Contents

[8.3] Modelli di Compulsione di Ripetizione

1. Definizione Operativa: La tendenza inconscia a ripetere gli errori di sicurezza passati o i fallimenti procedurali, spesso in circostanze simili (es. ora del giorno, tipo di avviso), nonostante la consapevolezza della procedura corretta.

2. Metrica Principale & Algoritmo:

- **Metrica:** Tasso di Errore Ripetuto (RER). Formula: `RER = Conteggio_Eventi_Errore_Ripetuto / Eventi_Errore_Totali`.
- **Pseudocodice:**

```
def calculate_rer(analyst_id, start_date, end_date):
    # 1. Interroga tutti gli eventi di errore registrati dai log di ticketing o SOAR
    all_errors = query_errors(analyst_id, start_date, end_date)  # es. ticket mal classif

    # 2. Raggruppa gli errori per tipo e contesto (es. stesso tipo di errore, ora simile,
    repeated_errors = 0
    for error in all_errors:
        # Trova errori passati simili dello stesso analista (es. ultimi 30 giorni)
        similar_past_errors = find_similar_errors(analyst_id, error, time_delta=30)
        if similar_past_errors:
            repeated_errors += 1

    # 3. Calcola il rapporto
    rer = repeated_errors / len(all_errors) if all_errors else 0
    return rer
```

- **Soglia di Allerta:** `RER > 0.3` (30% degli errori sono ripetizioni di un errore precedente).

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

- **Piattaforma SOAR:** Log di esecuzione playbook (campi `user`, `playbook_name`, `error_type`, `timestamp`, `asset_involved`).
- **Sistema di Ticketing:** API Jira/ServiceNow per i ticket contrassegnati come "classificati in modo non corretto" o "riaperti" a causa di errore dell'analista (campi `assignee`, `status`, `status_changes`, `comments`).
- **SIEM:** Log di azioni di override manuale che successivamente si sono rivelate scorrette.

4. Protocollo di Audit Umano-Umano: Revisiona i rapporti di incidente passati che coinvolgono l'individuo/team in un formato post-mortem senza colpe. Chiedi: "Abbiamo visto un problema simile prima. Cosa era diverso nel contesto questa volta? Cosa potremmo mettere in atto per rendere l'azione corretta più automatica o più facile da ricordare la prossima volta?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare una formazione "just-in-time" nei playbook

SOAR; se un utente fallisce una fase, il sistema offre immediatamente un modulo di micro-formazione su quell'azione specifica.

- **Mitigazione Umana/Organizzativa:** Integrare i post-mortem senza colpe nella procedura operativa standard per rompere il ciclo di vergogna e ripetizione.
- **Mitigazione del Processo:** Creare e mantenere una checklist di "errori comuni" per procedure specifiche ad alto rischio da consultare prima di finalizzare un'azione.