Contents

[8.6] Interferenza dei Meccanismi di Difesa

1. Definizione Operativa: L'uso inconscio di meccanismi di difesa psicologica (es. negazione, razionalizzazione, proiezione) che interferiscono attivamente con l'esecuzione dei doveri di sicurezza, come l'ignorare chiare prove di una violazione.

2. Metrica Principale & Algoritmo:

- **Metrica:** Rapporto di Rifiuto di Evidenza (EDR). Formula: `EDR = Conteggio_IoC_Alto_Fiducia_Rifiuta / IoC_Alto_Fiducia_Presentati_Totali`.
- **Pseudocodice:**

```
def calculate_edr(analyst_id, start_date, end_date):
    # 1. Interroga gli Indicatori di Compromissione (IoC) ad alta fiducia dalla threat int
    # (es. da Threat Intelligence Platform (TIP) o avviso SIEM)
    high_confidence_iocs = query_iocs(confidence_min=85, analyst_id, start_date, end_date)

    # 2. Interroga le azioni dell'analista su questi IoC (es. rifiutati, ignorati, esclus
    dismissed_iocs = 0
    for ioc in high_confidence_iocs:
        if get_ioc_status(ioc, analyst_id) in ['dismissed', 'ignored', 'false_positive']:
            dismissed_iocs += 1

    # 3. Calcola il rapporto
    edr = dismissed_iocs / len(high_confidence_iocs) if high_confidence_iocs else 0
    return edr
```

- **Soglia di Allerta:** `EDR > 0.1` (Rifiuto di più del 10% della threat intelligence ad alta fiducia).

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

- **Piattaforma Threat Intelligence (TIP):** API per ottenere IoC (campi `ioc_value`, `ioc_type`, `confidence_score`, `timestamp`).
- **SIEM/SOAR:** Log delle azioni dell'analista sugli avvisi contenenti questi IoC (campi `user`, `action`, `alert_id`, `ioc_value`).

4. Protocollo di Audit Umano-Umano: Presenta l'analista con un caso recente in cui ha rifiutato un IoC ad alta fiducia in un esercizio simulato. Usa una tecnica di intervista cognitiva: "Raccontami il tuo processo di pensiero quando hai visto questo indicatore. Quali altre possibilità hai considerato? Cosa avrebbe dovuto essere diverso perché tu escalassi questo?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare una regola di "secondo sguardo" nel SOAR: se un analista rifiuta un IoC ad alta fiducia, viene automaticamente messo in coda per una breve revisione da parte di un altro analista o da un senior.

- **Mitigazione Umana/Organizzativa:** Integrare la formazione sui bias cognitivi e sui meccanismi di difesa nei programmi di consapevolezza della sicurezza per gli analisti SOC.
- **Mitigazione del Processo:** Mantenere un "pre-mortem" per i principali closures di incidente, dove il team presume brevemente che la violazione *sia successa* e deve elencare quali prove avrebbe potuto perdere.