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: August 9, 2023	**Entry:** #1
Description	Documenting ransomware attack on a U.S. healthcare clinic, disrupting primary-care services and business operations, while conducting thorough review and documentation of the incident details.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. ● **Who:** An organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. ● **What:** Several employees reported that they were unable to use their computers to access files like medical records. ● **When:** The incident occurred on a Tuesday at 9:00am. ● **Where:** The incident happened at a small U.S. health care clinic. ● **Why:** The incident happened because an unethical hacker group was able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation

	was financial because of the ransom note they left demanding a large sum of money in exchange for the decryption key.
Additional notes	● How could the health care company prevent an incident like this from occurring again? ● Has there been quarterly training for employees to be self aware of phishing emails?

Date: August 12, 2023	**Entry:** #2
Description	Leveraged VirusTotal to investigate a potential phishing attack by threat actor, tracking event timeline for comprehensive analysis.
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● A malicious threat actor by the name of BlackTech ● Employee downloaded a trojan file from a phishing email. ● Incident occurred at 1:15pm ● Internal inside the financial services company. ● This security incident occurred due to the actions of the malicious actor BlackTech, who conducted a successful phishing attack. They exploited an employee’s action of downloading a trojan file named Flagpro, which granted unauthorized access. Upon execution, this trojan proceeded to run multiple files on the compromised computer, allowing the attacker to potentially control and exploit the system.

Additional notes	Has there been quarterly on phishing email awareness and what do once you suspect one? How can this incident be prevented in the future?

Date: August 13, 2023	**Entry:** #3
Description	Following a phishing alert, a financial services firm applied the phishing playbook to assess the downloaded suspicious file and ascertain appropriate follow-up measures.
Tool(s) used	Phishing Playbook
The 5 W's	Capture the 5 W's of an incident. ● Malicious threat actor by the name of BlackTech. ● A Trojan file was downloaded that sent an alert message. ● The incident occurred at 1:15pm. ● The incident where it occurred was internal by an employee. ● The security incident occurred because a user unwittingly interacted with a malicious email, leading them to download a harmful attachment. The subsequent security alert was triggered as a potential phishing attempt. The threat actor BlackTech exploited this by deploying the Flagpro Trojan through the download attachment, which initiated the execution of multiple executable files in an attempt to establish unauthorized command and control over the compromised system.
Additional notes	Include any additional thoughts, questions, or findings.

Date: August 13, 2023	**Entry:** #4
Description	Assessed conclusive report on significant security incident at medium-sized retail firm. Determined incident details, timeline, response, and proposed future measures after thorough review.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● An external malicious threat actor ● Customer’s PII was stolen and held for ransom ● Occurred on December 28, 2022 at 7:20pm PT. ● On the company’s e-commerce web application ● There was a vulnerability in the site that allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated.
Additional notes	Include any additional thoughts, questions, or findings.

Date: August 14, 2023	**Entry:** #5
Description	Examined potential security concern at Buttercup Games, focusing on failed SSH logins via Splunk SIEM tools. Summarized findings in an outlined timeline.
Tool(s) used	Splunk
Outline	Upon accessing the Splunk dashboard, the security analyst initiated a log analysis on a data file to address a potential security concern. The initial search was performed using the query “index=main” with a time range parameter set to “All Time.” The outcome displayed 109,864 events in the log data originating from 5 hosts. To refine the investigation, the analyst selected the “mailsv” host under “SELECTED FIELDS,” narrowing the events down to 9,829. Focusing on events associated with the mail server, a search was conducted for failed SSH logins by inputting the query “index=main host=mailsv fail* root.” As a result, the events were further reduced to 346 instances. Notably, these failed attempts occurred consistently at 1:39am each day between February 28, 2023 and March 6, 2023. Given the concentrated failed attempts during non-business hours, this pattern suggests the involvement of a malicious threat actor.
Additional notes	Include any additional thoughts, questions, or findings.

Date: August 14, 2023	**Entry:** #6
Description	Examined financial services firm’s potential phishing incident alert by Chronicle SIEM. Investigated phishing attempt, outlining findings with a detailed incident

	timeline.
Tool(s) used	Chronicle
Outline	Upon reviewing the Chronicle dashboard, the security analyst responded to an alert concerning a potential phishing email. Our investigation led us to a suspicious domain, signin.office365x24.com, which was confirmed to exist in the ingested data. The threat intelligence from VT Context identified this domain as malicious, categorized as “Drop site for logs or stolen credential,” with a medium severity level according to the ET Intelligence Rep list. The incident occurred on January 31, 2023 between 2:40 pm and 2:51 pm. The Resolved IP address associated with the incident was successfully blocked at a high severity level. The analysis indicated that 8 users’ assets accessed the malicious domain, and an additional domain, signin.accounts-google.com, was linked to the same Resolved IP address. Due to the serious nature of this security threat, the incident is being escalated to a Level 2 SOC analyst for further review.
.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.

---

1. Were there any specific activities that were challenging for you? Why or why not?

   The specific activities that were challenging for me was the Splunk and Chronicle dashboard. Having a clear understanding of what I’m looking for to get the answers I needed then implementing those results into the incident journal had me stumped for a moment. I wasn’t sure on how I should format my entry when the 5 Ws did not align with the activity at hand.

2. Has your understanding of incident detection and response changed since taking this course?

   My understanding of incident detection and response has changed my outlook not only on how to respond to security incidents, but also navigating everyday life problems.It has presented to me a whole new perspective and appreciation on Cybersecurity and has only furthered my aspirations of entering into this career field.

3. Was there a specific tool or concept that you enjoyed the most? Why?

   I would say even though it was challenging the SIEM tools I still enjoyed learning them. My interest in learning new tools and being able to navigate and tinker with tools to find the answer for the problem that I need to solve gives me a sense of enjoyment and satisfaction. I look forward to expanding my knowledge on these tools and new avenues.