Contents

[2.4] Bias del Presente negli Investimenti di Sicurezza

1. Definizione Operativa: La tendenza dei decisori a dare priorità ai progetti di sicurezza con risultati immediati e visibili rispetto a quelli con valore strategico a lungo termine, portando a una negligenza dell'igiene di sicurezza fondamentale.

2. Metrica Principale e Algoritmo:

- **Metrica:** Rapporto di Investimento Strategico (SIR). Formula: `SIR = man_hours_long_term / total_security_man_hours`.
- **Pseudocodice:**

  python

  ```
  def calculate_sir(projects, fiscal_year):
      """
      projects: Lista di oggetti progetto con campi: ['project_id', 'type', 'man_hours_consu
      project.type: 'reactive' (es. incident response, risultati di pentest), 'strategic' (e
      """
      strategic_hours = 0
      total_hours = 0

      for project in projects:
          if project.fiscal_year == fiscal_year:
              total_hours += project.man_hours_consumed
              if project.type == 'strategic':
                  strategic_hours += project.man_hours_consumed

      if total_hours > 0:
          SIR = strategic_hours / total_hours
      else:
          SIR = 0

      return SIR
  ```

- **Soglia di Allarme:** `SIR < 0.25` (Meno del 25% dello sforzo è speso in lavoro di sicurezza strategico a lungo termine).

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

- **Strumento di Portfolio Progettuale (Jira Portfolio, Asana):** Endpoint `projects`. Campi: `custom_field.strategic_flag`, `time_tracked`.
- **Sistema di Gestione Finanziaria (SAP, QuickBooks):** `cost_centers` per il budget di sicurezza. Analizzare la spesa in nuovi strumenti (reattivi) vs. addestramenti/platform engineering (strategici).
- **Software di Time Tracking (Toggl, Harvest):** `time_entries` taggati con ID progetto, analizzati in base alla classificazione del progetto.

4. Protocollo di Audit da Persona a Persona: Esaminare il portfolio progettuale dell'ultimo anno con il CISO e i responsabili dei team: "Quali di questi progetti è stata una risposta diretta a un incidente o a un risultato di audit? Quali sono state iniziative proattive? Quale percentuale del tempo del tuo team stimate venga speso in emergency response vs. building?" Confrontare la loro percezione con i dati.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare dashboard che visualizzano la metrica SIR per la leadership, legandola agli indicatori di rischio chiave.
- **Mitigazione Umana/Organizzativa:** Legare una parte dei bonus di performance della leadership della sicurezza al miglioramento della metrica SIR nel tempo.
- **Mitigazione dei Processi:** Obbligare un'aliquota minima (es. 30%) degli obiettivi e risultati chiave (OKR) trimestrali del team della sicurezza a essere dedicata a iniziative strategiche.