Contents

[1.6] Gradiente di autorità che inibisce la segnalazione della sicurezza

1. Definizione operativa: La riluttanza osservabile del personale junior a segnalare problemi di sicurezza, violazioni di politica o potenziali incidenti agli individui di livello superiore a causa di barriere gerarchiche percepite o paura di conseguenze negative.

2. Metrica principale e algoritmo:

- **Metrica:** Indice di gradiente di segnalazione (RGI). Formula: `RGI = 1 - (N_rapporti_da_junior / N_rapporti_da_senior)`.
- **Pseudocodice:**

  python

  ```
  def calculate_rgi(ticketing_data, hr_data, start_date, end_date):
      # Ottenere tutti i ticket relativi alla sicurezza
      sec_tickets = query_tickets(type='security_incident', date_range=(start_date, end_date

      junior_count = 0
      senior_count = 0

      for ticket in sec_tickets:
          reporter_role = get_employee_role(ticket.reporter_id, hr_data)
          if reporter_role in ['junior', 'analyst_i', 'associate']:
              junior_count += 1
          elif reporter_role in ['senior', 'manager', 'director', 'vp']:
              senior_count += 1

      total_reports = junior_count + senior_count
      if total_reports == 0:
          return 0 # Evitare la divisione per zero

      # Se junior e senior segnalano allo stesso modo, RGI=0. Se solo i senior segnalano, RG
      RGI = 1 - (junior_count / total_reports)
      return RGI
  ```

- **Soglia di avviso:** `RGI > 0.7` (ad es., il personale junior contribuisce con meno del 30% di tutti i rapporti di sicurezza).

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

- **API del sistema di ticketing** (ServiceNow, Jira): Campi `reporter`, `created_date`, `type`.
- **API HRIS** (Workday, SAP SuccessFactors): Per mappare `reporter` al loro grado di lavoro/ruolo (`employee_id`, `job_level`).

4. Protocollo di audit da umano a umano: Eseguire un sondaggio anonimo chiedendo: "Ti sentirai a tuo agio a segnalare un errore di sicurezza commesso dal tuo supervisore diretto?" e "Hai

mai testimoniato un problema di sicurezza che non hai segnalato? Se sì, perché?" Analizzare le risposte per grado di lavoro.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Implementare e promuovere pesantemente un canale di segnalazione completamente anonimo (ad es., linea telefonica, modulo web) gestito da una terza parte o da un dipartimento separato come l'Etica.
- **Mitigazione umana/organizzativa:** La leadership deve pubblicamente elogiare e premiare gli individui (in particolare i junior) per aver sollevato le preoccupazioni. I manager devono condividere storie dei loro stessi errori di sicurezza passati.
- **Mitigazione dei processi:** Formalizzare un processo di segnalazione "Near-Miss" non punitivo che sia disaccoppiato dalle revisioni delle prestazioni.