticated users are authorized access to content.

Reflections/Notes:

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

- Writing custom rules for IDS/IPS proved to be a complex and quite specific task, but it has to be. Although it was a challenge, I enjoyed it and in doing so learned quite a bit about how thorough this structured process of detecting anomalies in a system is.

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

- Based on my previous NOC experience, I have a finely tuned sense of urgency and real-time incident management. Of course, monitoring network performance is not the same as analyzing events that point to a security incident.

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

- I found "Chronicle" to be a very useful tool. The information is categorized and easy to filter and read. Navigating through the different menus and gathering relevant information was very satisfying.