Contents

[1.4] Bypass della sicurezza per comodità del superiore

1. Definizione operativa: Il comportamento osservato in cui un dipendente disabilita o aggira un controllo di sicurezza (ad es., restrizioni USB, whitelist di applicazioni) perché un superiore diretto ha chiesto di farlo per completare un'attività più rapidamente.

2. Metrica principale e algoritmo:

- **Metrica:** Frequenza di bypass non autorizzato (UBF). Formula: `UBF = Conteggio(bypass_events) / Numero_di_dipendenti`.
- **Pseudocodice:**

  python

  ```
  def calculate_ubf(edr_logs, ticketing_system, start_date, end_date):
      # Interrogare EDR per gli eventi in cui i controlli di sicurezza sono stati modificati
      bypass_events = query_edr_events(
          action=['disable', 'bypass', 'override'],
          feature=['firewall', 'av', 'device_control'],
          date_range=(start_date, end_date)
      )

      # Arricchire con dati di ticketing per trovare eventi senza un ticket valido e pre-app
      unauthorized_events = []
      for event in bypass_events:
          # Verificare se un ticket è stato approvato per questa azione su questo asset
          related_tickets = query_tickets(asset_id=event.asset_id, action_requested=event.ac
          approved_ticket_exists = any(t.status == 'approved' for t in related_tickets)
          if not approved_ticket_exists:
              unauthorized_events.append(event)

      total_employees = get_active_employee_count()
      UBF = len(unauthorized_events) / total_employees
      return UBF
  ```

- **Soglia di avviso:** `UBF > 0.05` (ad es., più del 5% della forza lavoro ha eseguito un bypass non autorizzato nel periodo).

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

- **Log EDR/XDR** (ad es., CrowdStrike, Microsoft Defender): Eventi di modifica del controllo di sicurezza.
- **API del sistema di ticketing** (ad es., ServiceNow, Jira): Per fare riferimento incrociato alle modifiche con richieste di modifica approvate.
- **Database di gestione della configurazione (CMDB):** Per ottenere una mappatura accurata da asset a proprietario.

4. Protocollo di audit da umano a umano: Intervistare i manager del team e i loro rapporti diretti separatamente. Chiedi ai manager: "Hai mai chiesto al tuo team di bypassare una politica di sicurezza per rispettare una scadenza?" Chiedi ai dipendenti: "Il tuo manager ti ha mai chiesto di bypassare un controllo di sicurezza? Come lo hai gestito?" Cercare discrepanze e istanze ammesse.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Implementare controlli tecnici che richiedono l'autorizzazione di più persone (MFA/MofN) per le modifiche critiche delle politiche di sicurezza.
- **Mitigazione umana/organizzativa:** Formazione sulla leadership sui rischi operativi del bypass della sicurezza e supporto chiaro dal top management per i dipendenti che rifiutano ordini non etici.
- **Mitigazione dei processi:** Creare e promuovere un processo spedito e legittimo per richiedere eccezioni di sicurezza temporanee, riducendo la necessità percepita di bypass non autorizzati.