Contents

[2.10] Temporal Consistency Pressure

1. Operational Definition: The psychological pressure to maintain consistent activity levels or outputs over time, which can lead to security personnel generating or actioning low-value work simply to appear productive, rather than focusing on high-priority, strategic security tasks.

2. Main Metric & Algorithm:

- **Metric:** Low-Value Activity Ratio (LVAR). Formula: `LVAR = N_low_value_actions / N_total_actions`.
- **Pseudocode:**

  python

  ```
  def calculate_lvar(actions, low_value_indicators):
      """
      actions: List of action objects (e.g., alerts closed, tickets created, reports run).
      low_value_indicators: A list of patterns that signify low-value work (e.g., closing fa
      """
      total_actions = len(actions)
      low_value_count = 0

      for action in actions:
          for indicator in low_value_indicators:
              # e.g., if action.description contains "false positive" or action.type is "aut
              if indicator.matches(action):
                  low_value_count += 1
                  break # Count action only once

      if total_actions > 0:
          LVAR = low_value_count / total_actions
      else:
          LVAR = 0

      return LVAR
  ```

- **Alert Threshold:** `LVAR > 0.6` (Over 60% of an analyst's or team's actions are classified as low-value).

3. Digital Data Sources (Algorithm Input):

- **SIEM (Splunk):** Search for `(status=closed AND (resolution="false_positive" OR resolution="duplicate"))` by user.
- **Ticketing System (Jira):** `worklog` API. Analyze time spent on tickets tagged `"routine"`, `"maintenance"`.
- **Productivity Monitoring Tools:** If available, data on application usage (e.g., time in email client vs. threat intelligence platform).

4. Human-to-Human Audit Protocol: Conduct a work activity audit with a sample of analysts: "Walk me through your actions from yesterday. For each task, who was the beneficiary? What was the security outcome?" This helps distinguish between value-generating work and "busy work."

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Use the LVAR metric as a key performance indicator (KPI) for SOC efficiency, encouraging a focus on value over volume. Develop automation to handle routine low-value tasks.
- **Human/Organizational Mitigation:** Train managers to evaluate performance based on the impact and outcomes of work, not just the volume of activity. Shield analysts from pressure to be constantly "busy."
- **Process Mitigation:** Implement a weekly review where analysts propose one low-value process to automate or eliminate. Empower them to spend freed-up time on proactive threat hunting or research.