Contents

[4.4] Attaccamento ai Sistemi Legacy

1. Definizione Operativa: Una preferenza emotiva per sistemi legacy familiari che porta all'evitamento della migrazione, all'esclusione dei loro rischi di sicurezza e alla razionalizzazione del mantenimento di software e hardware obsoleti.

2. Metrica Principale e Algoritmo:

- **Metrica:** Legacy Risk Acceptance Score (LRAS). Formula: `LRAS = (N_asset_legacy * CVSS_medio) / N_asset_totali`.
- **Pseudocodice:**

  python

```
def calculate_lras(cmdb_assets, vuln_scans):
    """
    cmdb_assets: Lista da CMDB con ['asset_id', 'name', 'os', 'is_legacy' (bool)]
    vuln_scans: Lista dallo scanner di vulnerabilità con ['asset_id', 'cve_id', 'cvss_scor
    """
    # Ottenere tutti gli asset contrassegnati come legacy (es. OS EOL come Win7, software
    legacy_assets = [a for a in cmdb_assets if a['is_legacy']]
    total_assets = len(cmdb_assets)

    # Per ogni asset legacy, trovare le sue vulnerabilità aperte e calcolare un CVSS medio
    total_legacy_risk = 0
    for asset in legacy_assets:
        asset_vulns = [v for v in vuln_scans if v['asset_id'] == asset['asset_id'] and v['
        avg_cvss = sum([v['cvss_score'] for v in asset_vulns]) / len(asset_vulns) if asset
        total_legacy_risk += avg_cvss

    # Calcolare il punteggio generale
    lras = (len(legacy_assets) * (total_legacy_risk / len(legacy_assets))) / total_assets
    return lras
```

- **Soglia di Allarme:** `LRAS > 0.25` AND `len(legacy_assets) > 0` (Una parte significativa della base di asset è legacy e presenta alto rischio).

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

- **CMDB (ServiceNow/AWS Tags):** Query API REST per ottenere elenco di asset con un tag personalizzato `is_legacy` o basato su `os_version`.
- **Gestione delle Vulnerabilità (Qualys/Tenable):** API per recuperare tutte le vulnerabilità aperte Alto/Critico, i loro punteggi CVSS e gli asset interessati.

4. Protocollo di Audit Umano-su-Umano: Intervistare gestori IT e di sicurezza: "Qual è il piano per la disattivazione di [specifico sistema legacy]? Quali sono le barriere percepite?" Rivedere i charter dei progetti e i budget per prove di progetti di migrazione legacy che vengono rinviati o deprioritizzati.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Imporre una rigorosa segmentazione di rete e microsegmentazione per tutti i sistemi legacy identificati per contenere potenziali violazioni.
- **Mitigazione Umana/Organizzativa:** Eseguire workshop per mappare le dipendenze emotive e pratiche dai sistemi legacy, creando una visione condivisa e oggettiva del rischio.
- **Mitigazione del Processo:** Integrare una "Legacy System Impact Assessment" obbligatoria nel processo di accettazione del rischio, richiedendo l'approvazione del CISO per qualsiasi eccezione.