**Incident handler's journal (My Responses)**

**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:**  Record the date of the journal entry.  10/1/2025 | **Entry:**  Record the journal entry number.  #1 |
| Description | Provide a brief description about the journal entry.  A report on a cybersecurity incident at a heath care clinic. |
| Tool(s) used | List any cybersecurity tools that were used.  N/A; This is writing a report and details provided in scenario. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? An organized group of unethical hackers breaching a company. * **What** happened? A ransomware cyber security incident/hacking. * **When** did the incident occur? It occurred at a small heath care clinic company in the U.S. specializing in delivering primary-care services. * **Where** did the incident happen? The cyber incident happened on a Tuesday morning approximately 9:00 am. * **Why** did the incident happen? The ransomware incident happened at a small healthcare clinic in the U.S. on a Tuesday morning around 9:00 a.m., when employees suddenly found they couldn’t access important files, like patient medical records. It turned out that some staff members had received phishing emails with a sketchy attachment. When someone opened the attachment, it installed malware that gave hackers access to the clinic’s systems. From there, the hackers who are an organized group known for targeting healthcare and transportation companies, launched a ransomware attack that locked up all the clinic’s critical files. A ransom note popped up on multiple computers, demanding a large sum of money in exchange for the decryption key. The message made it clear that this was all about money. The attack caused major disruptions since no one could do their job without access to the clinic’s systems. As a result, the clinic had to shut everything down and reach out to different organizations for help dealing with the situation. |
| Additional notes | Include any additional thoughts, questions, or findings.  **1. Prevention Steps:**   * **Employee training:** Regular cybersecurity awareness training to help staff spot phishing emails and avoid downloading malicious attachments. * **Email filtering & anti-malware tools:** Use advanced email security to block phishing attempts and malware before they reach users. * **Multi-factor authentication (MFA):** Adds extra security to employee logins. * **Regular data backups:** Store backups offline and test them regularly to ensure fast recovery without paying ransom. * **Access control:** Limit employee access to only what they need, reducing damage if an account is compromised. * **System updates:** Keep all software and systems up to date to patch known vulnerabilities. * **Incident response plan:** Prepare a clear plan for responding quickly to future attacks. * **Security audits:** Regular checks to find and fix system weaknesses.   **2. Ransom pay or not pay?**   * **Generally, no – paying is not recommended** because:   + There’s **no guarantee** the hackers will provide a working decryption key.   + It **encourages more attacks** and funds criminal activity.   + **Stolen data** may still be leaked or sold. * **Instead, the company should:**   + Try restoring data from **secure backups**.   + Report the attack to the **FBI, CISA, and legal authorities**.   + Work with cybersecurity experts to investigate and recover. * **Exceptions might be considered** if:   + Backups are unavailable or also encrypted.   + Patient care is at risk due to inaccessible data. * **Legal risks:** Paying ransom to certain groups could violate U.S. sanctions and be illegal. |

**Scenario:**

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.

**Step 2: Review the scenario**

Review the details of the scenario. Consider the following key details:

* A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations.
* 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.
* 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

**Step 3: Record a journal entry**

Use the incident handler's journal to document your first journal entry about the given scenario. Ensure that you fill in all of the fields:

1. In the **Date** section, record the date of your journal entry. This should be the actual date that you record the entry, not a fictional date.
2. In the **Entry** section, provide a journal entry number. For example, if it is your first journal entry, enter 1.
3. In the **Description** section, provide a description about the entry.
4. In the **Tool(s) used** section, if any cybersecurity tools were used, list them here.
5. In the **The 5 W's** section, record the details about the given scenario.
   1. Who caused the incident?
   2. What happened?
   3. When did the incident occur?
   4. Where did the incident happen?
   5. Why did the incident happen?
6. In the **Additional notes** row, record any thoughts or questions you have about the given scenario.

**What to Include in Your Response**

Be sure to include the following elements in your completed activity:

* The journal entry date and number
* A description of the journal entry
* 1-2 sentences addressing each of the 5 W's of the scenario:
  + Who caused the incident?
  + What happened?
  + When did the incident occur?
  + Where did the incident happen?
  + Why did the incident happen?
* 1-2 sentences on any additional thoughts or questions about the scenario.

