Post-Incident Analysis and Continuous Improvement

Root Cause Analysis (RCA): Use 5 Whys and Fishbone diagrams to identify underlying causes beyond symptomatic fixes.

5 Whys Example (phishing):

1) Why was credential stolen? -> User clicked malicious link.

2) Why clicked? -> Email filter missed it / training gap.

3) Why filter missed? -> No tuned rules for this campaign.

4) Why no rules? -> Lack of threat intel correlation.

5) Why no correlation? -> No integrated feed ingestion & enrichment.

Metrics: MTTD (Mean Time To Detect) = time from compromise to detection. MTTR (Mean Time To Respond) = time from detection to containment. Dwell Time = compromise to remediation.

Continuous Improvement: Use RCA insights to update playbooks, detection rules, and training. Maintain a lessons-learned register.