Contents

[10.3] Vulnerabilità dei Punti di Flesso

1. Definizione Operativa: Una soglia quantificabile nel carico del sistema, nel volume degli avvisi o nei livelli di stress oltre il quale le prestazioni del team di sicurezza si degradano rapidamente e in modo non lineare, portando a un netto aumento degli errori.

2. Metrica Principale e Algoritmo:

- **Metrica:** Coefficiente del Punto di Flesso (TPC). Questo identifica il valore di soglia per una metrica (X) oltre il quale il tasso di errore (Y) aumenta significativamente. Viene trovato adattando un modello di regressione in pezzi per trovare il punto di frattura.
- **Pseudocodice:**

  python

  ```
  # Questo richiede librerie statistiche (ad es. `pwlf` per Python)
  def find_tipping_point(historical_data):
      # historical_data è un elenco di tuple: (independent_var, error_rate)
      # ad es. (hourly_alert_volume, missed_alert_percentage)
      x = [point[0] for point in historical_data]
      y = [point[1] for point in historical_data]

      # Adatta una regressione lineare in pezzi con un punto di frattura
      my_pwlf = pwlf.PiecewiseLinFit(x, y)
      breakpoint = my_pwlf.fit(1)  # Adatta per 1 punto di frattura

      # Calcola la pendenza dopo il punto di frattura
      slopes = my_pwlf.slopes
      post_tip_slope = slopes[1]  # Pendenza del secondo segmento

      return breakpoint[0], post_tip_slope
  ```

- **Soglia di Avviso:** Un sistema di monitoraggio in tempo reale attiva un avviso quando la metrica definita (ad es. volume degli avvisi) supera il valore `breakpoint` calcolato.

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

- **SIEM:** (ad es. Splunk) per dati in serie temporali su `alert_volume_per_hour`.
- **Sistema di Ticketing:** (ad es. Jira) per il corrispondente `missed_alerts_per_hour` o `MTTA_per_hour`.

4. Protocollo di Audit Umano-Umano: Intervista i manager e gli analisti del SOC: "A che punto durante una giornata impegnativa le prestazioni del team iniziano a diminuire? È un declino graduale o uno 'scatto' improvviso? Qual è il segno rivelatore che sei sopraffatto?" Correla questi dati qualitativi con l'analisi del punto di frattura quantitativa.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Configura gli avvisi per notificare in modo preventivo i manager quando le metriche chiave (ad es. lunghezza della coda degli avvisi) si avvicinano al punto di flesso storico.
- **Mitigazione Umana/Organizzativa:** Implementa l'allocazione dinamica delle risorse: disponi di un piano predefinito per portare analisti aggiuntivi in turno o spostare i carichi di lavoro una volta raggiunto il punto di flesso.
- **Mitigazione dei Processi:** Riprogetta i processi di triage per includere il filtraggio aggressivo degli avvisi e le regole di deprioritizzazione che si attivano automaticamente quando viene raggiunto il punto di flesso.