Contents

[2.2] Time pressure cognitive degradation

1. Operational Definition: A state where excessive time pressure impairs an analyst's cognitive functions (e.g., attention, memory, logical reasoning), leading to an increase in errors during security task performance.

2. Main Metric & Algorithm:

- **Metric:** Error Rate During High-Pressure Periods (ERHPP). Formula: `ERHPP = (Number of erroneous actions during high-pressure periods) / (Total actions during high-pressure periods)`.
- **Pseudocode:**

  python

```
def calculate_erhpp(action_logs, ticket_data, pressure_threshold_minutes=30):
    """
    action_logs: Logs of analyst actions (e.g., alert closures, rule modifications)
    ticket_data: Ticket data to determine pressure periods (high volume + short deadlines)
    """
    # 1. Identify high-pressure periods (e.g., ticket volume > 90th percentile AND avg. de
    pressure_periods = identify_high_pressure_periods(ticket_data, pressure_threshold_minu

    # 2. Filter actions that occurred during these periods
    actions_during_pressure = [
        action for action in action_logs
        if is_during_period(action.timestamp, pressure_periods)
    ]

    # 3. Identify erroneous actions (e.g., misclassified severity, incorrect asset tag, fa
    erroneous_actions = [
        action for action in actions_during_pressure
        if action.result == 'false_negative' or action.was_rolled_back is True
    ]

    # 4. Calculate ERHPP
    total_actions = len(actions_during_pressure)
    ERHPP = len(erroneous_actions) / total_actions if total_actions > 0 else 0
    return ERHPP
```

- **Alert Threshold:** `ERHPP > 0.25` (More than 25% of actions during high-pressure periods are erroneous)

3. Digital Data Sources (Algorithm Input):

- **SIEM/Ticketing System API:** To calculate ticket volume and deadline metrics to define pressure periods.

- **SOAR Platform Logs / Git History / Configuration Management Logs:** To get a detailed audit trail of analyst actions and their outcomes (e.g., `action`, `timestamp`, `user`, `success_status`, `rollback_status`).

4. Human-to-Human Audit Protocol: Conduct a retrospective analysis (blameless post-mortem) of a recent incident or false negative. Guide the discussion: "Walk us through your thought process during the event. What was the time pressure like? Did you feel it was difficult to concentrate or remember procedures at any point?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement a "circuit breaker" in the SOAR platform that flags for supervisory review any high-severity action taken by an analyst who has been processing a high volume of tickets in a short time window.
- **Human/Organizational Mitigation:** Introduce mandatory, enforced micro-breaks (5 minutes every hour) during declared high-pressure incidents or periods of critical vulnerability patching.
- **Process Mitigation:** Develop and train on "high-pressure playbooks" that simplify decision trees and provide clear, step-by-step guidance for the most critical and time-sensitive tasks.