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. 10/3/2025 | **Entry:**  Record the journal entry number.  2 |
| Description | Provide a brief description about the journal entry.  Malicious file downloaded by employee; malware execution detected. |
| Tool(s) used | List any cybersecurity tools that were used.  **VirusTotal, SHA256 hashing tool** |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Employee unknowingly triggered the incident by downloading the malicious attachment. * **What** happened? Employee received a malicious email attachment, entered the password, and opened the file, causing malware to execute. * **When** did the incident occur? The incident occurred on 10/3/2025, between 1:11 p.m. and 1:20 p.m. * **Where** did the incident happen? The incident occurred on the employee’s computer at their workplace. * **Why** did the incident happen? The employee was targeted through a phishing email containing a password-protected malicious file, which they unknowingly opened. |
| Additional notes | Include any additional thoughts, questions, or findings.  The file was identified as **Flagpro** malware, commonly used by the BlackTech threat group. The hash was reported as malicious by over 50 vendors on VirusTotal. Additional indicators of compromise were collected, including other hash values, IP addresses, and network artifacts associated with the file.  - The **SHA256 hash** of the malicious file is **54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b**.  - **VirusTotal** flagged this file as malicious based on results from over **50 security vendors**.  - The file is identified as **Flagpro** malware, commonly used by the **BlackTech** APT (Advanced Persistent Threat) group. This actor is known for sophisticated attacks targeting financial institutions.  - The malware was executed on the employee's computer at **1:13 p.m.**, triggering multiple unauthorized **executable files** to be created at **1:15 p.m.**  - An **intrusion detection system (IDS)** flagged the incident at **1:20 p.m.**, and the SOC was alerted.  - The malware appears to leverage **social engineering tactics**, as the employee was lured into opening a password-protected file.  - **Indicators of Compromise (IoCs)** associated with the file include additional **hashes (MD5, SHA-1)**, **IP addresses**, and **domain names**. The investigation is ongoing, and the file’s behavior is currently being analyzed in more depth.  - A potential **remediation strategy** could involve **blocking** any associated **domains** and **IP addresses** identified during this investigation. Further **network traffic analysis** is needed to understand the full extent of the compromise.  - The incident may have potential ties to other **historical** attacks associated with **BlackTech**. Further monitoring of the employee’s system and internal network is recommended to ensure no persistence mechanisms remain. |

**Notes: Review the following scenario. Then complete the step-by-step instructions.**

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.

Note: Use the incident handler's journal you started in a previous activity

to take notes during the activity and keep track of your findings.

Note: You might recall creating SHA256 hashes in the lab activity on hash values

from a previous course. Step 2: Review the details of the alert

The following information contains details about the alert that will help you complete this activity. The details include a file hash and a timeline of the event. Keep these details for reference as you proceed to the next steps.

SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

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.

Step 3: Enter the file hash into VirusTotal

Go to the VirusTotal website

. Click SEARCH, enter the SHA256 file hash in the search box, and press enter. The SHA256 file hash is listed in Step 2 of this activity.

Note: For the purpose of this activity, you'll focus on evaluating VirusTotal results. However, no single tool can detect all types of malicious activity. Security analysts will often use a combination of other tools to carefully evaluate the results of a scan before making a decision about the file.

Step 4: Analyze the VirusTotal report

Once you've retrieved VirusTotal's report on the file hash, take some time to examine the report details. You can start by exploring the following tabs:

Detection: This tab provides a list of third-party security vendors and their detection verdicts on an artifact. Detection verdicts include: malicious, suspicious, unsafe, and others. Notice how many security vendors have reported this hash as malicious and how many have not.

Details: This tab provides additional information extracted from a static analysis of the IoC. Notice the additional hashes associated with this malware like MD5, SHA-1, and more.

Relations: This tab contains information about the network connections this malware has made with URLs, domain names, and IP addresses. The Detections column indicates how many vendors have flagged the URL or IP address as malicious.

Behavior: This tab contains information related to the observed activity and behaviors of an artifact after executing it in a controlled environment, such as a sandboxed environment. A sandboxed environment is an isolated environment that allows a file to be executed and observed by analysts and researchers. Information about the malware's behavioral patterns is provided through sandbox reports. Sandbox reports include information about the specific actions the file takes when it's executed in a sandboxed environment, such as registry and file system actions, processes, and more. Notice the different types of tactics and techniques used by this malware and the files it created.

Pro tip: Sandbox reports are useful in understanding the behavior of a file, but they might contain information that is not relevant to the analysis of the file. By default, VirusTotal shows all sandbox reports in the Behavior tab. You can select individual sandbox reports to view. This is helpful because you can view the similarities and differences between reports so that it's easier to identify which behaviors are likely to be associated with the file.

