**4. Analysis – MITRE ATT&CK & Diamond Model Mapping**

**MITRE ATT&CK View:**

* Tactics (top row): Initial Access → Execution → Persistence → Exfiltration
* Techniques: Phishing, PowerShell, Credential Dumping, C2 via HTTPS
* Mapping observed IOCs and behaviors to known TTPs

**Diamond Model Quadrants:**

* **Adversary** – Who (named or unknown group)
* **Capability** – What tools/malware (e.g., Qakbot, Cobalt Strike)
* **Infrastructure** – Where from (e.g., IPs, domains)
* **Victim** – Targeted sector or role (e.g., hospital finance team)

**Outcome:** Threat actor attribution and prioritization of threat relevance