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: 1 Aug 2023	**Entry:** #1
Description	Employee are unable to access medical records due to files being encrypted by ransomware attack
Tool(s) used	N/A

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ Organized group of unethical attacks who are known to attack healthcare and transportation industries
	• **What** happened?
	  ○ Hackers deployed ransomware on network, encrypting all files and demanding sum of money to be paid for access to files
	• **When** did the incident occur?
	  ○ Tuesday morning 9:00 AM
	• **Where** did the incident happen?
	  ○ Small U.S health clinic specializing in primary healthcare
	• **Why** did the incident happen?

	○ Phishing emails were sent to employees, employees downloaded files containing malicious code allowing attacks to gain a beachhead on the network.
Additional notes	Clinic shut down systems and reported the incident to incident response teams and other organizations for assistance. This may have future unintended consequences on clients and business.

Date: 2 Aug 2023	**Entry:** #2
Description	Malicious Excel spreadsheet executed malicious code on employee computer
Tool(s) used	Virus Total
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ Employee ● **What** happened? ○ Employee received email with excel spreadsheet attachment, open entering accompanying password malicious code was executed ● **When** did the incident occur? ○ 1:11 p.m.: Employee receives an email containing a file attachment. ○ 1:13 p.m.: Employee downloads and opens the file. ○ 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer.

	○ 1:20 p.m.: IDS detects the executable files and sends out an alert to the SOC. ● **Where** did the incident happen? ○ Employee workstation of a financial services company. ● **Why** did the incident happen? ○ Putting the file hash into VirusTotal confirmed the file to be a malicious trojan horse that checks user input, most likely the employee was targeted so attacks could learn employees credentials through the keylogger
Additional notes	MD5 Hash: 287d612e29b71c90aa54947313810a25 VirusTotal also reports the malware interacting with site name "org.misecure.com" with dns searches and HTTP requests to IP address 207.148.109.242. Malware intended to set up a Command and Control connection to attack to use input capture tools the malware was code with.

Date: 3 Aug 2023	**Entry:** #3
Description	Data breach affecting 1 million+ users
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ Individual who gained unauthorized access to customer PII ● **What** happened?

	○ Employee received an email from an external email address informing them data had been stolen and demanded a payout of $25,000. ○ Employee deleted email assuming spam. ○ Same email address sentincreased ransom demand of $50,000 and sample of stolen data. ○ Employee reported this to the incident response team. ○ Incident response concentrated on discovering how the data was stolen ● **When** did the incident occur? ○ 3:13 p.m., PT, on December 22, 2022, Employee received an email from an external email address informing them data had been stolen and demanded a payout. ○ Employee deleted email assuming spam. ○ December 28, 2022, same address delivered same email with increased ransom demands and sample of stolen data ○ Employee reported this to the incident response. ○ December 28 and December 31, 2022, Incident response concentrated on discovering how the data was stolen ● **Where** did the incident happen? ○ Mid-sized retail company that does business in e-commerce ● **Why** did the incident happen? ○ Vulnerability identified in e-commerce websites. ○ Force browser attack allowed attacker access to customer purchase orders and their PII ○ Attacker used this information to ransom customer information
Additional notes	Information about data breach was passed onto customers and were offered free identity protection services as compensation. Recommendations from the final report: ● Perform routine vulnerability scans and penetration testing.

	● Implement the following access control mechanisms: ○ Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range. ○ Ensure that only authenticated users are authorized access to content.

Date: 5 Aug 2023	**Entry:** #4
Description	Investigation into suspected phishing
Tool(s) used	Chronicle

The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ Suspected phishing attacks that own the IP address 40.100.174.34 ● **What** happened? ○ Chronicle search of domain name `signin.office365x24.com` returns suspicious activity. Threat intelligence says the site is used as a “Drop site for logs and stolen credentials”. ○ 2 POST requests to “login.php” were made after 6 GET requests, each POST suggests successful phishing attempts and login. ○ Victims where being redirected to another domain 40.100.174.34 ● **When** did the incident occur? ○ Attacks happened on: 2023-01-31, 2023-07-08 and 2023-07-09 ● **Where** did the incident happen? ○ At domain name `signin.office365x24.com` ● **Why** did the incident happen? ○ Successful phishing attempt on unsuspecting victims
Additional notes	The assets that were victims of the phishing attacker were also found on chronicle: The names are: ● Ashton-davidson-pc ● emil-palmer-pc

---

Date:	**Entry:**

5 Aug 2023	#5
Description	Investigation of failed SSH logins
Tool(s) used	Splunk

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ Mail server had more than 100 failed SSH login attempts when searching for failure on the “mailsv” host
	• **What** happened?
	  ○ 346 Failed Password entry for root user as alert message describes the event
	• **When** did the incident occur?
	  ○ Every day at 01:39:51.000 between 27/02/2023 and 06/03/2023
	• **Where** did the incident happen?
	  ○ Ecommerce Company, Buttercup Games
	• **Why** did the incident happen?
	  ○ Appears to be a brute force attack

Additional notes	Strongly suggest MFA to ensure lowered success for attackers

---

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.

- Splunk and Chronicle are very useful tools to search logs and do log analysis
- The variety of attacks that can be discovered using tools such as Splunk and Chronicle combined with methodologies such as the Pyramid of Pain makes identifying threats more streamlined
- IoC and IoA are very intuitive methods of detection
- There are many many forms of detecting threats and analyzing them