Incident handler's journal

Instructions

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.

Date: 07/July/2023	**Entry: #1**
Description	This journal is based on the ransomware attack
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A group of unethical hackers caused the incident. • **What** happened? All the company's critical files were encrypted . • **When** did the incident occur? The incident occurred on tuesday at 9AM • **Where** did the incident happen? The incident took place on the organizations computer systems • **Why** did the incident happen? The incident was able to happen because of a phishing attack. The email contained a malicious attachment
Additional notes	The employees of the organization must be educated on social engineering attacks to prevent attacks of such kind from happening in future.

Date: 08/July/2023	**Entry: #2**
Description	A Phishing attack
Tool(s) used	**Hashing and VirusTotal**
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An attacker sent malicious email to an employee • **What** happened? The malicious email was downloaded by the employee, malicious code was executed on their computer • **When** did the incident occur? N/A • **Where** did the incident happen? N/A • **Why** did the incident happen? Because the employee downloaded the file, the incident was able to take place.
Additional notes	Educate employees on different types of attacks such as phishing.

Date:	**Entry:#3**

15/July/2023	
Description	An attacker was able to steal PII just by modifying the URL parameters
Tool(s) used	**Server logs,** Perform routine vulnerability scans and penetration testing, allowlisting
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An individual attacker • **What** happened? The attacker was able to steal the PII and card details of the customers who used to shop online • **When** did the incident occur? The organization experienced a security incident on December 28, 2022, at 7:20 p.m., • **Where** did the incident happen? • **Why** did the incident happen? There was a vulnerability in the website that allowed the attacker to modify the URL parameters and gain access to sensitive information.
Additional notes	Implement allowlisting, Ensure that only authenticated users are authorized access to content.

Date: 22/07/2023	**Entry: #4**
Description	Using a playbook to respond to a phishing attack
Tool(s) used	Playbook, ticketing system, IDS
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An attacker was able to get into the employees system • **What** happened? The attacker sent an email that contained a malicious attachment, the employee opened the attachment and affected the system • **When** did the incident occur? Around 12:45 PM • **Where** did the incident happen? The incident took place at company's headquarters • **Why** did the incident happen? The user did not verify if the mail was from a legitimate source.
Additional notes	Employees must be educated on possible social engineering attacks. file. Furthermore, the alert severity is reported as medium. With these findings, I chose to escalate this ticket to a level-two SOC analyst to take further action.

Date: 128/07/2023	**Entry: #5**
Description	Journal on how to use Splunk cloud
Tool(s) used	Splunk cloud
Steps	Create a splunk account Settings >Add Data files Drop the files > Click next Select segment in Path > enter “1” as Segment Number > Click review Click Submit Click Search and Reporting In the search bar enter your query. Eg: index=main or index=*
Additional notes	With splunk we can perform queries on data from the logs such as server log for failed login attempts. We can adjust the time based on the occurrence of the security event.