Step 5: Determine whether the file is malicious

Review the VirusTotal report to determine whether the file is malicious. The following sections will be helpful to review before making this determination:

The Vendors' ratio is the metric widget displayed at the top of the report. This number represents how many security vendors have flagged the file as malicious over all. A file with a high number of vendor flags is more likely to be malicious.

The Community Score is based on the collective inputs of the VirusTotal community. The community score is located below the vendor's ratio and can be displayed by hovering your cursor over the red X. A file with a negative community score is more likely to be malicious.

Under the Detection tab, the Security vendors' analysis section provides a list of detections for this file made by security vendors, like antivirus tools. Vendors who have not identified the file as malicious are marked with a checkmark. Vendors who have flagged the file as malicious are marked with an exclamation mark. Files that are flagged as malicious might also include the name of the malware that was detected and other additional details about the file. This section provides insights into a file's potential maliciousness.

Review these three sections to determine if there is a consistent assessment of the file's potential maliciousness such as: a high vendors' ratio, a negative community score, and malware detections in the security vendors' analysis section.

In the first slide of your Pyramid of Pain template, indicate whether this file is malicious. Then, explain your reasoning based on your findings.

Note: The Vendors' ratio is based on security vendors' detections and vendors might not always detect malicious files. The Community Score is based on the opinions and insights from the VirusTotal community. If a file's scores are low, it doesn't necessarily mean that the file is safe. It is recommended to use multiple sources of information when evaluating files.

Step 6: Fill in the template with additional indicators of compromise

After you've explored the sections in the VirusTotal report, you will uncover additional IoCs that are associated with the file according to the VirusTotal report.

Identify three indicators of compromise (IoCs) that are associated with this file hash using the tabs in the VirusTotal report. Then, enter the IoCs into their respective sections in the Pyramid of Pain template.

Indicators of compromise are valuable sources of information for security professionals because they are used to identify malicious activity. You can choose to identify any three of the six types of IoCs found in the Pyramid of Pain:

Hash value: Hashes convert information into a unique value that can't be decrypted. Hashes are often used as unique references to files involved in an intrusion. In this activity, you used a SHA256 hash as the artifact for this investigation. Find another hash that's used to identify this malware and enter it beside the Hash values section in the Pyramid of Pain template. You can use the Details tab to help you identify other hashes.

IP address: Find an IP address that this malware contacted and enter it beside the IP addresses section in the Pyramid of Pain template. You can locate IP addresses in the Relations tab under the Contacted IP addresses section or in the Behavior tab under the IP Traffic section.

Domain name: Find a domain name that this malware contacted and enter it beside the Domain names section in the Pyramid of Pain template. You can find domain name information under the Relations tab. You might encounter benign domain names. Use the Detections column to identify domain names that have been reported as malicious.

Network artifact/host artifact: Malware can create network-related or host-related artifacts on an infected system. Find a network-related or host-related artifact that this malware created and enter it beside the Network/host artifacts section in the Pyramid of Pain template. You can find this information from the sandbox reports under the Behavior tab or from the Relations tab.

Tools: Attackers can use tools to achieve their goal. Try to find out if this malware has used any tool. Then, enter it beside the Tools section in the Pyramid of Pain template.

Tactics, techniques, and procedures (TTPs): TTPs describe the behavior of an attacker. Using the sandbox reports from the Behavior tab, find the list of tactics and techniques used by this malware as identified by MITRE ATT&CK® and enter it beside the TTPs section in the Pyramid of Pain template.

Note: VirusTotal reports can contain legitimate domains and IP addresses that are not considered malicious.

Pro tip: To learn more about a section in VirusTotal, hover your cursor over the information icon to display information on what that section includes.

