Contents

[6.10] Meccanismi di Difesa Collettivi

1. Definizione Operativa: L'uso inconsio a livello di organizzazione di difese psicologiche (ad es. negazione, razionalizzazione, proiezione) per evitare l'ansia associata alle minacce di sicurezza. Questo si manifesta come un sistematico sottovalutamento delle metriche di rischio, attribuzione dei breach esclusivamente a "stati nazione sofisticati" (proiezione), o credenza "non accadrà a noi" (negazione).

2. Metrica Principale & Algoritmo:

- **Metrica:** Rapporto di Razionalizzazione del Rischio (RRR). Formula: `(Numero di avvisi veri positivi confermati) / (Numero di avvisi inizialmente chiusi come 'falso positivo' o 'rischio accettato')`.
- **Pseudocodice:**

```
def calculate_rrr(alerts):
    true_positives = 0
    rationalized_alerts = 0
    for alert in alerts:
        if alert.final_verdict == "True Positive":
            true_positives += 1
        if alert.initial_closure_reason in ["False Positive", "Risk Accepted", "Not Applic
            rationalized_alerts += 1
    return true_positives / rationalized_alerts if rationalized_alerts > 0 else 0
```

- **Soglia di Allarme:** `RRR > 0.1` (Più del 10% degli avvisi inizialmente licenziati sono effettivamente veri positivi, indicando un modello di razionalizzazione/negazione).

3. Fonti Dati Digitali (Input Algoritmo):

- **SIEM/SOAR:** Coda di avvisi. Campi: `initial_closure_reason`, `final_verdict` (da investigazione successiva o scoperta da pentest), `severity`.

4. Protocollo di Audit Umano-a-Umano: In una riunione di revisione post-incidente senza colpa per un vero positivo mancato, focalizzati sulla decisione di triage iniziale. Chiedi: "Quale era il processo di pensiero dietro la chiusura iniziale di questo come un non-problema? C'era qualche pressione, conscia o inconscia, per far andare giù la coda di avvisi? Ci siamo convinti che andasse bene perché affrontarlo sarebbe stato difficile?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare un passo obbligatorio di revisione tra pari per la chiusura di qualsiasi avviso ad alta severità come falso positivo. Richiedere un secondo parere.
- **Mitigazione Umana/Organizzativa:** La leadership deve attivamente promuovere una cultura di sicurezza psicologica in cui parlare dei rischi e ammettere errori sia premiato, non punito. Discuti i bias cognitivi apertamente.

- **Mitigazione del Processo:** Istituire un processo di "audit di avvisi" regolare (ad es. trimestrale) in cui un campione di avvisi chiusi, specialmente quelli licenziati come FP, è riesaminato da un diverso team (ad es. Red Team) per convalidare le conclusioni.