**Incident handler's journal**

| **Date:** Wednesday, July 20, 2022 | **Entry:2** | | |
| --- | --- | --- | --- |
| Description: | A phishing email was reported, so I updated the alert ticket. | | |
| Tool(s) used | SHA-256 Hash | | |
| The 5 W's | * **Who** caused the incident?   A malicious actor was disguised as Cylde West and supposedly worked for Def communication   * **What** happened?   A phishing attempt was made   * **When** did the incident occur?   20th July 2022   * **Where** did the incident happen?   It was a phising email   * **Why** did the incident happen?   The employee opened the malicious file which was shown to be a resume | | |
| Additional notes | The alert ticket is attached alongside | | |