**This is a fragment incident handler journal that describes some of the tasks performed during the Google certificate process. These records provide a summary of some of the tasks and I am sharing some here as part of my portfolio.**

|  |  |
| --- | --- |
| **Date:** 25.07.2023 | **Entry: 1** |
| Description | A small U.S. health clinic experienced a security incident where business operations were shut down due to ransomware attack. Attackers were able to gain access into company’s network using phishing emails which contained malicious attachments. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** Incident was caused by organized group of unethical hackers * **What:** Business operations were shut down due to ransomware attack * **Where:** Incident happened in U.S. health clinic * **When:** Incident occurred Tuesday 9:00 am * **Why:** Incident happened because several employees were successfully targeted in phishing campaign which used emails with malicious file attachments. |
| Additional notes | Incident highlighted importance of proper employees training. Staff was unaware of techniques used by malicious actors during phishing campaign. |

|  |  |
| --- | --- |
| **Date:** 31.08.2023 | **Entry:2** |
| Description | Organization experienced security incident during which malicious actor was able to steal PII and financial information. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who :** Malicious actor * **What:** PII and financial data was stolen. * **When**: Incident occurred on 28.12.2022 at 7:20 p.m. * **Where:** Incident happened in mid-sized retail company. * **Why**: Incident happened because of vulnerability in e-commerce web application. It allowed attacker to perform forced browsing attack to access customer transaction data by modifying the order number included in URL string |
| Additional notes | To prevent future recurrences, security team recommended:   * Perform routine vulnerability scans and penetration testing * Implement allowlisting to allow access to specified set of URLs and automatically block all request outside of this URL range * Ensure that only authenticated users are authorized access to content |

|  |  |
| --- | --- |
| **Date:** 01.08.2023 | **Entry:3** |
| Description | First time using Chronicle |
| Tool(s) used | Google Chronicle |
| The 5 W's | * **Who** N\A * **What** N\A * **When** N\A * **Where** N\A * **Why** N\A |
| Additional notes | This was first time I used Chronicle. I was excited to try SIEM tool and I must say this was fascinating experience. I have trouble with understanding tool output but I am sure it will come with experience! |

|  |  |
| --- | --- |
| **Date:** 01.08.2023 | **Entry: 4** |
| Description | First time using Splunk Cloud |
| Tool(s) used | Splunk Cloud |
| The 5 W's | * **Who** N\A * **What** N\A * **When** N\A * **Where** N\A * **Why** N\A |
| Additional notes | During Google Cybersecurity Professional Certificate I tried for the first time Splunk tool. It was quite interesting experience. I found Splunk to be more easy to understand than Google Chronicle or it is just me. But again I know that with experience I will find more comfort with using these tools. |

|  |
| --- |
| Reflections/Notes:   1. **Were there any specific activities that were challenging for you? Why or why not?**   I found activity with Chronicle to be quite challenging because I was new to using SIEM tool. I had trouble with understanding all information that was displayed on my screen. I felt quite overwhelmed but I overcame it and finished tasks thanks to instructions.   1. **Has your understanding of incident detection and response changed after taking this course?**   Before taking this course I had very little understanding of incident detection and response procedure. I always thought about cybersecurity as direct battle with hackers using computers. Now I know that cybersecurity is far more complex. Course helped me to understand importance of plans, processes, tools and teamwork during security incident.  **3. Was there a specific tool or concept that you enjoyed the most? Why?**  I really enjoyed Splunk. I was able to understand it interface quite fast. I was always curious of SIEM tools and during course this curiosity only increased. I am definitely interested in expanding my knowledge of Splunk in the future. |