Threat Hunting Methodologies

Overview: Threat hunting is a proactive activity where analysts create hypotheses about adversary behavior and search across telemetry to find evidence.

Methodologies: Two practical frameworks: **SqRR** (Search -> Query -> Retrieve -> Respond) and **TaHiTI** (Targeted Hunting integrating Threat Intelligence). SqRR encourages iterative queries; TaHiTI emphasizes using threat intelligence to prioritize hunts.

Data Sources: EDR traces, Windows Event Logs (4625 failed logon, 4672 privileged assignment), network flows, DNS logs, proxy logs, threat intelligence feeds (OTX, VirusTotal).

Example hypothesis: 'An adversary is abusing valid accounts (MITRE T1078) to perform privilege escalation.'

Example Elastic-like query (pseudo): *event.code:4672 AND user.name:(!system) AND timestamp:[now-7d TO now]* — investigate unexpected user role assignments.

Deliverable for a hunt: CSV table of findings (timestamp, user, event id, notes) and a short hunting report mapping results to MITRE techniques.