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: 07-29-2023	**Entry:** Journal Entry #1
Description	U.S. Health care clinic experienced a security incident
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • Unethical hackers who are known to target organizations in healthcare and transportation industries. • Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job. Ransomware installed into the system. • Tuesday morning, at approximately 9:00 a.m. • U.S Health care clinic • targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.
Additional notes	Who was the email sent to? Who opened it? Was the security system already

	experiencing vulnerabilities before the attack? Should the company pay the ransom?

Date: 07-29-2023	**Entry:** Journal Entry #2
Description	Received an alert about a suspicious file being downloaded on an employee's computer
Tool(s) used	VirusTotal,
The 5 W's	Capture the 5 W's of an incident. • **Who**: External attacker • **What**: Employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer. • **When**: 1:11pm • **Where**: Financial Service Company • **Why**: Employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.
Additional notes	Who was targeted? What information were they trying to gain access to? VirusTotal search found that this file hash has been reported as malicious by multiple vendors.

Date: 07-29-2023	**Entry:** Journal Entry #3
Description	I received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified to be malicious.
Tool(s) used	Playbook
The 5 W's	Capture the 5 W's of an incident. • **Who**: Clyde West - Sender • **What**: Phishing email alert • **When**: July 20, 2022 09:30am • **Where**: Financial Service Company • **Why**: Ticket alert showed that there may be potential phishing in an email received.
Additional notes	The email contains a file. Escalated to Level 2.

Date: 07-29-2023	**Entry:** Journal Entry #4
Description	Security incident, individual gained unauthorized access to PII and financial info.

Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • **Who**: External attacker • **What**: Attacker performed a forced browsing attack and • access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. • **When**: Between December 28, 2022 and December 31, 2022 • **Where**: Retail Company • **Why**: Attacker wanted ransom from the company. They were able to infiltrate through a vulnerability with the web application.
Additional notes	Instead of deleting the email, the employee should've sent a ticket in to report the email. Had it taken the company longer to find out, the possibility of a more severe result. Recommend training employees to spot and send in tickets.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident?

	• **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

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.

There wasn't anything difficult or too challenging in the activities. Everything was straight forward and I could find all the information I needed to complete the assignments. My understanding of incident response has definitely changed since taking the course. Everything here was new to me. I really enjoyed using Linux and SQL, I found those concepts really fun and engaging. It was my first time learning how to do any of these things.