Contents

[7.10] Vulnerabilità del Periodo di Recupero

1. Definizione Operativa: L'aumento della suscettibilità agli errori e ai lapsi nel giudizio immediatamente dopo un periodo di stress elevato o un incidente critico, a causa dell'esaurimento cognitivo e dello sforzo del corpo per ripristinare l'omeostasi, creando una finestra di vulnerabilità.

2. Metrica Principale e Algoritmo:

- **Metrica: Tasso di Errore Post-Incidente (PIER)**. Formula: `PIER = N_errors / N_actions` per `N_hours` dopo la risoluzione dell'incidente.
- **Pseudocodice:**

  python

  ```
  def calculate_pier(employee_id, incident_end_time, observation_hours=8):
      start_window = incident_end_time
      end_window = incident_end_time + timedelta(hours=observation_hours)

      # Ottenere tutte le azioni eseguite dall'analista nella finestra di recupero
      actions = query_soar_logs(employee_id, start_window, end_window)

      errors = 0
      for action in actions:
          # Definire un errore (es. esecuzione di script fallita, regola mal configurata, ap
          if action.status == "Failed" or action.comment == "":
              errors += 1

      total_actions = len(actions)
      if total_actions > 0:
          pier = errors / total_actions
      else:
          pier = 0
      return pier
  ```

- **Soglia di Allerta:** `PIER > 0.25` (25% delle azioni nelle 8 ore post-incidente sono erronee).

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

- **Piattaforma SOAR:** `playbook_execution_logs.status`, `timestamp`, `user`.
- **Sistema di Ticketing:** `issue.updates` (per i commenti), `user`, `timestamp`.

4. Protocollo di Audit Umano-Umano: Audit mirato del lavoro svolto nelle ore successive a un incidente significativo. Controllo informale da parte di un manager: "Come ti senti dopo quell'ultimo incidente? Ti sarebbe utile trasferire alcuni dei tuoi compiti di routine per il resto della giornata?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare un sistema che automaticamente contrassegna le azioni intraprese da analisti che sono stati appena coinvolti in un incidente critico per una revisione secondaria.
- **Mitigazione Umana/Organizzativa:** Formalizzare una politica di "periodo di recupero", offrendo agli analisti compiti di duty leggero, un turno accorciato, o tempo libero dopo una risposta agli incidenti critica.
- **Mitigazione di Processo:** Rendere obbligatorio un procedimento di handover in cui un analista che esce da un incidente ad alto stress deve fare un briefing al suo sostituto ed è esplicitamente sollevato dal servizio per un periodo definito.