| **Date:**  2nd August, 2025 | **Entry:**  #3 | | |
| --- | --- | --- | --- |
| Description | Phishing alert triggered by suspicious email attachment downloaded on employee workstation. File hash confirmed malicious | | |
| Tool(s) used | Security Incident Response Playbook | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A threat actor impersonating a job applicant named **Clyde West** * **What** happened? A malicious executable file (**bfsvc.exe**) was downloaded and opened from a phishing email * **When** did the incident occur? July 20, 2022 at 09:30 am * **Where** did the incident happen? Employee workstation ( IP: 176.157.125.93) * **Why** did the incident happen? The attacker disguised malware as a resume attachment in a fake job application email, tricking the user into downloading it | | |
| Additional notes | 1. File hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b confirmed malicious 2. Spoofed sender domain: [76tguy6hh6tgftrt7tg.su](http://76tguy6hh6tgftrt7tg.su) 3. Incident has been escalated to Level 2 SOC analyst for further investigation | | |