Contents

[4.3] Trasferimento della Fiducia ai Sistemi 1

[4.3] Trasferimento della Fiducia ai Sistemi

1. Definizione Operativa: L'attribuzione inconscia di affidabilità e infallibilità umana ai sistemi di sicurezza automatizzati (es. EDR, SIEM, strumenti AI), portando a eccessiva affidanza, ridotta vigilanza e incapacità di mettere in discussione output erronei.

2. Metrica Principale e Algoritmo:

- **Metrica:** Automated Decision Challenge Rate (ADCR). Formula: `ADCR = N_decisioni_contestate / N_decisioni_automatizzate_totali`.
- **Pseudocodice:**

  python

  ```
  def calculate_adcr(incident_log, time_window='7d'):
      """
      incident_log: Lista di incidenti dal sistema di ticketing (es. Jira) con chiavi ['key'
      """
      # Filtrare gli incidenti dove un sistema automatizzato ha fornito una raccomandazione
      automated_incidents = [i for i in incident_log if i['automated_recommendation'] is not

      # Contare gli incidenti dove la decisione finale DIFFERISCE dalla raccomandazione auto
      challenged_incidents = [i for i in automated_incidents if i['final_decision'] != i['au

      adcr = len(challenged_incidents) / len(automated_incidents) if automated_incidents els
      return adcr
  ```

- **Soglia di Allarme:** `ADCR < 0.1` (Meno del 10% delle raccomandazioni automatizzate è mai messo in discussione o ribaltato).

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

- **Sistema di Ticketing (Jira/ServiceNow):** Query API REST per recuperare incidenti. Richiede un campo personalizzato per `automated_recommendation` e il campo standard `resolution`.
- **Piattaforma SOAR:** Log delle raccomandazioni del playbook e delle successive azioni dell'analista.

4. Protocollo di Audit Umano-su-Umano: Eseguire un esercizio di tavolo dove un falso positivo ovvio e controllato viene iniettato dal sistema automatizzato. Osservare e intervistare gli analisti sul loro processo: "Perché hai fiducia/non hai fiducia nella raccomandazione del sistema?" Tracciare il tempo e i passaggi impiegati per identificare l'errore.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Modificare l'UI/UX per visualizzare i confidence score e le prove chiave per le decisioni automatizzate in modo prominente, piuttosto che solo un risultato binario.

- **Mitigazione Umana/Organizzativa:** Condurre formazione sulle limitazioni dell'AI/automazione, insegnando agli analisti *come* funzionano i sistemi e le loro modalità di guasto comuni.
- **Mitigazione del Processo:** Obbligare un processo di "second look" per il 10% casuale delle decisioni automatizzate, richiedendo un breve commento da un analista diverso.