Contents

[4.9] Avventatezza Indotta dall'Euforia

1. Definizione Operativa: Uno stato di eccessiva fiducia e eccitazione, spesso seguito da un successo, che porta a sottovalutare i rischi, saltare i passaggi di verifica e un generale rilassamento della vigilanza della sicurezza.

2. Metrica Principale e Algoritmo:

- **Metrica:** Post-Success Verification Bypass Rate (PSVBR). Formula: `PSVBR = N_azioni_non_verificate_` `/ N_azioni_totali_post_successo`.
- **Pseudocodice:**

  python

```
def calculate_psvbr(action_log, success_events, verification_window='1h'):
    """
    success_events: Una lista di risoluzioni di incidenti importanti o altri marcatori di
    """
    # Per ogni evento di successo, guardare le azioni nella finestra di tempo seguente
    total_actions_post_success = 0
    unverified_actions = 0

    for success in success_events:
        post_success_actions = get_actions_in_window(success.time, verification_window)
        total_actions_post_success += len(post_success_actions)

        # Verificare se le azioni mancavano di verifica (es. nessun MFA, nessun log di rev
        for action in post_success_actions:
            if not action['was_verified']: # Questo flag deve essere definito nei log
                unverified_actions += 1

    psvbr = unverified_actions / total_actions_post_success if total_actions_post_success
    return psvbr
```

- **Soglia di Allarme:** `PSVBR > 0.4` (Un aumento significativo delle azioni non verificate dopo un evento di successo).

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

- **Log SOAR/SIEM:** Per definire "eventi di successo" (es. incidente chiuso con "risolto").
- **Log di Autenticazione (es. Okta):** Per verificare MFA su azioni sensibili.
- **Controllo Versione (Git):** Per verificare le revisioni del codice prima dei commit post-successo.

4. Protocollo di Audit Umano-su-Umano: Nelle revisioni post-incidente per risoluzioni riuscite, chiedere esplicitamente: "Dopo che la minaccia è stata contenuta, quali sono stati i passaggi successivi? Qualcuno ha sentito un senso di sollievo o eccitazione che potrebbe aver portato ad affrettarsi?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Imporre regole di "cool-down" nei playbook SOAR che mantengono i controlli di sicurezza anche dopo che uno stato di successo è dichiarato.
- **Mitigazione Umana/Organizzativa:** La leadership e i responsabili dei team dovrebbero modellare e comunicare l'importanza di mantenere la procedura attraverso tutte le fasi di un incidente.
- **Mitigazione del Processo:** Integrare una "Post-Success Checklist" obbligatoria nei playbook di risposta agli incidenti, richiedendo la verifica dei passaggi chiave prima di dichiarare la risoluzione completa.