# 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:** 03/05/2024 | **Entry:** #1 |
|---|---|
| Description | Documenting a cybersecurity incident.<br><br>**Key Details of the scenario**:<br>- A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations.<br>- The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files.<br>- An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key |
| Tool(s) used | None |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who** caused the incident?<br>  ○ An organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. |

| | |
|---|---|
| | • **What** happened?<br>  ○ 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. This was because the unethical hackers encrypted critical files via ransomware.<br>• **When** did the incident occur?<br>  ○ It happened on a Tuesday morning at approximately 9:00am.<br>• **Where** did the incident happen?<br>  ○ A small U.S. health care clinic specializing in delivering primary-care services<br>• **Why** did the incident happen?<br>  ○ The incident happened because unethical hackers were 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 appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key. |
| Additional notes | I wonder what the small-clinic could have done to prevent an incident like this from occurring again? With smaller businesses, it is harder to allocate necessary resources toward a cybersecurity department to help inform employees on the dangers of phishing emails. |

| **Date:** 03/20/24 | **Entry:** #2 |
|---|---|
| Description | **Key Details of the scenario**:<br>- I am working as a SOC level 1 analyst that received an alert about a suspicious file being downloaded on an employee's computer<br>Here is a timeline of the events leading up to this alert:<br>- **1:11 p.m.**: An employee receives an email containing a file attachment.<br>- **1:13 p.m.**: The employee successfully downloads and opens the file.<br>- **1:15 p.m.**: Multiple unauthorized executable files are created on the employee's computer.<br>- **1:20 p.m.**: An intrusion detection system detects the executable files and sends out an alert to the SOC. |
| Tool(s) used | List any cybersecurity tools that were used: File hash used for VirusTotal tool: SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who** caused the incident?<br>○ An employee working for a financial service company<br>● **What** happened?<br>○ The employee received an email with an attachment that they downloaded and subsequently executed malicious file<br>● **When** did the incident occur?<br>○ Afternoon<br>● **Where** did the incident happen?<br>○ A financial services company<br>● **Why** did the incident happen?<br>○ Because an employee unknowingly downloaded a malicious file from an email attachment. |
| Additional notes | Include any additional thoughts, questions, or findings. |

| **Date:** 03/22/24 | **Entry:** #3 |
|---|---|
| Description | **Key Details of the scenario**:<br>- The organization experienced a security incident on December 28, 2022, at 7:20 p.m., PT, 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 | None |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who** caused the incident?<br>○ A threat actor<br>● **What** happened?<br>○ An employee of a mid-sized retail company received an email that stated a threat actor had successfully stolen customer transaction data and demanded a ransom of $25,000 in exchange for not releasing the data on a public forum on December 22, 2022. The employee assumed the email was spam and deleted it. That same employee received another email that included a sample of the stolen customer data and demanded $50,000 ransom this time.<br>● **When** did the incident occur? |

| | |
|---|---|
| | ○ December 22, 2022 and again on December 28, 2022<br>● **Where** did the incident happen?<br>○ At a mid-sized retail company<br>● **Why** did the incident happen?<br>○ The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability 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 vulnerability 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:** 03/26/24 | **Entry:** #4 |
|---|---|
| Description | **Key Details of the scenario**:<br>- You are a security analyst at a financial services company. You receive an alert that an employee received a phishing email in their inbox. You review the alert and identify a suspicious domain name contained in the email's body: signin.office365x24.com. You need to determine whether any other employees have received phishing emails containing this domain and whether they have visited the domain. You will use Chronicle to investigate this domain. |
| Tool(s) used | Google Chronicle |

| | |
|---|---|
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who** caused the incident?<br>○ A threat actor<br>● **What** happened?<br>○ An alert was sent to the security team after an employee received a phishing email in their inbox<br>● **When** did the incident occur?<br>○ 01/31/2023<br>● **Where** did the incident happen?<br>○ A financial services company<br>● **Why** did the incident happen?<br>○ The root cause of this incident was several employees clicking a link in a phishing email that redirected them to a malicious domain. |
| Additional notes | Assets on Chronicle that have accessed the domain: 6<br>- Ashton-Davidson, provided data to the malicious server<br>- Bruce-Monroe<br>- Coral-Alvarez<br>- Emil-Palmer, provided data to the malicious server<br>- Jude-Reyes<br>- Roger-Spence<br>Other domains associated with this IP include: signin.accounts-google.com and signin.office365x24.com |

---

Reflections/Notes:

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

- There were not any specific activities that were challenging for me. The incident handler's journal provided a very manageable way of organizing information for each scenario.

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

- Yes, my understanding of the incident detection and response process has changed since taking this course as the detail and system in which you go through responding to incidents is more systematic. I understand that in cybersecurity efficiency is key so reducing any steps that take longer time to do and having better organization brings urgency to a subject where speed matters.

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

- I enjoyed using VirusTotal the most as it allowed me to have another resource I could use on my own to quickly see if a website/URL/file is malicious based on community input. It further builds my toolbox of items to use to maximize efficiency in working as a future cybersecurity professional.