Contents

[4.5] Shame-Based Security Hiding

1. Operational Definition: The tendency to conceal security mistakes, near-misses, or lack of knowledge due to fear of embarrassment or punishment, preventing organizational learning and creating invisible vulnerabilities.

2. Main Metric & Algorithm:

- **Metric:** Near-Miss Reporting Rate (NMRR). Formula: `NMRR = N_reported_near_misses / E_estimated_near_misses`. *Since the true number is unknown, we estimate it (E) via other proxies.*
- **Pseudocode:**

  python

  ```
  def estimate_nmrr(ticketing_system, chat_logs, keywords):
      """
      Estimates NMRR by comparing official reports to discussions in informal channels.
      """
      # 1. Get OFFICIAL near-miss reports from ticketing system (e.g., tagged as 'near-miss'
      official_reports = query_jira('project = SOC AND labels = near-miss')

      # 2. Search PRIVATE channels for discussions indicating a near-miss was discovered but
      private_messages = query_slack_dms(keywords) # keywords: ["oops", "almost", "close cal
      # Use NLP/Topic modeling to cluster messages suggesting a near-miss event
      inferred_near_misses = topic_cluster(private_messages)

      # NMRR is the ratio of official reports to total inferred events
      nmrr = len(official_reports) / (len(official_reports) + len(inferred_near_misses)) if
      return nmrr
  ```

- **Alert Threshold:** `NMRR < 0.5` (Less than half of inferred near-misses are officially reported).

3. Digital Data Sources (Algorithm Input):

- **Ticketing System (Jira):** API to search for issues with a `near-miss` tag.
- **Communication Platform (Slack/Teams):** *Anonymized* API access to search for keywords in private channels/DMs. **CRITICAL: This must be done with full ethical oversight, using aggregated, anonymized data only.**

4. Human-to-Human Audit Protocol: Institute a blameless post-mortem process and track participation. Conduct anonymous surveys asking: "In the last 6 months, have you made a security error you did not report? Why?" Ensure psychological safety in the response process.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Create an anonymous reporting channel integrated with the ticketing system.

- **Human/Organizational Mitigation:** Leadership must publicly model vulnerability by discussing their own mistakes. Formalize and evangelize a blameless post-mortem culture.
- **Process Mitigation:** Implement a "Good Catch" program that rewards and celebrates the reporting of near-misses, decoupling it from punitive outcomes.