Contents

[4.6] Guilt-Driven Overcompliance

1. Operational Definition: A counter-reaction to a previous security failure or mistake, leading to excessively rigid adherence to protocols, which can hinder operational efficiency, create unnecessary friction, and cause alert fatigue from over-reporting.

2. Main Metric & Algorithm:

- **Metric:** Procedural Friction Index (PFI). Formula: `PFI = (N_rejected_requests + N_escalated_requests) / N_total_requests`.
- **Pseudocode:**

  python

  ```
  def calculate_pfi(access_logs, ticketing_system, team_id):
      """
      access_logs: Logs of access requests (e.g., to IAM system)
      ticketing_system: Tickets for access requests or security exceptions
      """
      # Get all access requests made by the team
      team_requests = query_requests(team_id)

      # Count requests that were rejected or required an escalation for approval
      rejected_or_escalated = [r for r in team_requests if r['status'] in ['rejected', 'esca

      pfi = len(rejected_or_escalated) / len(team_requests) if team_requests else 0
      return pfi
  ```

- **Alert Threshold:** `PFI > 0.4` (Over 40% of requests are being rejected or require escalation, indicating overly strict enforcement).

3. Digital Data Sources (Algorithm Input):

- **IAM System Logs:** (e.g., Azure AD, Okta) API to audit access request and approval logs.
- **Ticketing System (ServiceNow):** API to query the workflow history of access request tickets.

4. Human-to-Human Audit Protocol: Interview team members from development and other internal customer groups: "How would you describe the process of getting necessary access or exceptions from the security team? Does it feel collaborative or adversarial?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement a Just-In-Time (JIT) access system to reduce the need for standing privileges and permanent exceptions.
- **Human/Organizational Mitigation:** Provide training for security staff on risk-based decision making rather than binary compliance. Foster collaboration between security and other teams.

- **Process Mitigation:** Review and update access control policies to ensure they are aligned with business needs and not unnecessarily restrictive.
