**MITRE ATT&CK Mapping for Phishing Incident – Zenith Solutions SOC**

| **Tactic** | **Technique ID** | **Technique Name** |
| --- | --- | --- |
| Initial Access | T1566.001 | Spearphishing Link |
| Execution | T1059.001 | Powershell |
| Credential Access | T1078 | Valid Accounts |
| Persistence | T1114.002 | Auto-Forwarding Rules |
| Collection | T1114 | Email Collection |
| Defense Evasion | T1027 | Obfuscation |
| Indicator Removal | T1070.004 | Email Deletion |
| Command & Control | T1105 | Remote Script/Tool Transfer |
|  |  |  |