Contents

[7.1] Acute stress impairment

1. Operational Definition: A temporary degradation in cognitive and motor skills caused by the neuroendocrine response to an immediate, high-stakes security incident, manifesting as slowed reaction time, memory lapses, and physical tremors.

2. Main Metric & Algorithm:

- **Metric:** Stress-Induced Performance Degradation (SIPD). Formula: `SIPD = (Average task completion time during incidents) / (Average task completion time during calm periods)`.
- **Pseudocode:**

  python

  ```
  def calculate_sipd(task_logs, incident_periods):
      """
      task_logs: Logs of routine, repetitive tasks (e.g., run standard query, ticket triage)
      incident_periods: List of start/end times for major incidents
      """
      # 1. Calculate avg. task time during incident periods
      tasks_during_incidents = []
      for period in incident_periods:
          period_tasks = [t for t in task_logs if period.start <= t.timestamp <= period.end]
          tasks_during_incidents.extend(period_tasks)

      avg_time_during_incident = calculate_avg_task_time(tasks_during_incidents)

      # 2. Calculate avg. task time during calm periods (e.g., 1 week before incident)
      calm_period_tasks = get_tasks_from_calm_period(task_logs, incident_periods)
      avg_time_calm = calculate_avg_task_time(calm_period_tasks)

      # 3. Calculate SIPD ratio
      if avg_time_calm > 0:
          SIPD = avg_time_during_incident / avg_time_calm
      else:
          SIPD = 1  # No degradation if no baseline
      return SIPD
  ```

- **Alert Threshold:** `SIPD > 1.5` (Task performance is 50% slower during high-stress incidents)

3. Digital Data Sources (Algorithm Input):

- **SOAR Platform Logs:** Timestamps for the initiation and completion of automated or manual playbook steps.
- **Ticketing System API:** Time-to-acknowledge and time-to-resolution metrics for tickets.

- **Incident Declarations:** A log of when major incidents were formally declared and resolved.

4. Human-to-Human Audit Protocol: Simulate a high-fidelity, stressful incident in a training environment. Use biometric sensors (heart rate variability, galvanic skin response) to measure stress levels and correlate them with performance metrics on standardized tasks (e.g., time to contain a simulated breach). Debrief afterwards on subjective feelings of impairment.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Design SOAR playbooks for high-severity incidents to have more automated steps and fewer manual, error-prone tasks, reducing the cognitive load on the impaired analyst.
- **Human/Organizational Mitigation:** Introduce a "buddy system" during major incidents, pairing a stressed primary responder with a secondary analyst whose role is to double-check commands, provide calm guidance, and execute tasks under instruction.
- **Process Mitigation:** Mandate the use of written checklists for critical actions during a declared incident. The physical act of checking a box can help focus a stressed mind and prevent memory lapses or skipped steps.