Contents

[10.10] Hysteresis Security Gaps

1. Operational Definition: The lagging or persistent effect of a security incident or a period of high stress on the system or team, where performance or security posture does not return to its original state even after the initial cause has been removed.

2. Main Metric & Algorithm:

- **Metric:** Post-Incident Performance Decay (PIPD). Formula: `PIPD = (Baseline_MTTA - Post_Incident_MTTA) / Baseline_MTTA`. A negative value indicates performance is worse after the incident.
- **Pseudocode:**

  python

  ```
  def calculate_pipd(team_id, major_incident_date):
      # Define time windows: 30 days before (baseline) and 30 days after (recovery)
      baseline_start = major_incident_date - timedelta(days=30)
      baseline_end = major_incident_date
      recovery_start = major_incident_date
      recovery_end = major_incident_date + timedelta(days=30)

      # Calculate MTTA for the baseline period
      baseline_mtta = calculate_mtta_team(baseline_start, baseline_end, team_id)

      # Calculate MTTA for the recovery period
      recovery_mtta = calculate_mtta_team(recovery_start, recovery_end, team_id)

      # Calculate the percentage change
      if baseline_mtta > 0:
          pipd = (recovery_mtta - baseline_mtta) / baseline_mtta
      else:
          pipd = 0
      return pipd  # e.g., -0.15 means a 15% slowdown after the incident
  ```

- **Alert Threshold:** `PIPD < -0.1` (A greater than 10% performance degradation persists for a month after a major incident).

3. Digital Data Sources (Algorithm Input):

- **SIEM / SOAR:** For calculating `MTTA` for a specific team over defined time periods.

4. Human-to-Human Audit Protocol: Conduct a "lessons learned" session 4-6 weeks after a major incident. Go beyond "what went wrong" and ask: "How is the team doing now? Are we still feeling the effects? Are we making different (perhaps overly cautious) decisions because of that event?" This qualitative data reveals hysteresis.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Use the PIPD metric to automatically trigger additional support resources (e.g., contractor SOC analysts) for teams recovering from a major incident.
- **Human/Organizational Mitigation:** Provide access to professional psychological support or counseling for teams after critical incidents to mitigate burnout and trauma.
- **Process Mitigation:** Formalize a post-incident recovery process that includes workload lightening, mentoring, and a phased return to full responsibilities for the affected team.