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: 3/19/2024	**Entry: 1**
Scenario/ Description	A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. 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. Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key. The attackers were able to gain access into the company's network by using 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. Once the attackers gained access, they deployed their ransomware, which

	encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.
Tool(s) used	Ransomware, encryption, decryption key, phishing emails, ransomware
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ An organized group of unethical hackers ● **What** happened? ○ The unethical hackers targeted phishing emails to gain access to the company's network, they then used ransomware to encrypt critical files. A ransom note was then sent to employees demanding a large sum of money in exchange for the decryption key. ● **When** did the incident occur? ○ Tuesday at 9:00 a.m. ● **Where** did the incident happen? ○ At a small U.S. health care clinic ● **Why** did the incident happen? ○ The unethical hackers were looking to receive a large sum of money in exchange for the decryption key to the locked critical files.
Additional notes	Include any additional thoughts, questions, or findings. - The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

Date: 3/26/24	**Entry: 2.1**
Scenario/ Description	You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer. You investigate this alert and discover that the 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. You retrieve the malicious file and create a SHA256 hash of the file. You might recall from a previous course that a hash function is an algorithm that produces a code that can't be decrypted. Hashing is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint. Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file. Here is a timeline of the events leading up to this alert: ● 1:11 p.m.: An employee receives an email containing a file attachment. ● 1:13 p.m.: The employee successfully downloads and opens the file. ● 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer. ● 1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC.

Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ An unknown threat actor using email phishing ● **What** happened? ○ An employee downloaded a suspicious file attachment in an email sent to them. As a result a malicious payload was executed on their computer. ● **When** did the incident occur? ○ Around 1pm; date unknown ● **Where** did the incident happen? ○ On an employee computer at a financial services company. ● **Why** did the incident happen? ○ A threat actor sent an email with a malicious payload to infect the computer/network work with malware
Additional notes	

Date: 3/27/24	**Entry: 2.2**
Scenario/ Description	You are a level-one security operations center (SOC) analyst at a financial services company. Previously, you 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 as malicious. Now that you have this information, you must follow your organization's process to complete your investigation and resolve the alert. Your organization's security policies and procedures describe how to respond to specific alerts, including what to do when you receive a phishing alert. In the playbook, there is a flowchart and written instructions to help you complete your investigation and resolve the alert. At the end of your investigation, you will update the alert ticket with your findings about the incident.
Tool(s) used	Ticketing simulation
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> ● **What** happened? ○ The attacker posed as a job applicant sending a password protected resume and cover letter. The password protected file ended up being a phishing email containing malware. ● **When** did the incident occur? ○ Wednesday, July 20, 2022 09:30:14 AM ● **Where** did the incident happen? ○ The phishing email was sent to an HR hiring manager within the financial services company ● **Why** did the incident happen? ○ The attacker intended to infiltrate the company's systeme to disseminate malware.
Additional notes	Phishing email was sent to <hr@inergy.com> <176.157.125.93>

	Response to ticket: The investigator has chosen to escalate this ticket due to a high likelihood of it being malicious. The first reason for this is that the file hash is known for being malicious and has a high vendor's ratio on VirusTotal.com. Secondly, when the file was opened multiple unauthorized executable files were created on the employee's computer. Until we can rule out the files being malicious, escalation is necessary.

Date: 3/27/24	**Entry: 3**
Description	You recently joined the security team as a level-one security operation center (SOC) analyst at a mid-sized retail company. Along with its physical store locations, your company also conducts operations in e-commerce, which account for 80% of its sales. The organization experienced a security incident during which an individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information. Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential loss of revenue. The incident is now closed and a thorough investigation has been conducted.
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? ○ Unnamed attacker ● **What** happened?

	○ The attacker gained access to customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated. ● **When** did the incident occur? ○ December 28, 2022, at 7:20 p.m., PT ● **Where** did the incident happen? ○ E-commerce store ● **Why** did the incident happen? ○ The threat actor intended to us customer PII in exchange for $50,000
Additional notes	Recommendations: ● 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: 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.