Contents

[4.7] Errori Innescati dall'Ansia

1. Definizione Operativa: Uno stato di elevata ansia che compromette la funzione cognitiva, portando a errori procedurali, errori di configurazione ed esecuzione goffa durante compiti critici per la sicurezza.

2. Metrica Principale e Algoritmo:

- **Metrica:** Anxiety-Induced Error Rate (AIER). Formula: `AIER = N_errori_durante_alta_ansia / N_errori_totali`. *Usiamo il proxy dei periodi di "alta ansia" tramite conteggi di incidenti ad alta severità.*
- **Pseudocodice:**

  python

  ```
  def calculate_aier(error_log, incident_log, time_window='1h'):
      """
      error_log: Log di errori di configurazione, burst di accesso non riusciti, esecuzioni
      incident_log: Lista di incidenti di sicurezza con severità e tempo.
      """
      # Identificare i bin di tempo con incidenti di severità ALTA o CRITICA attivi
      high_stress_windows = get_high_severity_incident_windows(incident_log)

      total_errors = len(error_log)
      errors_in_stress = 0

      for error in error_log:
          # Verificare se questo errore si è verificato durante una finestra di stress eleva
          if is_during_window(error['time'], high_stress_windows):
              errors_in_stress += 1

      aier = errors_in_stress / total_errors if total_errors else 0
      return aier
  ```

- **Soglia di Allarme:** `AIER > 0.6` (Oltre il 60% degli errori si verificano durante periodi di elevata ansia).

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

- **SIEM/Syslog:** Log per i fallimenti di autenticazione, errori di gestione della configurazione, fallimenti di esecuzione degli script.
- **Sistema di Ticketing (Jira):** API per recuperare i dati degli incidenti, includendo `severity` e `start_time`/`end_time`.

4. Protocollo di Audit Umano-su-Umano: Durante un periodo di basso stress, intervistare gli analisti sui recenti incidenti ad alta severità: "Come ti sentivi durante l'incidente? Puoi descrivermi le tue azioni? Ricordi di aver commesso errori sotto pressione?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare controlli di sanità mentale automatizzati e controlli pre-commit per i comandi critici per catturare gli errori prima che vengano eseguiti.
- **Mitigazione Umana/Organizzativa:** Introdurre formazione sulla consapevolezza e la gestione dello stress nel SOC. Assicurare un personale adeguato e programmi di pausa durante i principali incidenti.
- **Mitigazione del Processo:** Sviluppare e praticare runbook e playbook ad alta fedeltà per scenari comuni ad alta tensione per ridurre il carico cognitivo.