Contents

[8.4] Transference to Authority Figures

1. Operational Definition: The unconscious redirection of feelings and desires from a past authority figure (e.g., a parent, former boss) onto a current security leader or tool, leading to either irrational compliance or rebellion against their directives.

2. Main Metric & Algorithm:

- **Metric:** Authority Directive Deviation Index (ADDI). Formula: `ADDI = (Count_of_Deviations + Severity_Weight) / Count_of_Directives`.
- **Pseudocode:**

  python

  ```
  def calculate_addi(analyst_id, team_lead_id, start_date, end_date):
      # 1. Query directives from the authority figure (e.g., tasks, policies from team lead)
      directives = query_directives(team_lead_id, analyst_id, start_date, end_date)

      # 2. Query analyst's actions for deviations (e.g., ignoring policy, implementing a dif
      deviations = 0
      severity_weight = 0
      for directive in directives:
          if not was_directive_followed(directive, analyst_id):
              deviations += 1
              severity_weight += directive.severity  # e.g., severity on a scale of 1-5

      # 3. Calculate index
      addi = (deviations + severity_weight) / len(directives) if directives else 0
      return addi
  ```

- **Alert Threshold:** `ADDI > 0.5` (Significant and/or severe deviations from authority directives).

3. Digital Data Sources (Algorithm Input):

- **Ticketing System:** Jira/ServiceNow API for tasks assigned by a lead to an analyst (fields `assignee`, `reporter`, `created`, `status`, `priority`).
- **SIEM/SOAR:** Logs of policy overrides or manual actions that contradict recently communicated policies or procedures from leadership.
- **Communication Platforms:** Microsoft Teams/Slack API to detect contentious or emotionally charged discussions in channels between the analyst and the authority figure.

4. Human-to-Human Audit Protocol: An independent auditor conducts separate interviews with the analyst and the team lead. Ask the analyst: "How do you decide when to follow a procedure exactly and when to adapt it? Can you tell me about your working relationship with [Team Lead's Name]?" Ask the lead: "How does [Analyst's Name] respond to your guidance and directives?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement technical enforcement for critical security policies (e.g., mandatory access controls) to reduce the opportunity for deviation based on emotional response.
- **Human/Organizational Mitigation:** Provide leadership training for security managers on conscious leadership and managing team dynamics. Offer coaching or mentoring for analysts showing high deviation.
- **Process Mitigation:** Formalize and document the process for challenging and improving security procedures, creating a safe channel for feedback that isn't perceived as rebellion.