**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:**  2023/08/25 | **Entry:**  0001 |
| Description | Cybersecurity incident  I was asked to review an incident in which hackers targeted phishing emails at certain firm personnel in order to obtain access to the network. When the employee downloaded the harmful attachment from the phishing emails, it infected their PC with malware. Critical files were encrypted by the ransomware the attackers used. The company's business activities were severely hampered by the inability to access vital patient data. The company was compelled to shut down its computers and get in touch with a number of organizations to report the occurrence and request technical support. |
| Tool(s) used | None |
| The 5 W's | Capture the 5 W's of an incident.   * Unethical hackers * A ransom cybersecurity incident * It happened on Tuesday 22nd 2023 by 09:00 am * A small U.S. health care clinic * There was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. The threat was launch for financial gain**.** |
| Additional notes | What can be done to prevent re-occurrence? |

|  |  |
| --- | --- |
| **Date:**  2023/08/26 | **Entry:**  0002 |
| Description | Examine packet information using Wireshark.  I analyzed a network packet capture file that contained information on the traffic generated when a user connected to a website. To determine the source and destination IP addresses used in this online surfing session, I filtered the data. Additionally, when network data is gathered, it is important to investigate the protocols that are employed when a user connects to a website and to analyze some data packets in order to determine the kind of information that is delivered and received by the systems that link to one another. |
| Tool(s) used | Wireshark |
| The 5 W's | **The 5 W's below were not applicable.**  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 | Using Wireshark for the first time It was exciting to me. |

|  |  |
| --- | --- |
| **Date:**  2023/08/26 | **Entry:**  0003. |
| Description | Examine packet information using tcpdump  In a Linux environment, I captured and filtered network traffic. I utilized tcpdump to capture network activity. I identified network interfaces, captured network data for inspection using the tcpdump command, and then investigated the data inside the packets to concentrate on kinds of traffic. analyzed the information that tcpdump outputs about the packet and stored and loaded packet data for subsequent analysis. |
| Tool(s) used | tcpdump. |
| The 5 W's | **The 5 W's below were not applicable.**  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 | Linux is not new to me. Improving on the commands is what I need to spend more time to explore. |

|  |  |
| --- | --- |
| **Date:**  2023-08-26 | **Entry:**  0004 |
| Description | Examined a suspicious file hash  I retrieved VirusTotal's report on the file hash from VirusTotal website and examined the report details to determine whether the file is malicious using the security vendor’s analysis, vendor’s ratio and the community score. A high vendors' ratio, a negative community score, and malware detections in the security vendors' analysis section revealed that it was a malicious file. Three (3) indicators of compromise (IoCs) that are associated with this file hash were identified. |
| Tool(s) used | VirusTotal tool was used. |
| The 5 W's | Capture the 5 W's of an incident.   * A malicious attacker * An employee received an email with a SHA 256 file attachment with file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * It happened on Friday 25th 2023 by 04:00 pm * A financial service company * There was a phishing email that contained a malicious attachment. Once it was downloaded, it installed a malware on the system. The attackers aim not yet established. |
| Additional notes | Can this occurrence be prevented? |

|  |  |
| --- | --- |
| **Date:**  2023/08/26 | **Entry:**  0005. |
| Description | Using organization’s playbook to resolve an alert.  I followed the organization’s process to complete my investigation and resolved the alert. My organization's security policies and procedures describe how to respond to specific alerts, including what to do when I receive a phishing alert. I completed my investigation and resolved the alert. At the end of my investigation, I escalated the alert ticket with my findings about the incident and forwarded it to the security operation center analyst level 2 for further action. |
| Tool(s) used | Phishing Playbook. |
| The 5 W's | Capture the 5 W's of an incident.   * A malicious attacker * An employee received an email with a SHA 256 file attachment with file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * It happened on Friday 25th 2023 by 04:00 pm * A financial service company * There was a phishing email that contained a malicious attachment. Once it was downloaded, it installed malware on the system. The attackers aim not yet established. |
| Additional notes | What needs to be improved on to reduce this risk to the organization? |

|  |  |
| --- | --- |
| **Date:**  2023/08/26 | **Entry:**  0006. |
| Description | Review of final report of a concluded investigation  A significant security incident that exposed the personal information of over a million users occurred at the organization. Since this was a recent and significant security breach, my team has worked to stop the incident from occurring in the future. This breach occurred before I started working there. I've been requested to review at the completed report. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * A malicious attacker was responsible. * The company was a victim of identity loss of some users through forced browsing. About 50,000 customer records were affected, which impacted on the company $100,000 in direct costs and potential loss of revenue. * The incident occurred on December 28, 2022, at 7:20 p.m * In the e-commerce web application * **T**he incident happened due to a vulnerability in the web app |
| Additional notes | There is need to invest in penetration test of all the company apps. |

|  |  |
| --- | --- |
| **Date:**  2023/08/27 | **Entry:**  0007. |
| Description | Examine alerts, logs, and rules with Suricata  I created custom rules and run them in Suricata, monitored traffic captured in a packet capture file, and examined the fast.log and eve.json output. |
| Tool(s) used | Suricata  Suricata is a program that keeps track of network interfaces and applies rules to the packets that pass through them. Suricata makes the decision of whether each packet should result in an alert, be dropped, rejected, or allowed to pass through the interface. |
| The 5 W's | **The 5 W's below were not applicable.**  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 | What needs to be improved on to reduce this risk to the organization? |

|  |  |
| --- | --- |
| **Date:**  2023/08/28 | **Entry:**  0008. |
| Description | Investigation of possible security issues with the mail server using Splunk  I experimented with some straightforward queries using pipes and wildcards in Splunk's querying language, known as Search Processing Language (SPL). I uploaded sample log data, searched through indexed data, evaluated search results, identified different data sources and located failed SSH login(s) for the root account. |
| Tool(s) used | Splunk enterprise and cloud  Splunk offers a platform for storing, analyzing, and reporting on data from various sources, making it a crucial component of a security analyst's toolkit. |
| The 5 W's | **The 5 W's below were not applicable.**  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 | What needs to be improved on to reduce this risk to the organization? |

|  |  |
| --- | --- |
| **Date:**  2023/08/29 | **Entry:**  0009. |
| Description | Use Chronicle to investigate a phishing email.  I investigated a suspicious domain that was used in a phishing email using Google Chronicle. I examined the HTTP events connected to the domain, analyzed the threat intelligence reports on the domain, determined which assets accessed the domain, determined which assets provided login information to the domain, and discovered further domains. |
| Tool(s) used | Chronicle.  A cloud service called Chronicle was created enabling businesses to privately store, process, and search the enormous volumes of security and network telemetry they produce. In order to give immediate insight and context on risky conduct, . Chronicle normalizes, indexes, correlates, and analyzes the data to provide instant analysis and context on risky activity.  One can search for events in Chronicle using either a Unified Data Mode (UDM) Search or a Raw Log Search. |
| The 5 W's | **The 5 W's below were not applicable.**  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:  The entire components of incident detection and response are interesting to me. I would like to know more about splunk and chronicle; how to mine information from them. My views have dramatically changed since the beginning of this course due to how google teams have simplified it. With these acquired hands-on experience, I am interested in working in a role that deals with detection and incident response because of the established processes and procedures with the proven tools that are out there. |