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: 01/17/2024	**Entry:** Entry: #1
Description	This is a Cybersecurity incident documentation of a ransomware attack that took place within a small U.S. Health care clinic. This incident occurred in two phases of the NIST incident response lifecycle: **Phase 1**: Detection and Analysis: In the Detection phase, the organization detected the ransomware incident. In the Analysis phase, several other organizations were contacted by the organization for assistance with the ransomware attack. **Phase 2**: Containment, Eradication, and Recovery: The organization detailed some of the steps they took to contain the incident (i.e., the company computer systems were shut down.). Since the company could not independently eradicate and recover from this incident, they contacted several other organizations for assistance.
Tool(s) used	none.

The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An organized group of unethical hackers caused the incident. • **What** happened? A ransomware security incident • **When** did the incident occur? The incident occurred on Tuesday at approximately 9:00 a.m. • **Where** did the incident happen? The incident occurred in a small U.S. Healthcare clinic. • **Why** did the incident happen? The hacker group sent several phishing emails to employees containing a malicious attachment, which ultimately initiated a ransomware attack that disrupted business operations and company access to patient files. The attackers' motivation appears to be financially driven, as they left a ransom note demanding a large payment in exchange for a decryption key.
Additional notes	Include any additional thoughts, questions, or findings. 1. Should the company pay the ransom? 2. How could this be prevented from happening in the future?

Date: 02/26/2024	**Entry:** Entry #2
Description	Investigate a suspicious file hash. An employee received an email with an attached spreadsheet. The employee downloaded the file, which executed a malicious payload onto their computer. This incident occurred in the Detection and Analysis phase of the NIST incident response lifecycle. The suspicious file was detected by the security systems

	within the SOC. As the security analyst, I conducted a thorough analysis and investigation of the suspicious file hash to determine if this incident was indeed a real threat.
Tool(s) used	VirusTotal was used as an investigative tool to analyze URLs and files for malicious content. VirusTotal analyzed the file hash that was reported as malicious. VirusTotal is beneficial in that it allows the user to quickly determine if an indicator of compromise, such as a file or website, has been reported by the cybersecurity community as malicious. The intrusion detection system detected the files and sent an alert to the SOC. SHA-256 hash file was created of the file and further investigation was done to determine if this was a definite threat.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An unknown malicious actor. • **What** happened? The employee received an email with a password-protected file. The password was provided in that email. The employee opened the file using the provided password, which unloaded the malicious payload onto their computer. The SHA-256 file had a hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. • **When** did the incident occur? At 1:11 p.m., The employee received the email. At 1:13 p.m., the employee successfully downloaded and opened the file. At 1:20 p.m., the alert was sent to the organization's SOC after the intrusion detection system detected the file. • **Where** did the incident happen? The incident occurred within the financial services office at the employee's computer. • **Why** did the incident happen? The incident occurred after a successful phishing attempt when the employee downloaded a malicious file via email.

Additional notes	Additional staff security training/awareness may be needed to prevent future phishing attempts from being successful.

Date: 2/27/2024	**Entry:** Entry #3
Description	After investigating the email, the attachment has been verified as malicious. Working towards resolving this alert. This incident occurred in the Detection and Analysis phase of the NIST incident response lifecycle due to detecting and assessing an email for malicious content.
Tool(s) used	VirusTotal.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An employee opened the email attachment, activating the malware. • **What** happened? Phishing attempt. The employee received an email from what appeared to be an applicant for an internal role. The attachment was described by the threat actor as a resume. • **When** did the incident occur? The employee received the email on Wednesday, July 20, 2022, at 09:30:14 AM. • **Where** did the incident happen? The incident occurred within the financial services office at the employees' workstation. • **Why** did the incident happen? The threat actor sent a malicious link posing as a resume for employment.
Additional notes	This phishing alert appears to be legitimate, as it contains misspellings in the email. Also, the sender's email address does not match the name within the

	email. The file is also listed as an executable file ("bfsvc.exe").

Date: 3/25/2023	**Entry:** Entry #4:
Description	As a security analyst, I have been tasked with identifying failed SSH logins with Buttercup games' mail servers. This incident investigation occurred in the Detection and Analysis phase, since we are detecting and assessing whether there were any failed SSH logins.
Tool(s) used	Splunk was used to detect and further assess the incident.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Multiple users. • **What** happened? There are over 600 failed SSH logins for the root account on the mail server. • **When** did the incident occur? Between February 27, 2023, and March 06, 2023. • **Where** did the incident happen? Multiple devices. • **Why** did the incident happen? Users entered the incorrect login information.
Additional notes	Include any additional thoughts, questions, or findings.

Date: 3/26/2024	**Entry:** Entry #5
Description	A suspicious domain was contained in an email body: signin.office365x24.com. It appears to be a phishing email. As a security analyst, I am tasked with investigating if others have received this email. This incident occurred in the Detection and Analysis phase. A
Tool(s) used	Google Chronicle was used to investigate and further assess the incident.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An unknown hacker. A phishing email, and subsequent access by employees. • **What** happened? An employee received a phishing email and clicked on the link. I reviewed the email and discovered a suspicious domain name in the email body: signin.office365x24.com. After further review, several other users (listed below) have also clicked on the malicious link. These assets accessed the domain: ashton-davidson-pc First accessed: January 31, 2023 Last accessed: July 09, 2023 bruce-monroe-pc First accessed: January 31, 2023 Last accessed: July 09, 2023 coral-alvarez-pc First accessed: January 31, 2023 Last accessed: July 09, 2023 emil-palmer-pc First accessed: January 31, 2023 Last accessed: July 09, 2023 jude-reyes-pc First accessed: January 31, 2023 Last accessed: July 09, 2023 roger-spence-pc

	First accessed: January 31, 2023 Last accessed: July 09, 2023 Viewing the timeline, the following may have been successfully phished, as determined by the 'post' request on "/login.php". - Emil-palmer-pc - Ashton-davidson-pc Further investigating the Resolved IP 40.100.174.34, I found that the following assets may have been successfully phished, given the post request. - Emil-palmer-pc - Ashton-davidson-pc - warren-morric-pc ● **When** did the incident occur? January 31, 2023. ● **Where** did the incident happen? Financial services company computers. ● **Why** did the incident happen? An unknown hacker sent a phishing email with a malicious link. Employees clicked on the domain within the phishing email.
Additional notes	Should the company provide security training?

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.

1. Were there any specific activities that were challenging for you? Why or why not? The activities were not exactly challenging in themselves. However, approaching a new software tool such as Splunk or Chronicle, was a little daunting. I anticipated some difficulty but soon realized, as with many things in life, just taking one step at a time is all that's needed to accomplish a task.

2. Has your understanding of incident detection and response changed since taking this course? My understanding of incident detection and response has mainly been changed by filling in the huge knowledge gap I had coming into this course. I knew cybersecurity analysts protected devices and networks, however, I was unaware of exactly how they implemented that protection. Throughout this course, I learned about the NIST incident response lifecycle, and that greatly assisted in my understanding of how security analysts respond to incidents.

3. Was there a specific tool or concept that you enjoyed the most? Why? The tools I enjoyed using most were Splunk and Chronicle, simply because it appears that these tools would be highly useful as a cybersecurity analyst.