**Incident handler's journal**

This document contains incident response journal entries completed as part of the Google Cybersecurity Certificate program. Each entry is based on a simulated real-world scenario and is designed to demonstrate my ability to apply cybersecurity concepts such as incident handling, log analysis, and documentation. The journal showcases both investigative entries using the 5 W’s framework and hands-on experience with essential cybersecurity tools like Splunk, Wireshark, and cloud security platforms. These entries reflect my growth as a security analyst and form a key part of my cybersecurity portfolio, which I plan to share with potential employers.

| Date: July 1, 2025 | Entry: 1 | | |
| --- | --- | --- | --- |
| Description | A ransomware attack targeted a small healthcare clinic in Western Australia, causing a complete shutdown of operations after staff reported they couldn’t access medical records or systems. A ransom note was displayed on employee computers demanding payment to decrypt the files. This occurred during the Detection and Analysis phase of the NIST Incident Response Lifecycle. | | |
| Tool(s) used | None at this stage. Tools to be considered for incident investigation may include antivirus software, email security tools, backup systems, and forensic analysis platforms. | | |
| The 5 W's | * Who: An organized cybercrime group known for targeting healthcare. * What: Ransomware attack via phishing email. * When: July 1, 2025, around 9:00 a.m. * Where: At a small healthcare clinic located in Western Australia. * Why: Employees opened malicious attachments, leading to encryption of critical systems. | | |
| Additional notes | Highlights the importance of phishing training, email filtering, and backup strategies. The organization should formalize its incident response plan. | | |

| Date**:** July 21, 2025 | Entry: 2 | | |
| --- | --- | --- | --- |
| Description | A data leakage incident occurred at a WA healthcare clinic due to a misconfigured cloud storage bucket. Sensitive patient data was made publicly accessible. This incident falls under the Containment, Eradication, and Recovery phase of the NIST framework. | | |
| Tool(s) used | Cloud Security Posture Management (CSPM), Azure configuration scanner, and data loss prevention (DLP) tool. | | |
| The 5 W's | * Who: Internal IT team (unintentional misconfiguration). * What: Patient records exposed due to public cloud bucket access. * When: Discovered during a routine audit on July 21, 2025. * Where: Cloud environment of a WA healthcare provider * Why: Lack of automated misconfiguration alerts and poor access control. | | |
| Additional notes | Cloud security audits and IaC security guardrails are essential for preventing similar incidents. | | |

| Date**:** July 23, 2025 | Entry: 3 | | |
| --- | --- | --- | --- |
| Description | Used Splunk Cloud to investigate a spike in failed SSH login attempts on a company mail server. This helped in identifying brute-force activity. This investigation is part of the Detection and Analysis phase. | | |
| Tool(s) used | * Splunk Cloud: Used index=main host=mailsv fail\* root to locate over 300 failed SSH login events targeting the root account * Filtered logs by host and sourcetype to isolate relevant entries * Analyzed timestamp and IP to identify attacker patterns | | |
| Additional notes | Splunk's filtering and visualization capabilities made it easier to isolate abnormal activity patterns in logs. | | |

| Date**:** July 24, 2025 | Entry: 4 | | |
| --- | --- | --- | --- |
| Description | Captured and analyzed DNS traffic using Wireshark to investigate potential command-and-control callbacks. This activity demonstrates the use of network analysis in the Detection and Analysis phase. | | |
| Tool(s) used | * Wireshark: Captured packet traffic from a test workstation * Used filters like dns.qry.name contains ".xyz" to detect unusual domains * Identified repetitive DNS queries to a suspicious dynamic DNS provider | | |
| Additional notes | Splunk's filtering and visualization capabilities made it easier to isolate abnormal activity patterns in logs. | | |