Contents

[6.6] Dependency Group Assumptions (baD)

1. Operational Definition: Based on Bion's Basic Assumption Dependency (baD), this is the unconscious assumption that an omnipotent leader, technology, or process will provide security and solve all problems. This manifests as a passive wait for instruction or tooling output and a lack of proactive threat hunting or independent analysis.

2. Main Metric & Algorithm:

- **Metric:** Proactive-to-Reactive Work Ratio (PRR). Formula: `(Time spent on proactive tasks) / (Time spent on reactive tasks)`.
- **Pseudocode:**

  python

  ```
  def calculate_prr(time_entries, proactive_categories):
      """
      time_entries: List of work log entries from a time-tracking tool.
      proactive_categories: List of project/task tags deemed 'proactive' (e.g., 'threat_hunt
      """
      proactive_time = 0
      reactive_time = 0
      for entry in time_entries:
          if entry.category in proactive_categories:
              proactive_time += entry.hours
          else:
              reactive_time += entry.hours
      return proactive_time / reactive_time if reactive_time > 0 else float('inf')
  ```

- **Alert Threshold:** `PRR < 0.2` (Less than 20% of time is spent on proactive work).

3. Digital Data Sources (Algorithm Input):

- **Time Tracking Software (e.g., Jira Tempo):** Fields: `author`, `timeSpentSeconds`, `category`, `project`.
- **SOAR/SIEM:** Can be used as a proxy by counting alerts handled (reactive) vs. hunting queries run (proactive).

4. Human-To-Human Audit Protocol: In one-on-one interviews, ask analysts: "What percentage of your time do you feel you spend waiting for alerts versus going out to look for threats? What prevents you from doing more proactive work? Do you feel you have the authority and tools to investigate things you find interesting?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Dedicate and protect "innovation time" in sprint plans. Implement and promote easy-to-use threat hunting platforms that empower analysts to explore data without needing deep SQL expertise.

- **Human/Organizational Mitigation:** Leadership must actively encourage and reward proactive behavior. Shift the performance metrics from purely reactive (MTTR, tickets closed) to include proactive measures (e.g., hunts completed, novel detection rules written).
- **Process Mitigation:** Schedule mandatory, rotating "hunting days" for each analyst where their primary responsibility is not to handle alerts but to pursue a proactive research question.