Contents

[1.8] Normalizzazione dell'eccezione esecutiva

1. Definizione operativa: Il modello stabilito in cui le politiche di sicurezza vengono regolarmente bypassate o le eccezioni vengono concesse ai dirigenti senior (livello C, VP), creando un sistema percepito "a due livelli" e minando la cultura generale della sicurezza.

2. Metrica principale e algoritmo:

- **Metrica:** Rapporto di eccezione esecutiva (EER). Formula: `EER = N_eccezioni_per_dirigenti / N_eccezioni_per_tutti_gli_altri`.
- **Pseudocodice:**

  python

  ```
  def calculate_eer(ticketing_data, hr_data, start_date, end_date):
      # Ottenere tutti i ticket di eccezione di politica di sicurezza approvati
      all_exceptions = query_tickets(type='security_exception', status='approved', date_rang

      exec_exceptions = 0
      non_exec_exceptions = 0

      for ticket in all_exceptions:
          requester_role = get_employee_role(ticket.requester_id, hr_data)
          if requester_role in ['c_level', 'vp', 'svp', 'executive']:
              exec_exceptions += 1
          else:
              non_exec_exceptions += 1

      EER = exec_exceptions / non_exec_exceptions if non_exec_exceptions > 0 else float('inf
      return EER
  ```

- **Soglia di avviso:** `EER > 1.5` (ad es., ai dirigenti vengono concesse eccezioni a un tasso del 50% superiore rispetto ai non dirigenti, aggiustato per la dimensione della popolazione).

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

- **API del sistema di ticketing** (ServiceNow, Jira): ticket `security_exception` con `requester`, `approval_status`.
- **API HRIS:** Per mappare `requester` al ruolo e al dipartimento del lavoro.

4. Protocollo di audit da umano a umano: Esaminare i verbali dei comitati di sicurezza governance o eccezioni. Analizzare il linguaggio utilizzato per giustificare le eccezioni per i dirigenti rispetto ad altri dipendenti. Intervistare i manager di medio livello sulla loro percezione dell'equità delle politiche.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Implementare controlli tecnici che siano agnostici dal ruolo. Se un'eccezione è tecnicamente necessaria per un dirigente, dovrebbe essere documentata e

applicata in modo da minimizzare il rischio, proprio come qualsiasi altra eccezione.

- **Mitigazione umana/organizzativa:** Il CISO e l'amministratore delegato devono pubblicamente impegnarsi agli stessi standard di sicurezza di tutti i dipendenti. La formazione sulla sicurezza deve essere obbligatoria dall'alto verso il basso.
- **Mitigazione dei processi:** Stabilire un comitato trasparente di governance delle eccezioni di sicurezza con rappresentanza multifunzionale (ad es., IT, Sicurezza, Legale, HR) per esaminare tutte le richieste di eccezione rispetto a criteri coerenti e basati sul rischio.