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry.  10/26/2025 | **Entry:**  Record the journal entry number.  #3 |
| Description | Provide a brief description about the journal entry.  Analyzing a packet capture file |
| Tool(s) used | List any cybersecurity tools that were used.  Wireshark was used to analyze a packet capture file. Based on the notes and videos, Wireshark is a network protocol analyzer that allows security analysts to capture and analyze network traffic, helping detect and investigate malicious activity. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? N/A * **What** happened? N/A * **When** did the incident occur? N/A * **Where** did the incident happen? N/A * **Why** did the incident happen? N/A |
| Additional notes | Include any additional thoughts, questions, or findings.  The labs helped me demonstrate Wireshark, as I did not use it often in the past, so this was insightful and refreshing to analyze a packet capture file to help understand network traffic. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry.  10/26/2025 | **Entry:**  Record the journal entry number.  #4 |
| Description | Provide a brief description about the journal entry.  Capturing packets demonstration labs |
| Tool(s) used | List any cybersecurity tools that were used.  In the labs, I learned to use tcpdump to capture and analyze network traffic, which is a network protocol analyzer that's accessed using the  command-line interface. This can help capture, filter, and analyze network traffic. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? N/A * **What** happened? N/A * **When** did the incident occur? N/A * **Where** did the incident happen? N/A * **Why** did the incident happen? N/A |
| Additional notes | Include any additional thoughts, questions, or findings.  I’ve used similar tools in past IT classes, but those relied on screenshots instead of hands-on practice. This class let me actually use the keyboard and run tcpdump commands myself, which was a great learning experience. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number.  #4 |
| Description | Provide a brief description about the journal entry.  Investigate a suspicious file hash (Might be a duplciate of #2?) |
| Tool(s) used | List any cybersecurity tools that were used.  **I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It stated to use VirusTotal to analyze a file hash, which was reported as malicious. Note: This incident occurred in the Detection and Analysis phase and after the suspicious file was detected by the security systems in place, I had to determine if the alert signified a real threat (high/low).** |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? unknown malicious actor * **What** happened? email sent to an employee contained a malicious file * attachment with the SHA-256 file hash of * 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **When** did the incident occur? At 1:20 p.m., an alert was sent to the organization's SOC after the * intrusion detection system detected the file * **Where** did the incident happen? An employee's computer at a financial services company * **Why** did the incident happen? An employee was able to download and execute a malicious file * attachment via e-mail. |
| Additional notes | Include any additional thoughts, questions, or findings.  **Prevention:** We could prevent this by improving security training so employees are more careful about what they click.  **Reflections:**   1. **Challenging Activity:** Using **tcpdump** was hard since I’m new to the command line. I kept getting errors at first, but redoing the steps slowly helped me figure it out. I learned to follow instructions carefully. 2. **What I Learned:** This course helped me understand incident detection and response better. I now know more about the incident lifecycle, the tools used, and why plans and processes are important. 3. **Enjoyed the most:**   This course helped me understand learning about network traffic analysis and demonstrated it with the tools through hands-on experience. It was better than some of the past classes I took, which only provided screenshots or just a video demonstration (no hands-on). It was great to have hands-on and show the significance of using these to learn about network tools. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry.  10/26/2025 | **Entry:**  Record the journal entry number.  #5 and #6 |
| Description | Provide a brief description of the journal entry.  Finalize the incident response journal and Labs: 1) Suricata logs and signatures; 2) Query with Wazuh setup. |
| Tool(s) used | List any cybersecurity tools that were used.  Incident handler’s journal and activity labs 1 and 2. (Suricata/Wazuh)  In this lab, I explored Suricata, an open-source IDS/IPS and network analysis tool, by creating and testing custom rules to monitor network traffic. I examined the structure of a Suricata rule, which consists of an action (e.g., alert, drop, pass, reject), a header defining the protocol, source/destination IPs, ports, and traffic direction, and options such as msg, flow, content, sid, and rev. Using a sample packet capture file (sample.pcap) and a custom rules file (custom.rules), I ran Suricata to trigger alerts and analyzed the output in both fast.log (for quick alert checks) and eve.json (a structured JSON log containing detailed network events). I also learned to extract and correlate key information from eve.json, including timestamps, flow IDs, alert signatures, protocols, and destination IPs, providing practical experience in monitoring network traffic, generating alerts, and performing event analysis with Suricata.  In Module 4, I explored log management, detection, and response using tools such as Wazuh and SIEM platforms like Splunk. The course covered best practices for collecting, managing, and analyzing logs, including understanding log formats and components. I practiced the concepts using Wazuh in the optional labs by ingesting sample data, performing searches, evaluating search results, and identifying security events, such as failed SSH logins on a mail server. Key skills included querying data with filters and wildcards, examining event fields such as host and log.file.path, and connecting logs to various internal assets. The exercises reinforced how these tools support effective security monitoring, incident detection, and response in real-world scenarios. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? N/A * **What** happened? N/A * **When** did the incident occur? N/A * **Where** did the incident happen? N/A * **Why** did the incident happen? N/A |
| Additional notes | Include any additional thoughts, questions, or findings.  Learned to explore signatures and logs with Suricata, learned about IDS, and then learned about Wazuh for query. Then, I finalized the journal here. |

### 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. |