Contents

[8.7] Confusione di Equazione Simbolica

1. Definizione Operativa: Il mancato inconscio di distinguere tra un simbolo di sicurezza (es. un certificato di conformità, il logo di un fornitore) e la realtà di sicurezza effettiva che rappresenta, portando a un falso senso di sicurezza.

2. Metrica Principale & Algoritmo:

- **Metrica:** Divario Simbolo vs Realtà (SRG). Formula: `SRG = (Punteggio_Conformità - Punteggio_Sicurezza_Tecnica)`
- **Pseudocodice:**

```
def calculate_srg(asset_id):
    # 1. Ottieni lo stato di conformità (il simbolo) - es. certificato PCI DSS
    compliance_score = get_compliance_score(asset_id)  # es. 1 se certificato, 0 se no

    # 2. Ottieni il punteggio di sicurezza tecnica effettiva (la realtà) - da scan di vul
    vuln_score = get_vuln_density(asset_id)
    config_score = get_config_hardening_score(asset_id)
    technical_score = normalize(1 - (vuln_score + config_score))  # Combina e normalizza

    # 3. Calcola il divario
    srg = compliance_score - technical_score
    return srg
```

- **Soglia di Allerta:** `SRG > 0.5` (Un punteggio di conformità elevato è abbinato a un punteggio di sicurezza tecnica significativamente basso).

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

- **Piattaforma GRC:** API ServiceNow GRC/RSAM (campi `asset_id`, `compliance_status`).
- **Gestione delle Vulnerabilità:** API Qualys/Tenable (campi `asset_id`, `vuln_count`, `severity`).
- **Gestione della Configurazione:** Risultati AWS Config/Azure Policy/Chef Inspec (campi `asset_id`, `config_compliance_score`).

4. Protocollo di Audit Umano-Umano: Intervista i proprietari di asset e il personale di sicurezza: "Questo sistema è [CONFORME]. Significa che è sicuro? Puoi descrivere i controlli di sicurezza specifici che lo proteggono adesso, oltre a quello che è stato controllato per la conformità?" L'obiettivo è vedere se riescono ad articolare la realtà pratica oltre la certificazione simbolica.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Costruire una dashboard che correlati automaticamente lo stato di conformità con i punteggi di sicurezza tecnica live (vulnerabilità, configurazioni) e avvisa su grandi divari.
- **Mitigazione Umana/Organizzativa:** Addestrare i valutatori dei rischi e gli architetti a valutare i meriti di sicurezza tecnica indipendentemente dalle certificazioni di conformità.

- **Mitigazione del Processo:** Integrare i test di sicurezza tecnica (penetration testing, red teaming) come passaggio obbligatorio *dopo* il conseguimento della certificazione di conformità per i sistemi critici.