**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.

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

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.

|  |  |
| --- | --- |
| **Date:** 7/23/25 | **Entry:** #1 |
| Description | A group of unethical hackers successfully phished some employees with a malicious attachment which was able to encrypt critical files and hold them for ransom. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** **caused the incident?** A group of unethical hackers * **What happened?** Employees were phished via email and critical files were encrypted and held for ransom. * **When** **did the incident occur?** Tuesday at 9:00 A.M. * **Where did the incident happen?** A small U.S. healthcare clinic * **Why** **did the incident happen?** The motivation behind this incident appears to be purely monetary. Once the phishing attempts succeeded, the hackers had everything they needed to execute their plan. |
| Additional notes | The company should be doing a better job of educating their employees about phishing attempts and other various means that unethical hackers use to gain access to a company’s network. |

|  |  |
| --- | --- |
| **Date:** 8/12/25 | **Entry:** #2 |
| Description | I analyzed a packet capture file for the first time. |
| Tool(s) used | Wireshark, a network protocol analyzer with an intuitive GUI. |
| Additional notes | At first, Wireshark is very overwhelming. There are a lot of numbers and unfamiliar lines of text everywhere. After just a few minutes of digesting what was on my screen, it made a lot more sense. I was able to learn how to filter for what I am looking for and analyze the packet once I get there. |

|  |  |
| --- | --- |
| **Date:** 8/14/25 | **Entry:** #3 |
| Description | I captured a packet for the first time. |
| Tool(s) used | Tcpdump, a network protocol analyzer that is similar to Wireshark, but lacks a GUI. |
| Additional notes | I tend to prefer a GUI over the CLI, so using tcpdump was slightly more challenging than Wireshark. Long strings of numbers are much more readable in a decent GUI than the CLI. Despite that, I felt like I was quicker with my work while using tcpdump. |

**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.

|  |  |
| --- | --- |
| **Date:** 8/15/25 | **Entry:** #4 |
| Description | I am to investigate a suspicious file hash that an employee was phished into opening. |
| Tool(s) used | VirusTotal, a website that holds a database of malicious files and other content. Users can vote on these files to let the community know if they are dangerous or not. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who caused the incident?** An unknown malicious actor. * **What happened?** An employee was phished into opening a malicious file attachment. The SHA-256 file hash is 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **When did the incident occur?** N/A * **Where did the incident happen?** A financial services company * **Why did the incident happen?** An employee was phished into opening a malicious file attachment. Once opened, it was able to execute malicious code onto the employee’s computer. |
| Additional notes | VirusTotal is a very simple and helpful tool that is powered by the community. |

**Review the scenario. Then complete the step-by-step instructions.**

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 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.

|  |  |
| --- | --- |
| **Date:** 8/18/25 | **Entry:** #5 |
| Description | I used a playbook to respond to a phishing incident. |
| Tool(s) used | A phishing incident response playbook |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** **caused the incident?** An unknown malicious actor * **What happened?** An employee downloaded a file that was later confirmed to be malicious. I used the playbook to guide my response and it had me evaluate the alert ticket itself, the phishing email, and the email’s attachment. Once I deemed the attachment to be malicious, I escalated the ticket. * **When did the incident occur?** N/A * **Where did the incident happen?** A financial services company * **Why did the incident happen?** This incident happened because of a successful phishing attempt on one of the company’s employees |
| Additional notes | Playbooks make an analyst’s job easier and ultimately takes the stress out of a situation by providing clear step-by-step instructions. |

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

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.

You are spending your first week of training becoming familiar with the company's security processes and procedures. Recently, the company experienced a major security incident involving a data breach of over one million users. Because this was a recent and major security incident, your team is working to prevent incidents like this from happening again. This breach happened before you began working at the company. You have been asked to review the final report. To gain an understanding of the incident's life cycle, your goals for your review are as follows:

* Goal 1: Identify exactly what happened.
* Goal 2: Identify when it happened.
* Goal 3: Identify the response actions that the company took.
* Goal 4: Identify future recommendations.

|  |  |
| --- | --- |
| **Date:** 8/19/25 | **Entry:** #6 |
| Description | As part of my training, I reviewed an incident final report. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** **caused the incident?** A malicious actor * **What happened?** Customer data was stolen via a forced browsing attack. The malicious actor attempted to extort the company in exchange for not releasing the data. * **When did the incident occur?** December 28, 2022 at 7:20 P.M. PT * **Where did the incident happen?** A mid-sized retail company * **Why did the incident happen?** There was a vulnerability in the company’s e-commerce web application. The URL strings for purchase confirmation pages were able to accessed by any IP address. To remediate, the security team implemented allowlisting for those pages. |
| Additional notes | This is a good example of how a huge exploit can be hiding in plain sight. |