Contents

[2.2] Degradazione cognitiva da pressione temporale

1. Definizione Operativa: Uno stato in cui la pressione temporale eccessiva compromette le funzioni cognitive di un analista (es. attenzione, memoria, ragionamento logico), portando a un aumento degli errori durante l'esecuzione di compiti di sicurezza.

2. Metrica Principale e Algoritmo:

- **Metrica:** Tasso di Errori Durante Periodi ad Alta Pressione (ERHPP). Formula: `ERHPP = (Numero di azioni erronee durante periodi ad alta pressione) / (Azioni totali durante periodi ad alta pressione)`.
- **Pseudocodice:**

  python

  ```
  def calculate_erhpp(action_logs, ticket_data, pressure_threshold_minutes=30):
      """
      action_logs: Log delle azioni degli analisti (es. chiusure di allarmi, modifiche di re
      ticket_data: Dati dei ticket per determinare i periodi di pressione (alto volume + dea
      """
      # 1. Identificare periodi ad alta pressione (es. volume ticket > 90° percentile AND de
      pressure_periods = identify_high_pressure_periods(ticket_data, pressure_threshold_minu

      # 2. Filtrare le azioni che si sono verificate durante questi periodi
      actions_during_pressure = [
          action for action in action_logs
          if is_during_period(action.timestamp, pressure_periods)
      ]

      # 3. Identificare azioni erronee (es. gravità mal classificata, tag asset errato, fals
      erroneous_actions = [
          action for action in actions_during_pressure
          if action.result == 'false_negative' or action.was_rolled_back is True
      ]

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

- **Soglia di Allarme:** `ERHPP > 0.25` (Più del 25% delle azioni durante periodi ad alta pressione sono erronee)

3. Fonti di Dati Digitali (Input dell'Algoritmo):

- **API del Sistema SIEM/Ticketing:** Per calcolare le metriche di volume dei ticket e deadline per definire i periodi di pressione.

- **Log della Piattaforma SOAR / Cronologia Git / Log di Gestione della Configurazione:** Per ottenere un audit trail dettagliato delle azioni degli analisti e dei loro risultati (es. `action`, `timestamp`, `user`, `success_status`, `rollback_status`).

4. Protocollo di Audit da Persona a Persona: Condurre un'analisi retrospettiva (post-mortem senza colpa) di un incidente recente o di un falso negativo. Guidare la discussione: "Ripercorri il tuo processo di pensiero durante l'evento. Qual era il livello di pressione temporale? Hai sentito fosse difficile concentrarsi o ricordare le procedure in qualche momento?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare un "circuit breaker" nella piattaforma SOAR che contrassegna per la revisione supervisiva qualsiasi azione ad alta gravità intrapresa da un analista che ha elaborato un alto volume di ticket in una breve finestra di tempo.
- **Mitigazione Umana/Organizzativa:** Introdurre micro-pause obbligatorie applicate (5 minuti ogni ora) durante incidenti dichiarati ad alta pressione o periodi di patching critico di vulnerabilità.
- **Mitigazione dei Processi:** Sviluppare e addestrare "playbook ad alta pressione" che semplificano gli alberi decisionali e forniscono una guida chiara e passo-passo per i compiti più critici e sensibili al tempo.