Contents

[4.2] Assunzione di Rischio Indotta da Rabbia

1. Definizione Operativa: Uno stato in cui la rabbia elevata porta il personale di sicurezza a aggirare i protocolli, prendere decisioni affrettate o impegnarsi in ritorsioni aggressive contro minacce percepite, aumentando così l'instabilità del sistema e creando nuove superfici di attacco.

2. Metrica Principale e Algoritmo:

- **Metrica:** Anger-Induced Action Ratio (AIAR). Formula: `AIAR = N_azioni_rapide_ad_alta_severità / N_azioni_totali_ad_alta_severità`.
- **Pseudocodice:**

  python

  ```
  def calculate_aiar(actions_log, user_id, time_window='1h'):
      """
      actions_log: Lista di dict con chiavi ['user', 'action_type', 'severity', 'timestamp',
      """
      # Filtrare le azioni ad alta severità dell'utente specifico (es. bloccare IP, mettere
      user_actions = [a for a in actions_log if a['user'] == user_id and a['severity'] == 'h

      # Definire una soglia per un'azione "rapida" (es. < 2 minuti dall'avviso all'azione su
      rapid_action_threshold = 120  # secondi

      # Contare le azioni eseguite più velocemente della soglia
      rapid_actions = [a for a in user_actions if a['time_to_execute'] < rapid_action_thresh

      # Calcolare il rapporto
      aiar = len(rapid_actions) / len(user_actions) if user_actions else 0
      return aiar
  ```

- **Soglia di Allarme:** `AIAR > 0.3` (Più del 30% delle azioni ad alta severità sono eseguite con deliberazione minima).

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

- **Log della Piattaforma SOAR:** (es. Splunk Phantom, Cortex XSOAR) API per recuperare log di esecuzione playbook, includendo `user`, `action_name`, `start_time`, `end_time` e tag di severità dall'avviso che innesca.
- **SIEM/Syslog:** Log di autenticazione e comandi da sistemi critici (es. log amministrativi del firewall, log della console EDR) per catturare azioni manuali fuori banda.

4. Protocollo di Audit Umano-su-Umano: Condurre un sondaggio anonimo e confidenziale con domande basate su scenari: "Ricevi un messaggio beffardo da un attaccante su un sistema critico. Qual è il tuo primo istinto?" e fornire risposte a scelta multipla. Seguire con interviste one-on-one dopo incidenti critici per discutere il processo decisionale e lo stato emotivo.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare un ritardo obbligatorio di "raffreddamento" per i playbook SOAR ad alto impatto, richiedendo l'approvazione di un secondo analista per l'esecuzione entro i primi 5 minuti.
- **Mitigazione Umana/Organizzativa:** Integrare tecniche di de-escalation e regolazione emotiva nella formazione sulla sicurezza. Stabilire un sistema di coppia per la revisione tra pari durante incidenti ad alta tensione.
- **Mitigazione del Processo:** Creare una checklist di revisione post-incidente che include esplicitamente l'analisi dello stato emotivo dei responder e il suo impatto sulle decisioni.