**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.

In the **Description** section in a journal entry in your incident handler's journal, include a brief description of the entry (20-50 words). You can also identify which phase(s) of the NIST Incident Response Lifecycle the incident investigation occurred in and why. As a refresher, the phases are: Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activity.

|  |  |
| --- | --- |
| **Date:** 06/16/2023  Record the date of the journal entry. | **Entry: 1**  Record the journal entry number. |
| Description | Provide a brief description about the journal entry.  This entry is for the Google Cybersecurity Professional certificate Portfolio Activity: Document an incident with an incident handler's journal. And the scenario is:   * 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 |
| Tool(s) used | None |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   organized group of unethical hackers who are known to target organizations in healthcare and transportation industries   * **What** happened?   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. 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.   * **When** did the incident occur?   Tuesday morning, at approximately 9:00 a.m   * **Where** did the incident happen?   A small U.S. health care clinic specializing in delivering primary-care services   * **Why** did the incident happen?   The group of unethical hackers who are known to target organizations in healthcare and transportation industries and wanted a sum of money |
| Additional notes | The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance. |

|  |  |
| --- | --- |
| **Date:** 06/17/2023  Record the date of the journal entry. | **Entry: 2**  Record the journal entry number. |
| Description | In the security operations center (SOC) an analyst at a financial services company receives an alert about a suspicious file being downloaded on an employee's computer. |
| Tool(s) used | Virustotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   An employee at the company, but the malware originated from a threat actor called BlackTech.   * **What** happened?   The Analyst discovered 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. This is the SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b   * **When** did the incident occur?   **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.   * **Where** did the incident happen?   On the employee’s computer   * **Why** did the incident happen?   The employee didn’t properly vet the email attachment |
| Additional notes | 55 security vendors and 2 sandboxes flagged this file as malicious and has a community threat score of 55/71. On Virustotal it is mentioned that this hashed filed is commonly known as trojan.flagpro/jaik and is a trojan horse malware called flagpro and is commonly used by the threat actor BlackTech. |

|  |  |
| --- | --- |
| **Date:** 6/18/2023  Record the date of the journal entry. | **Entry: 3**  Record the journal entry number. |
| Description | An alert ticket was created for the phishing email sent which had a downloadable hash file. The ticket was investigated and then escalated to the level 2 SOC analyst for further analysis since the attachment was malicious as per the phishing playbook. |
| 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?   The initial perpetrator who sent the phishing email was BlackTech   * **What** happened?   A phishing email was sent and a alert ticket was created after it was picked up by an IDS which was then responded to by the level one SOC analyst who determined the attachment in the email to be malicious. Then the ticket was escalated to level two SOC analyst.   * **When** did the incident occur?   The phishing email was sent on July 20, 2022 09:30:14 AM   * **Where** did the incident happen?   Through email   * **Why** did the incident happen?   Possibly to down the organizations network or disrupt business. |
| Additional notes | This activity was just to learn how the alert ticketing process works and to follow the phishing playbook. |

|  |  |
| --- | --- |
| **Date:** 6/20/2023  Record the date of the journal entry. | **Entry: 4**  Record the journal entry number. |
| Description | 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 | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   The final report doesn’t mention who caused the incident and just says “an individual” had sent the email.   * **What** happened?   An employee received an email from an external email address, claiming the sender has successfully stolen data and wanted $25k in cryptocurrency or else they would make it public. But the employee deleted the email thinking it was spam. Then the same employee receives another email but with proof of the missing data but now the demand has increased to $50k. The security team was notified the same day and the team concentrated on determining how the data was stolen and the extent of the theft for 2-3 days.   * **When** did the incident occur?   The incident began on 3:13 p.m. PT, December 22, 2022, but the incident was detected on December 28, 2022, at 7:20 p.m., PT   * **Where** did the incident happen?   On the company’s e-commerce website   * **Why** did the incident happen?   The root cause of the incident was identified as a vulnerability in the e-commerce web  application. |
| Additional notes | The vulnerability on the e-commerce website 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.  Remediations that the company is going to take:  ● Perform routine vulnerability scans and penetration testing.  ● Implement the following access control mechanisms:  ○ Implement allowlisting to allow access to a specified set of URLs and  automatically block all requests outside of this URL range.  ○ Ensure that only authenticated users are authorized access to content. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| Description | Learning how to use Splunk |
| Tool(s) used | Splunk |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| **Date:** 6/22/2023  Record the date of the journal entry. | **Entry: 6**  Record the journal entry number. |
| Description | Learning how to use Google’s Chronicle responding to a phishing email |
| Tool(s) used | Google Chronicle |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened?   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.   * **When** did the incident occur?   Incident first started on 01-23-2023 on 14:40:40 UTC by ashton-davidson-pc   * **Where** did the incident happen?   In the domains signin.accounts-gooqle.com along with signin.office365x24.com and office365x24.com which is the parent domain   * **Why** did the incident happen?   multiple assets might have been impacted by the phishing campaign as logs showed that login information was submitted to the suspicious domain via **POST** requests. |
| Additional notes | 1 security vendor flagged [signin.office365x24.com](https://www.virustotal.com/gui/search/signin.office365x24.com) as malicious  4 security vendors flagged [office365x24.com](https://www.virustotal.com/gui/search/office365x24.com) as malicious  In the ET intelligence rep list this domain was in the category of “Drop site for logs or stolen credentials”  6 assets have accessed the phishing link   * Ashton-davidson-pc * Jude-reyes-pc * Coral-alvarez-pc * Emil-palmer-pc * Bruce-monroe-pc * Roger-spence-pc   2 POST/login.php requests (data was sent to the domain) one from Ashton and the other from Emil  1 POST/login.php request was made by Warren-morris-pc and another asset Amir-david-pc sent a GET request to the domain  Another domain associated with the original domain is signin.accounts-gooqle.com along with signin.office365x24.com this is a form of typosquatting by examining the resolved IP address |

### 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. |