Contents

[8.9] Modelli dell'Inconscio Collettivo

1. Definizione Operativa: La manifestazione di predisposizioni profondamente radicate e specifiche della specie all'interno della cultura di sicurezza di un'organizzazione, portando a reazioni universali ma spesso non ottimali alle minacce (es. la paura innata di serpenti/ragni che si traduce in un'enfasi eccessiva su certi tipi di malware).

2. Metrica Principale & Algoritmo:

- **Metrica:** Disparità nel Focus di Minaccia (TFD). Formula: `TFD = (Risorse_Allocate_a_Minacce_Archet / (Risorse_Allocate_a_Minacce_Effettivamente_Prevalenti)`.
- **Pseudocodice:**

```
def calculate_tfd(org_id, start_date, end_date):
    # 1. Definisci le minacce archetipiche e prevalenti (richiede input di esperti)
    archetypal_threats = ['ransomware', 'apt', 'zero-day', 'insider']
    prevalent_threats = get_top_threats_from_intel(org_id, 10)  # es. ['phishing', 'confi

    # 2. Misura le risorse allocate a ciascuno (es. spesa, strumenti, tempo dell'analista)
    # Questa è una metrica proxy complessa. Esempio: conteggio degli avvisi lavorati per
    arch_alerts = query_alert_count(archetypal_threats, start_date, end_date)
    prev_alerts = query_alert_count(prevalent_threats, start_date, end_date)

    # 3. Calcola un semplice rapporto
    total_arch = sum(arch_alerts.values())
    total_prev = sum(prev_alerts.values())
    tfd = total_arch / total_prev if total_prev > 0 else float('inf')
    return tfd
```

- **Soglia di Allerta:** `TFD > 2.0` (Spesa di più del doppio delle risorse su minacce archetipiche vs. prevalenti).

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

- **SIEM:** Log degli avvisi categorizzati per tipo di minaccia.
- **Sistema di Ticketing:** Tracciamento del tempo sugli incidenti per categoria.
- **Finanza/Procurement:** Dati sulla spesa per strumenti di sicurezza e servizi per categoria di minaccia.

4. Protocollo di Audit Umano-Umano: Condurre un workshop con la leadership di sicurezza. Presentare i dati sul panorama di minacce effettivo affrontato dall'organizzazione rispetto all'allocazione delle risorse. Chiedi: "Perché pensiamo che ci sia una disparità? Quali paure o convinzioni radicate potrebbero influenzare la nostra strategia di investimento?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Usa una piattaforma di threat intelligence basata su dati per segnalare regolarmente sulle *effettive* minacce principali per l'organizzazione e confrontarle

automaticamente con le allocazioni di controllo.

- **Mitigazione Umana/Organizzativa:** Assumi o consulta analisti di threat intelligence che possono fornire una visione obiettiva e basata su dati del panorama di minacce.
- **Mitigazione del Processo:** Integrare una revisione obbligatoria del "panorama di minacce" nel processo annuale di budgeting della sicurezza, richiedendo giustificazione per investimenti che si discostano significativamente dalle minacce effettivamente prevalenti.