Contents

[2.10] Pressione di Coerenza Temporale

1. Definizione Operativa: La pressione psicologica di mantenere livelli di attività o output coerenti nel tempo, che può portare al personale della sicurezza di generare o agire su lavoro a basso valore semplicemente per apparire produttivo, piuttosto che concentrarsi su compiti di sicurezza strategici ad alta priorità.

2. Metrica Principale e Algoritmo:

- **Metrica:** Rapporto di Attività a Basso Valore (LVAR). Formula: `LVAR = N_low_value_actions / N_total_actions`.
- **Pseudocodice:**

  python

  ```
  def calculate_lvar(actions, low_value_indicators):
      """
      actions: Lista di oggetti azione (es. allarmi chiusi, ticket creati, report eseguiti).
      low_value_indicators: Una lista di pattern che significano lavoro a basso valore (es.
      """
      total_actions = len(actions)
      low_value_count = 0

      for action in actions:
          for indicator in low_value_indicators:
              # es. se action.description contiene "false positive" o action.type è "automat
              if indicator.matches(action):
                  low_value_count += 1
                  break # Contare l'azione solo una volta

      if total_actions > 0:
          LVAR = low_value_count / total_actions
      else:
          LVAR = 0

      return LVAR
  ```

- **Soglia di Allarme:** `LVAR > 0.6` (Oltre il 60% delle azioni di un analista o di un team sono classificate come a basso valore).

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

- **SIEM (Splunk):** Cercare `(status=closed AND (resolution="false_positive" OR resolution="duplicate"))` per utente.
- **Sistema di Ticketing (Jira):** API `worklog`. Analizzare il tempo speso su ticket taggati `"routine"`, `"maintenance"`.

- **Strumenti di Monitoraggio della Produttività:** Se disponibili, dati sull'utilizzo dell'applicazione (es. tempo nel client email vs. piattaforma di threat intelligence).

4. Protocollo di Audit da Persona a Persona: Condurre un audit dell'attività lavorativa con un campione di analisti: "Illustrami le tue azioni da ieri. Per ogni compito, chi era il beneficiario? Qual era l'esito della sicurezza?" Questo aiuta a distinguere tra lavoro generante valore e "busy work".

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Usare la metrica LVAR come indicatore chiave di prestazione (KPI) per l'efficienza del SOC, incoraggiando un focus sul valore rispetto al volume. Sviluppare automazione per gestire compiti di routine a basso valore.
- **Mitigazione Umana/Organizzativa:** Addestrare i manager a valutare le prestazioni in base all'impatto e ai risultati del lavoro, non solo al volume dell'attività. Proteggere gli analisti dalla pressione di essere costantemente "occupati".
- **Mitigazione dei Processi:** Implementare una revisione settimanale in cui gli analisti propongono un processo a basso valore da automatizzare o eliminare. Abilitarli a spendere il tempo liberato sulla threat hunting proattiva o sulla ricerca.