Contents

[1.5] Fear-Based Compliance Without Verification

1. Operational Definition: Compliance with a security directive or request primarily driven by anxiety or fear of reprisal from an authority figure, leading to the omission of standard verification or critical thinking steps.

2. Main Metric & Algorithm:

- **Metric:** Fear-Based Action Rate (FAR). Formula: `FAR = N_fear_actions / N_total_actions`.
- **Pseudocode:**

  python

  ```
  # This metric requires correlating behavior with communication tone.
  def calculate_far(comms_data, action_logs, start_date, end_date):
      # 1. Identify high-pressure commands in comms (e.g., "DO THIS NOW OR ELSE", "URGENT: Y
      high_pressure_comms = analyze_sentiment_and_tone(comms_data, keywords=["urgent", "imme

      far_actions = 0
      # 2. For each high-pressure comm, find subsequent security-sensitive actions by the re
      for comm in high_pressure_comms:
          user_actions = get_user_actions(user=comm.recipient, timeframe=comm.timestamp + ti
          # Look for actions that are atypical for the user or lack normal verification flag
          for action in user_actions:
              if action.sensitivity == 'high' and action.verification_level == 'low':
                  far_actions += 1

      total_high_risk_actions = count_high_risk_actions(action_logs)
      FAR = far_actions / total_high_risk_actions if total_high_risk_actions > 0 else 0
      return FAR
  ```

- **Alert Threshold:** A statistically significant positive correlation (`p-value < 0.05`) between high-pressure communications and subsequent low-verification, high-risk actions.

3. Digital Data Sources (Algorithm Input):

- **Communication Platforms API** (Slack, Teams): To analyze the tone and content of directives from managers/superiors.
- **SIEM/Application Logs:** To capture subsequent security-sensitive user actions (e.g., data access, system changes).
- **Identity and Access Management (IAM) Logs:** To establish a baseline of normal user behavior.

4. Human-To-Human Audit Protocol: During security culture surveys, include questions like: "I have felt pressured to bypass a security step to avoid disappointing my manager." Use a Likert scale. Conduct confidential interviews to explore positive responses in depth.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement mandatory technical “circuit breakers” that force a delay and a verification check for critical actions, even under an admin context.
- **Human/Organizational Mitigation:** Foster a blameless culture focused on psychological safety. Leadership must explicitly reward employees for questioning orders and following secure procedures.
- **Process Mitigation:** Institute a formal, anonymous channel for reporting pressure to violate security policies.