Contents

[1.9] Prova sociale basata sull'autorità

1. Definizione operativa: La tendenza degli individui ad adottare comportamenti non sicuri perché osservano figure di autorità o una maggioranza percepita dei loro coetanei che si impegnano negli stessi comportamenti, assumendo che debba essere accettabile.

2. Metrica principale e algoritmo:

- **Metrica:** Latenza di adozione della pratica non sicura (IPAL). Formula: `IPAL = Tempo medio tra l'azione non sicura osservata di una figura di autorità e la sua prima replica da parte di un subordinato`.
- **Pseudocodice:**

  python

  ```
  # Questo è complesso e potrebbe richiedere l'analisi di sequenze di eventi.
  def calculate_ipal(log_data, hr_org_chart, start_date, end_date):
      # 1. Definire un elenco di azioni non sicure (ad es., 'disable_av', 'use_unsanctioned_
      insecure_actions = [...]

      # 2. Trovare queste azioni eseguite da manager/director/VP
      authority_events = query_events(users=get_authority_users(hr_org_chart), actions=insec

      replication_times = []
      # 3. Per ogni evento di autorità, verificare se i loro rapporti diretti hanno eseguito
      for auth_event in authority_events:
          reports = get_direct_reports(auth_event.user, hr_org_chart)
          for report in reports:
              report_events = query_events(users=[report], actions=[auth_event.action], date
              if report_events:
                  time_delta = report_events[0].time - auth_event.time
                  replication_times.append(time_delta)

      IPAL = sum(replication_times, timedelta(0)) / len(replication_times) if replication_ti
      return IPAL
  ```

- **Soglia di avviso:** Una correlazione statisticamente significativa (`p < 0.05`) tra un'azione non sicura dell'autorità e successive azioni simili dal team, con un `IPAL < 7 giorni` medio.

3. Fonti di dati digitali (input dell'algoritmo):

- **Log EDR/Proxy/SIEM:** Per rilevare azioni non sicure specifiche (ad es., esecuzione di software non approvato, accesso a siti bloccati).
- **API HRIS:** Per ottenere dati sulla gerarchia organizzativa (`manager_id`, `employee_id`).

4. Protocollo di audit da umano a umano: Nei focus group, presenta uno scenario: "Il tuo manager usa spesso un Dropbox personale per condividere file di grandi dimensioni per il lavoro perché è 'più veloce.' Cosa faresti?" Misurare il livello di accettazione di questo comportamento.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Applicare i controlli tecnici in modo uniforme. Se una pratica non è sicura, il sistema dovrebbe impedirla per tutti, indipendentemente dal ruolo.
- **Mitigazione umana/organizzativa:** I leader devono essere tenuti a uno standard superiore e agire come modelli di comportamento sicuro. Denunciare pubblicamente e correggere le pratiche non sicure a tutti i livelli.
- **Mitigazione dei processi:** Creare canali sicuri per i dipendenti a segnalare comportamenti non sicuri che osservano nella leadership senza paura di ritorsioni.