SIEM & SOC Fundamentals - Cheat Sheet

Topic	Key Points
SIEM Definition	SIEM = Security Information and Event Management. Real-time alert analysis from logs.
Elastic Stack Components	Beats -> Logstash -> Elasticsearch -> Kibana. Log ingestion, storage, analysis, and visualization.
Kibana Query Language (KQL)	event.code:4625 AND user.name:admin* - filters failed logins by admin users. Use : for match.
SOC Roles	Tier 1: Monitor & escalate | Tier 2: Deep analysis | Tier 3: Threat hunting | Engineer: Maintains tools.
MITRE ATT&CK	Tactics (what) + Techniques (how). Used in threat detection, red teaming, intel enrichment.
SIEM Use Case Lifecycle	Steps: Requirements -> Data Points -> Log Validation -> Design -> Implement -> Test -> Tune.
Common Event IDs	4624: Successful login | 4625: Failed login | 4732/4733: Added/Removed from group.
Triaging Steps	1. Review Alert -> 2. Classify -> 3. Enrich -> 4. Risk Assess -> 5. Respond or Escalate.