Contents

[6.6] Assunzioni di Dipendenza di Gruppo (baD)

1. Definizione Operativa: Basato sull'Assunzione Fondamentale Bioniana di Dipendenza (baD), questa è l'assunzione inconscia che un leader onnipotente, una tecnologia o un processo fornirà la sicurezza e risolverà tutti i problemi. Questo si manifesta come un'attesa passiva di istruzioni o output di strumenti e una mancanza di ricerca proattiva di minacce o analisi indipendente.

2. Metrica Principale & Algoritmo:

- **Metrica:** Rapporto di Lavoro Proattivo-a-Reattivo (PRR). Formula: `(Tempo speso su compiti proattivi) / (Tempo speso su compiti reattivi)`.
- **Pseudocodice:**

```
def calculate_prr(time_entries, proactive_categories):
    """
    time_entries: Lista di voci di registro del lavoro da uno strumento di tracciamento de
    proactive_categories: Lista di tag di progetto/compito ritenuti 'proattivi' (ad es. 'i
    """
    proactive_time = 0
    reactive_time = 0
    for entry in time_entries:
        if entry.category in proactive_categories:
            proactive_time += entry.hours
        else:
            reactive_time += entry.hours
    return proactive_time / reactive_time if reactive_time > 0 else float('inf')
```

- **Soglia di Allarme:** `PRR < 0.2` (Meno del 20% del tempo è speso in lavoro proattivo).

3. Fonti Dati Digitali (Input Algoritmo):

- **Software di Tracciamento del Tempo (ad es. Jira Tempo):** Campi: `author`, `timeSpentSeconds`, `category`, `project`.
- **SOAR/SIEM:** Può essere utilizzato come proxy contando gli avvisi gestiti (reattivi) rispetto alle query di ricerca eseguite (proattive).

4. Protocollo di Audit Umano-a-Umano: In colloqui uno-a-uno, chiedi agli analisti: "Quale percentuale del tuo tempo pensi di spendere in attesa di avvisi rispetto all'uscire a cercare minacce? Cosa ti impedisce di fare più lavoro proattivo? Senti di avere l'autorità e gli strumenti per investigare cose che trovi interessanti?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Dedicare e proteggere il "tempo di innovazione" nei piani di sprint. Implementare e promuovere piattaforme di ricerca di minacce facili da usare che autorizzano gli analisti a esplorare i dati senza necessità di esperienza SQL profonda.
- **Mitigazione Umana/Organizzativa:** La leadership deve incoraggiare attivamente e premiare il comportamento proattivo. Spostare le metriche di prestazione puramente reattive

(MTTR, ticket chiusi) per includere misure proattive (ad es. cacce completate, nuove regole di rilevamento scritte).

- **Mitigazione del Processo:** Programmare giorni di "ricerca" obbligatori e rotanti per ogni analista in cui la loro responsabilità principale non è gestire gli avvisi ma perseguire una domanda di ricerca proattiva.