Contents

[2.1] Bypass della sicurezza indotto dall'urgenza

1. Definizione Operativa: La tendenza del personale a eludere i protocolli di sicurezza stabiliti quando soggetto a pressione temporale percepita, aumentando significativamente il rischio di errore e introducendo vulnerabilità.

2. Metrica Principale e Algoritmo:

- **Metrica:** Tasso di Bypass della Sicurezza (SBR). Formula: `SBR = (Numero di violazioni delle procedure di sicurezza) / (Numero totale di opportunità di violazione)`.
- **Pseudocodice:**

  python

  ```
  def calculate_sbr(access_logs, change_logs, start_date, end_date):
      """
      access_logs: Log dai sistemi sicuri
      change_logs: Log dal sistema di gestione dei cambiamenti
      """
      # 1. Identificare "opportunità": Azioni ad alto impatto eseguite (es. deployment in pr
      all_actions = get_high_impact_actions(access_logs, change_logs, start_date, end_date)

      # 2. Per ogni azione, verificare se ha violato la procedura (nessun ticket, al di fuor
      violations = 0
      for action in all_actions:
          # Verificare se esiste un ticket di cambio approvato per questa azione/ora/sistema
          corresponding_ticket = find_change_ticket(action)
          if not corresponding_ticket or corresponding_ticket.status != 'approved':
              violations += 1

      total_actions = len(all_actions)
      SBR = violations / total_actions if total_actions > 0 else 0
      return SBR
  ```

- **Soglia di Allarme:** `SBR > 0.1` (Oltre il 10% delle azioni ad alto impatto bypassano il controllo dei cambiamenti)

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

- **API del Sistema di Gestione dei Cambiamenti:** Per ottenere un elenco dei cambiamenti approvati (`ticket_id`, `approved_time`, `affected_systems`).
- **Log dell'Infrastruttura (commit Git, pipeline CI/CD, Log Firewall/Admin):** Per ottenere un elenco di tutte le azioni ad alto impatto effettivamente eseguite (`action`, `timestamp`, `system`, `user`).

4. Protocollo di Audit da Persona a Persona: Esaminare un campione di recenti modifiche ad alto impatto. Per ogni modifica, intervistare la persona che l'ha eseguita e il suo manager: "Qual

era il driver aziendale per questo cambio? Illustrami il processo di approvazione dei cambiamenti." Corrobora la storia con l'audit trail del sistema di gestione dei cambiamenti.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare l'enforcement tecnico (es. pipeline di deployment che richiedono un numero di ticket di cambio valido prima di eseguire) invece di fare affidamento sui controlli procedurali.
- **Mitigazione Umana/Organizzativa:** Promuovere una cultura in cui il rispetto di un deadline non è una giustificazione accettabile per il bypass della sicurezza, rinforzata dalla leadership.
- **Mitigazione dei Processi:** Introdurre un processo di cambio di emergenza expedito (ma non saltato) con revisione obbligatoria post-implementazione per gestire l'urgenza genuina.