# Contents



## [3.10] Reputation Management Conflicts

**1. Operational Definition:** The conflict that arises when an individual must choose between adhering to security protocols (e.g., reporting a mistake) and performing an action that protects their personal or professional reputation (e.g., hiding the mistake), often leading to security risks being concealed.

**2. Main Metric & Algorithm:**

- **Metric: Incident Obfuscation Rate (IOR).** Formula: `IOR = N_hidden / N_estimated_total`, where `N_hidden` is the number of incidents found through forensic means that were not self-reported.
- **Pseudocode:**

  python

  ```
  # This algorithm is inherently retrospective and probabilistic.
  def calculate_ior(reported_incidents, detected_incidents, period):
      """
      reported_incidents: Incidents logged via official reporting (ticketing).
      detected_incidents: Incidents found via scans, audits, or external reports.
      """
      # Find incidents that were detected but not reported
      hidden_incidents = set(detected_incidents) - set(reported_incidents)

      # The true total is what we found via both channels
      estimated_total_incidents = set(reported_incidents) | set(detected_incidents)

      IOR = len(hidden_incidents) / len(estimated_total_incidents) if estimated_total_incide
      return IOR
  ```

- **Alert Threshold:** `IOR > 0.1` (Over 10% of incidents are being hidden/not reported).

**3. Digital Data Sources (Algorithm Input):**

- **Ticketing System (Jira, ServiceNow):** Source for `reported_incidents`. Fields: `incident_id`, `reporter`, `report_time`.
- **SIEM/SOC Alert Logs (Splunk, Elastic):** Source for `detected_incidents`. Fields: `alert_id`, `generation_time`, `severity`.
- **Vulnerability Scan Logs (Qualys, Nessus):** Another source for `detected_incidents`.

**4. Human-to-Human Audit Protocol:** Institute a formal, blameless post-mortem process for all security incidents. The explicit promise of no punishment for human error (except for malicious intent) is crucial to uncover the true root causes and measure the rate of previously hidden incidents.

**5. Recommended Mitigation Actions:**

- **Technical/Digital Mitigation:** Implement robust detective controls (logging, monitoring, scanning) that automatically find incidents, reducing the opportunity to hide them.

- **Human/Organizational Mitigation:** Leadership must actively and repeatedly promote a **blameless culture**. Celebrate and reward employees who proactively report their own errors or near-misses, framing it as a strength that improves organizational security.
- **Process Mitigation:** Formalize the blameless post-mortem process. Ensure it is focused on learning and improving systems, not on assigning blame to individuals.