Contents

[2.6] Pattern di Esaurimento Temporale

1. Definizione Operativa: Uno stato di capacità cognitiva ridotta e vigore della sicurezza che si verifica prevedibilmente in certi momenti durante un periodo di lavoro (es. poco prima di una pausa, fine di un turno lungo), portando a un aumento degli errori.

2. Metrica Principale e Algoritmo:

- **Metrica:** Tasso di Errori da Esaurimento (EER). Formula: `EER = N_errors_last_hour / N_errors_total`.
- **Pseudocodice:**

  python

  ```
  def calculate_eer(events, shift_start, shift_duration_hours):
      """
      events: Lista di oggetti errore/incidente con un timestamp.
      Esempio: Allarmi SIEM chiusi falsamente, tentativi di login falliti da analisti SOC, e
      """
      total_errors = len(events)
      # Ottenere gli errori dell'ultima ora del turno
      errors_last_hour = [e for e in events if e.timestamp > (shift_start + shift_duration_h

      if total_errors > 0:
          EER = len(errors_last_hour) / total_errors
      else:
          EER = 0

      return EER
  ```

- **Soglia di Allarme:** `EER > 0.3` (Più del 30% degli errori si verificano nell'ultima ora di un turno).

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

- **SIEM (Splunk, Elastic):** Query per `(event_type="alert" AND status="closed" AND resolution="false_positive")` per analista, raggruppato per ora del loro turno.
- **Log di Accesso:** Log `vpn` o `bastion_host` per tentativi di login falliti da analisti SOC, raggruppati per ora del giorno.
- **Log CI/CD:** Esecuzioni di pipeline fallite o rollback, analizzate in base all'ora del giorno in cui sono state avviate.

4. Protocollo di Audit da Persona a Persona: Sondaggio anonimo agli analisti: "Su una scala da 1 a 5, come ti senti la concentrazione e l'attenzione ai dettagli nell'ultima ora del tuo turno rispetto alla prima ora?" Correlare le risposte con la metrica quantitativa.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare una regola di "rilevamento dell'affaticamento" nella piattaforma SOAR che escalate automaticamente tutti gli allarmi dall'ultima ora di un turno a un analista secondario per peer review.
- **Mitigazione Umana/Organizzativa:** Obbligare una revisione "fresh-eyes" per i cambiamenti critici o le chiusure di allarmi proposte nell'ultima ora di un turno. Adattare i modelli di turno per evitare periodi lunghi e ininterrotti su compiti ad alta intensità.
- **Mitigazione dei Processi:** Pianificare la manutenzione critica e i compiti complessi al di fuori delle finestre di esaurimento note. Istituire micro-pause obbligatorie ogni 90 minuti.