Contents

[3.8] Conformità alle Norme Non Sicure

1. Definizione Operativa: La tendenza degli individui ad allineare il loro comportamento al comportamento normativo percepito del loro gruppo, anche se quel comportamento è non sicuro, perché deviare dal gruppo comporta un costo sociale.

2. Metrica Principale e Algoritmo:

- **Metrica: Indice di Deviazione dalle Norme (NDI)**. Formula: `NDI = 1 - (U_conforme / U_totale)`, calcolato per un gruppo di pari. Un NDI elevato indica una norma di non conformità nel gruppo.
- **Pseudocodice:**

  python

```
# Simile a DPP (3.3), ma focalizzato sulla conformità a una specifica policy nota.
def calculate_ndi(logs, policy_rules, peer_groups):
    """
    policy_rules: Un set di regole che definiscono le azioni conformi vs. non conformi.
    """
    ndi_results = {}
    for group, users in peer_groups.items():
        non_compliant_users = 0
        for user in users:
            user_actions = get_actions(logs, user)
            # Verifica se l'utente ha violato una delle regole di policy definite
            if not is_compliant(user_actions, policy_rules):
                non_compliant_users += 1

        NDI = non_compliant_users / len(users)
        ndi_results[group] = NDI
    return ndi_results
```

- **Soglia di Allerta:** `NDI > 0.5` (Oltre il 50% di un gruppo è non conforme a una policy, indicando una forte norma non sicura).

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

- **Strumenti di Scansione della Conformità (ad esempio, Qualys PC, Azure Policy, AWS Config):** Segnalano direttamente lo stato di conformità per le risorse e gli utenti rispetto alle policy. Campi: `user/resource_id`, `compliance_state`, `policy_id`.
- **Vari Log (come in 3.3):** Per dedurre il comportamento di conformità.

4. Protocollo di Audit Umano-Umano: Usa interviste di gruppo o focus group. Presenta i dati quantitativi (NDI) al gruppo e chiedi: "I dati suggeriscono che seguire [X policy] non è la norma qui. Perché pensi che sia così? Quali sono le barriere alla conformità? Cosa renderebbe più facile per tutti seguire questa regola?".

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Dove possibile, utilizza l'enforcing tecnico (ad esempio, forzare la crittografia, bloccare software non autorizzato) rispetto alle policy procedurali per rimuovere la scelta di essere non conforme.
- **Mitigazione Umana/Organizzativa:** Identifica e lavora con gli influencer all'interno del gruppo per modellare e promuovere il comportamento sicuro desiderato, spostando la norma percepita.
- **Mitigazione del Processo:** Rivedi la policy problematica. È eccessivamente complicata? Lavora con il gruppo per semplificare il processo mantenendo gli obiettivi di sicurezza, aumentando l'adesione.