Contents

[3.3] Manipolazione della Prova Sociale

1. Definizione Operativa: La tendenza degli individui ad adottare le azioni o i comportamenti di un gruppo, anche se quei comportamenti violano le policy di sicurezza, perché percepiscono il comportamento come corretto o normale in base alla sua prevalenza.

2. Metrica Principale e Algoritmo:

- **Metrica: Prevalenza della Pratica Deviante (DPP)**. Formula: `DPP = U_deviante / U_totale`, dove `U_deviante` è il numero di utenti che si impegnano in una specifica pratica non sicura e `U_totale` è il numero totale di utenti in un gruppo di pari.
- **Pseudocodice:**

  python

```
def calculate_dpp(logs, peer_groups, insecure_action_patterns):
    """
    logs: Log consolidati da varie fonti che mostrano le azioni degli utenti.
    peer_groups: Un mapping degli utenti ai loro team/dipartimenti.
    insecure_action_patterns: Un elenco di regex o pattern che definiscono il comportament
    """
    dpp_results = {}
    for group, users in peer_groups.items():
        total_users = len(users)
        deviant_users = set()

        for user in users:
            user_actions = get_actions(logs, user, period='30d')
            # Verifica se l'utente ha effettuato una delle azioni non sicure definite
            if any(action_matches_pattern(action, insecure_action_patterns) for action in
                deviant_users.add(user)

        dpp = len(deviant_users) / total_users
        dpp_results[group] = dpp
    return dpp_results
```

- **Soglia di Allerta:** `DPP > 0.4` (Oltre il 40% di un gruppo di pari si impegna nella pratica).

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

- **Log Proxy/Firewall (ad esempio, Zscaler, Palo Alto):** Per rilevare visite a cloud storage o siti web non autorizzati. Campi: `user`, `url`, `category`.
- **Log Endpoint DLP (ad esempio, Microsoft Purview, Symantec DLP):** Per rilevare trasferimenti di file non autorizzati. Campi: `user`, `file_name`, `action` (ad esempio, `upload`, `copy`), `destination`.
- **Log Cloud Access Security Broker (CASB) (ad esempio, Netskope, McAfee MVISION):** Per rilevare l'utilizzo di shadow IT. Campi: `user`, `app_name`, `activity`.

4. Protocollo di Audit Umano-Umano: Distribuisci un sondaggio anonimo ai dipartimenti: "Approssimativamente quale percentuale dei tuoi colleghi pensi che utilizzi [X metodo non sicuro, ad esempio email personale] per condividere i file di lavoro?" Confronta la percentuale percepita con la metrica DPP calcolata dai log. Una correlazione elevata conferma che il bias è attivo.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Utilizza strumenti CASB o DLP per bloccare automaticamente gli upload a servizi non autorizzati e reindirizzare gli utenti all'alternativa sicura approvata dall'organizzazione.
- **Mitigazione Umana/Organizzativa:** I leader e i campioni della sicurezza dovrebbero pubblicamente promuovere e riconoscere i comportamenti di sicurezza corretti per fornire una prova sociale positiva.
- **Mitigazione del Processo:** Documenta chiaramente e comunica la *effettiva* prevalenza del comportamento sicuro (ad esempio, "Il 95% del team di finanza utilizza correttamente lo strumento di condivisione sicura approvato") per contrastare le percezioni false delle norme devianti.