Threat Hunting Workflow

1) Hypothesis: Define what gap you are testing.

2) Data collection: Identify relevant logs (EDR, Windows Events, DNS).

3) Query: Run focused queries in Elastic/SIEM.

4) Validate: Cross-check IOCs with OTX/VirusTotal.

5) Respond: If confirmed, create case and contain.

6) Document: Produce hunting report and update detections.