**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:** 05/31/2023 | **Entry:**  1 |
| --- | --- |
| Description | A small US health care clinic experienced a security incident on Tuesday at 9:00am which disrupted their business operations, it was done by sending the phising email to the company employees which consist of malicious attachment that installed malware(ransomware) on the employee computer and then encrypted the critical files, the attackers asked for a large amount of money to decrypt the critical files |
| Tool(s) used | List any cybersecurity tools that were used.  -) None |
| 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?   -) Health Care Clinic employees that are targeted by the phishing email  -) All critical files that includes patient data and medical records  -) Incident occured on Tueday morning 9:00am  -) It happen on a small US health care clinic specilaizing in primmary care service.  -) Incident happend because the organized group of unethical hackers wants largee sum of money from the company |
| Additional notes | This type of attack is a phising email attack that trick the company employee to open the email which contains malicious attachment, as a result of opening the attachment it malware(ransomware) is deployed and encrypt the company critical files including patient datat, and medical records.  -) How the company educate the employees about the phising email attacks for future attacks? |

| **Date:**  06/2/2023 | **Entry:**  **2** |
| --- | --- |
| Description | A suspecious file being downloaded on an employee computer, the file was sent as an attachment "bfsvc.exe" in an email on Wednesday, July 20, 2022 at 09:30:14 AM the email stating about the intrest of a candidate in the engineer role with the password: "paradise10789" to open thre attachment "bfsvc.exe" that consist of candidate resume and cover letter, employee mistakenly open the attachment and become the victim of phishing attack. |
| Tool(s) used | List any cybersecurity tools that were used.  -) VirusTotal |
| 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?   -) The incident was caused by employee of the company  -) Employee computer is infected by the trojan malware  -) Incident happened on Wednesday, July 20, 2022 09:30:14 AM  -) Incident happened on Ingegry company employee computer  -) Incident happened because the company employee mistakenly open the attachment "bfsvc.exe" which contains "torjan" malware. |
| Additional notes | Include any additional thoughts, questions, or findings.  -) This is a type of a phising attack to the company employee, the file is used as an attachment which consists of "trojan" malware as a result critical files in employee computer is affected.  -) How company should educate the employee about the phising attack?  -) After examine these finding phishing alert needed to be generated  1) the attach file "bfsvc.exe can cause more damage if it open or send to other employees  2) It also effect the company network and other devices also be affected by these virus |

| **Date:**  06/05/2023 | **Entry:**  **3** |
| --- | --- |
| Description | Buttercup games e-commerce given tasked to identify if there are any possible security issues with the mail server for that as a security analyst at the company I have to explore failed SSH login attempts for the root account to exmpore the dat I use Splunk Cloud platform. |
| Tool(s) used | List any cybersecurity tools that were used.  Splunk Cloud |
| 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?   -) NA  -) After uploading Buttercup e-commerce data set file and to evaluate fields in search bar there are "109,864" event shows after filtering on mail server there are more than 300 failed attempts were made.  -) 06/05/2023  -) N/A |
| Additional notes | Include any additional thoughts, questions, or findings.  After finding more than 300 failed login attempts, as a security analyst I report to Buttercup games e-commerce, and further investigate the timestamp of the these login attempts |

| **Date:**  06/05/2023 | **Entry:**  **4** |
| --- | --- |
| Description | Financial services company recieved and alert that an employee recieved a phising email in their inbox. As a security analyst at this company I review the email and find out that the suspicious domain name "signin.office365x24.com", in this incident I have to further investigate that  if any other employee have recieved phishing emails. |
| Tool(s) used | List any cybersecurity tools that were used.  -) Google Chronicles. |
| 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?   1) Incident was caused by the financial services company employee who becomce the victim of phishing email.  2) After investigate the domain " signin.office365x24.com" name using Google Chronilces under "Assets" it shows there are 6 Assets(employees) who access the domain following are the names of employess.  1) ashton-davidson-pc  2) bruce-monroe-pc  3) coral-alvarez-pc  4) emil-palmer-pc  5) jude-reyes-pc  6) roger-spence-pc  -) After further investigation under "Timeline" tab in Google Chrome it shows that 2 out of 6 employees become the victim of phising attack form this domain because the TimeLine log shows the POST http request from there sides following are the names of the employees  1) ashton-davidson-pc (Phished-showing POST request under Timeline).  2) emil-palmer-pc (Phished-showing POST request under Timeline).  After invetigating the IP address it shows the attacker also used another domain "40.100.174.34" under Resolved IPS tab in the Google chronicles, by seraching the "Assets" and "Timeline" of this domain it shows there are other 2 employees that access the domain among which 1 is targeted by phishing attack by investigating the "Timeline" log of this domain  1) amir-david-pc  2) waren-morris-pc (Phished-showing POST request under Timeline). |
| Additional notes | Include any additional thoughts, questions, or findings.  -) After these findings financial services employee needs to be alerted by giving the names of the employee who beceome the victim of phising attack, and educate the employee to not given there credentials to any unknown domains  -) under Firewall security and router settings have to block these domains " signin.office365x24.com" and "40.100.174.34" so that other employees will not access the domain. |

| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| --- | --- |
| Description | Provide a brief description about the journal entry. |
| 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? * **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:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| --- | --- |
| Description | Provide a brief description about the journal entry. |
| 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? * **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. |

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?  -) Entry number 3 from my Incident handler's journal that challanging for me because I am unable to upload the dataset from the Buttercup game e-commerce to Splunk Cloud platform  2. Has your understanding of incident detection and response changed since taking this course?  2) This course helps me to understand how to keep track of incident handler's journal as well as how to monitor and detect phising attacks, and suspicious domain names and to respond that using playbook and Alert ticket.  3. Was there a specific tool or concept that you enjoyed the most? Why?  1) SIEM tool (Google Chronilce): I like the GUI, which make it easy to monitor suspicious domain) |
| --- |