Contents

[6.2] Fenomeni di Risky Shift

1. Definizione Operativa: Una tendenza per un team di sicurezza a prendere decisioni più rischiose come gruppo rispetto a quello che i singoli membri avrebbero fatto da soli. Questo si manifesta come un aumento misurabile nell'accettazione di azioni più rischiose (ad es., ritardare una patch critica, approvare una regola firewall borderline) durante le deliberazioni di gruppo rispetto alle posizioni pre-deliberazione individuali.

2. Metrica Principale & Algoritmo:

- **Metrica:** Coefficiente di Risky Shift (RSC). Formula: `Media(Punteggio Rischio Individuale) - Punteggio Rischio Finale di Gruppo`. Un RSC positivo indica uno spostamento verso un maggior rischio.
- **Pseudocodice:**

```
def calculate_risky_shift(individual_scores, group_score):
    """
    individual_scores: Lista di punteggi di rischio pre-riunione (1-10) di N membri del te
    group_score: Punteggio di rischio finale (1-10) concordato dal gruppo per quella decis
    """
    avg_individual_score = sum(individual_scores) / len(individual_scores)
    risky_shift_coefficient = avg_individual_score - group_score
    return risky_shift_coefficient
```

- **Soglia di Allarme:** `RSC > 1.5` (Uno spostamento coerente di più di 1.5 punti su una scala di 10 punti tra più decisioni indica un modello significativo).

3. Fonti Dati Digitali (Input Algoritmo):

- **Sistemi di Ticketing (Jira, ServiceNow):** Ticket per cambiamenti (ad es. ticket CHG per patching, regole firewall). Campi: `created_by`, `created_date`, `risk_assessment_score` (input individuale pre-riunione), `final_risk_score`, `approvers`.
- **Piattaforme di Collaborazione (Slack, Teams API):** Metadati da canali dedicati alle discussioni sui rischi (ad es. `#security-risk-board`). Dati: `thread_id`, `participants`, `message_count` (per identificare l'intensità della deliberazione).

4. Protocollo di Audit Umano-a-Umano: Condurre un workshop facilitato che presenta 3-5 decisioni di sicurezza storiche recenti. Per primo, fai punteggiare privatamente e anonimamente ogni partecipante al rischio che avrebbe assegnato (1-10). Quindi, facilita una discussione su quale fosse il punteggio finale e perché. Confronta il punteggio anonimo medio con il punteggio finale storico per calcolare il RSC in un'impostazione controllata.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare una funzione "pre-meeting sentiment" nella piattaforma di gestione del rischio in cui i singoli devono inviare il loro punteggio di rischio prima di una riunione di revisione di gruppo.

- **Mitigazione Umana/Organizzativa:** Addestrare i facilitatori di riunioni sul fenomeno di risky shift e tecniche per mitigarlo, come invitare un "avvocato del diavolo" designato o utilizzare strumenti di sondaggio anonimo all'inizio delle discussioni.
- **Mitigazione del Processo:** Integrare un passo obbligatorio nel flusso di lavoro di accettazione del rischio che richiede di documentare deviazioni significative (`RSC > 1.5`) dal punteggio di rischio individuale medio pre-riunione, inclusa una giustificazione.