# Contents



## [7.8] Memoria Compromessa da Cortisolo

**1. Definizione Operativa:** L'impatto negativo degli ormoni dello stress cronico sulla memoria di lavoro e il ricordo, portando a passaggi dimenticati nelle procedure, dettagli mancati negli avvisi, o un'incapacità di applicare lezioni apprese dai passati incidenti.

**2. Metrica Principale e Algoritmo:**

- **Metrica: Tasso di Deviazione Procedurale (PDR)**. Formula: `PDR = N_tasks_missing_steps / N_audited_tasks`.
- **Pseudocodice:**

  python

  ```
  def calculate_pdr(employee_id, start_date, end_date):
      # Ottenere un campione di compiti completati (es. incidenti chiusi)
      completed_tasks = query_soar_for_completed_tasks(employee_id, start_date, end_date)

      deviations = 0
      for task in completed_tasks:
          # Verificare i registri di esecuzione del playbook rispetto allo standard aureo
          expected_steps = get_playbook_steps(task.playbook_id)
          executed_steps = get_executed_steps(task.incident_id)
          if expected_steps != executed_steps:  # Confrontare gli insiemi di passaggi richie
              deviations += 1

      total_audited = len(completed_tasks)
      if total_audited > 0:
          pdr = deviations / total_audited
      else:
          pdr = 0
      return pdr
  ```

- **Soglia di Allerta:** `PDR > 0.15` (15% dei compiti controllati mostrano passaggi critici mancati).

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

- **Piattaforma SOAR (es. XSOAR):** `playbook_id`, `task.executed_steps`, `incident.owner`.
- **Database CMDB / Procedure:** `standard_playbook.steps`.

**4. Protocollo di Audit Umano-Umano:** Osservazione diretta o metodo "walk-through" in cui l'analista spiega come eseguirebbe una procedura di routine. "Puoi illustrarmi i passaggi del playbook di contenimento per un incidente di phishing?"

**5. Azioni di Mitigazione Consigliate:**

- **Mitigazione Tecnica/Digitale:** Integrare le checklist interattive direttamente nel flusso di lavoro dell'analista all'interno di SOAR o del sistema di ticketing per guidarli passo-passo.

- **Mitigazione Umana/Organizzativa:** Implementare un sistema di micro-formazione just-in-time che fornisce moduli di formazione brevi e focalizzati in base ai recenti errori.
- **Mitigazione di Processo:** Semplificare e standardizzare le procedure. Incoraggiare l'uso di wiki personali o block notes per gli analisti per annotare i punti chiave di apprendimento.