Contents

[3.7] Peer Pressure Compliance

1. Operational Definition: The act of violating security protocols due to real or perceived pressure from colleagues or a group, often to avoid conflict, fit in, or not be seen as an obstacle.

2. Main Metric & Algorithm:

- **Metric: Coerced Action Frequency (CAF)**. This is difficult to quantify digitally and is often best identified through audits and simulations.
- **Pseudocode:**

  python

  ```
  # This is a placeholder. Primary detection is via audit protocol.
  def monitor_for_pressure_keywords(chat_logs):
      """
      Looks for linguistic signals of pressure in communications.
      """
      pressure_patterns = [
          "just approve it", "don't be difficult", "everyone else does it",
          "why are you blocking this?", "we don't have time for this"
      ]
      flagged_messages = query_chat_logs(chat_logs, keywords=pressure_patterns)
      return flagged_messages
  ```

- **Alert Threshold:** Any instance of pressure keywords in a security-related context should be flagged for human review.

3. Digital Data Sources (Algorithm Input):

- **Communication Platform API (Slack/Teams):** Primary source for detecting pressure language. Fields: `channel`, `user`, `text`, `timestamp`.
- **Access/Request Logs:** To correlate pressured communications with subsequent security actions.

4. Human-to-Human Audit Protocol: This is the primary method. Conduct confidential interviews or anonymous surveys: "Have you ever felt pressured by a colleague or manager to bypass a security rule? Can you describe the circumstances without naming names?" Run facilitated workshops with teams to discuss scenarios where security and peer pressure might conflict.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement an anonymous reporting channel for security concerns, allowing employees to report peer pressure without fear of reprisal.
- **Human/Organizational Mitigation:** Foster a strong "culture of security" from top leadership down, where upholding security protocols is valued and celebrated, and where pushing back on insecure requests is seen as professional, not difficult.

- **Process Mitigation:** Create and empower "security champions" within teams to be points of contact for these situations, providing a supportive peer who can validate the employee's concern and help address the pressure.