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: 10/06/2023	**Entry:** #1
Description	Documenting Ransomware cybersecurity incident
Tool(s) used	N/A
The 5 W's	• **Who:** An organized group of unethical hackers. • **What:** Encrypted the organization's files and demanded ransom to have those files decrypted. • **When**: Tuesday at 9:00am. • **Where**: U.S. healthcare clinic • **Why**: This incident occurred because the group of unethical hackers were able to gain access into the organization's network and systems. They did this by conducting a phishing attack to gain entry into a computer. Once into the network they were able to launch their ransomware to encrypt the organization's files. The attack seems to be due to financial motivating factors due to the ransom note demanding a large sum of money to decrypt the files.
Additional notes	By having proper disaster recovery techniques in place the organization could

	have recovered from this incident and not have to pay a ransom. The organization could have also prevented this incident from spreading to their other computers by implementing the principles of least privilege.

Date: 10/12/2023	**Entry:** # 2
Description	Investigate a suspicious file hash
Tool(s) used	VirusTotal
The 5 W's	• **Who:** Financial Services company. • **What**: Phishing email containing malware was opened by an employee. • **When**: Around 1:11 p.m. to 1:20 p.m. • **Where**: Malicious file was opened nn the employees computer. • **Why**: Phishing attempt
Additional notes	**SHA256 file hash**: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b When reviewing the SHA256 hash of the suspected file on VirusTotal has revealed that this same file has been reported by 55 other vendors. This malware is known as trojan flagpro.

Date: 10/16/2023	**Entry:** #3
Description	Received a phishing alert about a suspicious file being downloaded on an employee's computer.
Tool(s) used	Phishing incident response runbook
The 5 W's	Capture the 5 W's of an incident. • **Who:** Employee opened a phishing email containing malicious content. • **What:** Phishing email was opened and malicious content was activated. • **When:** Around 1:11 p.m. to 1:20 p.m. • **Where**: On the employees computer. • **Why**: The contents of the phishing email was opened.
Additional notes	Utilized phishing incident response runbook to analyze the email and its contents. As the alert was categorized as a medium alert it was escalated to a level-two SOC analyst.

Date: 10/28/2023	**Entry:** #4
Description	Analyze failed SSH logins on root Account for e-commerce store Buttercup Games. Attempting to identify if there are any issues with their mail server.
Tool(s) used	SIEM - Splunk Buttercup Games log data

The 5 W's	Capture the 5 W's of an incident. • **Who:** Buttercup Games • **What**: Analyze mail server for any possible security issues • **When** From 02/27/2023 to 03/06/2023 • **Where** On Buttercup Games mail server • **Why** Failed login to the mail server from root account
Additional notes	By utilizing Splunk I was able to search through Buttercup Games log data for their mail server by using the following search query: `index=main host=mailsv fail* root` The results indicate that there were 346 failed login attempts made for the root account between the dates 02/27/2023 to 03/06/2023

Date: 10/28/2023	**Entry:** #5
Description	There has been an alert at a financial company that an employee received a phishing email in their inbox. A suspicious domain name is contained in the email's body: signin.office365x24.com
Tool(s) used	SIEM - Chronicle
The 5 W's	Capture the 5 W's of an incident. • **Who**: Employee received phishing email • **What**: A phishing email containing a suspicious domain name was sent to a financial employee

	• **When**: On 01/31/2023 six employee computers had contact with the suspicious domain • **Where** on the employees computers • **Why** Employees opened the phishing email and interacted with the email contents. These GET and POST actions can be seen in the logs via Chronicle of the interactions between the organization's assets and the suspicious domain.
Additional notes	The logs from Chronicle indicate that there were six employee computers who were affected by the phishing emails. When identifying the suspicious domain name: signin.office365x24.com the IP addresses 40.100.174.34 & 104.215.148.63 were found to be related to it. On Chronicle the domain itself is categorized as Drop site for logs or stolen credentials. It would seem this domain is involved in phishing campaigns and might have impacted a few of the organization's assets.
