**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:** 06/23/2023  Record the date of the journal entry. | **Entry: 1**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. A small U.S. health care clinic experienced a security incident. The company became infected with ransomware which encrypted the company’s files by an organized group of unethical hackers who demanded payment to decrypt the organization's files. | | |
| 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? An organized group of unethical hackers. * **What** happened? The hackers sent out targeted phishing emails that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization’s computer files. * **When** did the incident occur? Tuesday morning, at approximately 9:00 a.m. * **Where** did the incident happen? At a small U.S. health care clinic. * **Why** did the incident happen? The hackers motive appears to be money, they left a note demanding a large sum of money from the healthcare clinic in exchange for restoring access to the encrypted files. | | |
| Additional notes | Include any additional thoughts, questions, or findings. How could the health clinic prevent this from happening again? | | |

| **Date:**  Record the date of the journal entry. | **Entry: 2**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. I received an alert about a suspicious file being downloaded on an employee's computer. | | |
| Tool(s) used | List any cybersecurity tools that were used. Threat Intelligence tool Virustotal.com | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Malicious actor * **What** happened? An employee receives an email containing a file attachment. The employee successfully downloads and opens the file. Multiple unauthorized executable files are created on the employee’s computer. An intrusion detection system detects the executable files and sends out an alert to the security operations center (SOC) * **When** did the incident occur? 1:11p.m, 1:13p.m, 1:15p.m, 1:20p.m. * **Where** did the incident happen? * **Why** did the incident happen? To steal sensitive info | | |
| Additional notes | Include any additional thoughts, questions, or findings. Training employees on the awareness of phishing attempts needs to be implemented. | | |

| **Date:**  Record the date of the journal entry. | **Entry: 3**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. An employee received a phishing email and downloaded the attachment. After investigating the email attachment file's hash, the attachment has already been verified to be malicious. | | |
| Tool(s) used | List any cybersecurity tools that were used. Phishing Playbook with (flowchart). | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Malicious actor * **What** happened? The user may have opened a malicious email and opened attachments or clicked links. * **When** did the incident occur? July 20,2022 at 9:30:14 a.m. * **Where** did the incident happen? At a company named Inergy. * **Why** did the incident happen? To gain access and steal sensitive information. | | |
| Additional notes | Include any additional thoughts, questions, or findings. Training employees on the awareness of phishing attempts needs to be implemented. | | |

| **Date:**  Record the date of the journal entry. | **Entry: 4**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. 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. | | |
| 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? Threat Actor * **What** happened? An employee received an email from an external email address. The email sender claimed that they had successfully stolen customer data. The security team discovered a vulnerability in the e-commerce web application 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. * **When** did the incident occur? 3:13 p.m December 22, 2022, and December 28, 2022 7:20 p.m. * **Where** did the incident happen? The organization's e-commerce website. * **Why** did the incident happen? The attacker’s motive was money, In exchange for not releasing the data to public forums, the sender requested a $50,000 cryptocurrency payment. | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

| **Date:**  Record the date of the journal entry. | **Entry: 5**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. You've been tasked with identifying whether there are any possible security issues with the mail server. | | |
| Tool(s) used | List any cybersecurity tools that were used. Splunk SIEM tool. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Threat actor * **What** happened? I’ve discovered 346 failed login attempts on the mail server. * **When** did the incident occur? From Feb 27, 2023 - March 06, 2023 at 1:39:51 a.m. * **Where** did the incident happen? E-commerce store named Buttercup Games. * **Why** did the incident happen? The threat actor tried to gain access to the company’s mail server to possibly steal PII. | | |
| Additional notes | Include any additional thoughts, questions, or findings. I would implement a password policy and a multi factor authentication set up to help authenticate authorized employee logins. | | |

| **Date:**  Record the date of the journal entry. | **Entry: 6**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. At a financial services company. I received an alert that an employee received a phishing email in their inbox. I need to determine whether any other employees have received phishing emails containing this domain and whether they have visited the domain. | | |
| Tool(s) used | List any cybersecurity tools that were used. Chronicle SEIM tool. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Malicious actor * **What** happened? I reviewed the alert and identified a suspicious domain name contained in the email's body: **signin.office365x24.com**. I discovered that these six employees accessed the signin.office365x24.com suspicious website, Ashton-davidson-pc, bruce-monroe-pc, coral-alvarez-pc, emil-palmer-pc, jude-reyes-pc, roger-spence-pc. These two hosts sent out POST requests to the signin.office365x24.com domain, Ashton-davidson-pc, and emil-palmer-pc. * **When** did the incident occur? January 31, 2023 * **Where** did the incident happen? A Financial services company. * **Why** did the incident happen? To steal host login credentials. | | |
| Additional notes | Include any additional thoughts, questions, or findings. An additional domain was associated with signin.office365x24.com named signin.accounts-google.com. Two additional affected assets have been found Amir-david-pc and warren-morris-pc. One additional POST request was sent to the other domain signin.accounts-google.com by warren-morris-pc. | | |

### 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? Using certain commands for the Suricata tool was a little confusing, I never read up on the jq commands. 2. Has your understanding of incident detection and response changed since taking this course? I have a greater knowledge of the (SEIM) tools that’s used to collect and analyze log data. 3. Was there a specific tool or concept that you enjoyed the most? Why? I really enjoyed working with the Google Chronicle (SEIM) tool, it was fun searching the information to determine who was infected by the malicious domain, and whether or not the suspicious domain was malicious in the first place. |
| --- |