Contents

[5.4] Multitasking Degradation

1. Operational Definition: The performance cost and increased error rate associated with frequently switching between different security tasks (e.g., monitoring, investigating, reporting), which prevents deep focus on any single task.

2. Main Metric & Algorithm:

- **Metric:** Context Switch Frequency (CSF). Formula: `CSF = (Number of distinct alert/ticket IDs worked on by an analyst) / (Total shift time in hours)`.
- **Pseudocode:**

  python

  ```
  def calculate_csf(events, analyst_id, shift_start, shift_end):
      # Get all events for the analyst during their shift
      shift_events = get_events(assigned_to=analyst_id, start_time=shift_start, end_time=shi

      # Extract unique alert/ticket IDs that were interacted with (opened, updated, closed)
      unique_worked_items = set()
      for event in shift_events:
          if event.action in ['acknowledge', 'investigate', 'update', 'close']:
              unique_worked_items.add(event.alert_id)

      shift_duration_hours = (shift_end - shift_start).total_seconds() / 3600

      return len(unique_worked_items) / shift_duration_hours
  ```

- **Alert Threshold:** `CSF > 8` (The analyst is switching context more than 8 times per hour on average).

3. Digital Data Sources (Algorithm Input):

- **SIEM/SOAR Audit Logs:** The definitive source for user interactions. Query logs for `user=$analyst_id` and filter for actions like `alert_acknowledge`, `ticket_update`, `investigation_start`. Fields: `timestamp`, `user`, `action`, `object_id`.

4. Human-to-Human Audit Protocol: Interview the analyst: "How many different incidents or tasks are you typically juggling at once?" and "How often are you interrupted by new alerts, chats, or calls while working on something else?" High, frustrated numbers correlate with high CSF.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Configure alert queues to be assigned to roles, not individuals, allowing one analyst to focus on a deep investigation while others handle incoming triage.

- **Human/Organizational Mitigation:** Implement "focus blocks" on the shift schedule where analysts are not assigned new alerts and can work uninterrupted on complex investigations.
- **Process Mitigation:** Create a team protocol where non-urgent interruptions (Slack messages, questions) are channeled to a dedicated "help" role or channel instead of directly to analysts in deep work.