Contents

[6.8] Fantasie di Speranza di Pairing (baP)

1. Definizione Operativa: Basato sull'Assunzione Fondamentale Bioniana Pairing (baP), questa è la credenza inconscia del gruppo che un evento futuro, una tecnologia o un'assunzione ("il proiettile d'argento") risolverà tutti i problemi di sicurezza attuali. Questo si manifesta come ricerca continua e acquisizione di nuovi strumenti senza implementare o padroneggiare pienamente quelli esistenti, e un ritardo nell'affrontare i problemi attuali.

2. Metrica Principale & Algoritmo:

- **Metrica:** Punteggio di Utilizzo dello Strumento (TUS). Formula: `(Numero di caratteristiche attivamente utilizzate di uno strumento) / (Numero totale di caratteristiche disponibili)`.
- **Pseudocodice:**

```
def calculate_tus(tool_audit_list):
    """
    tool_audit_list: Una lista per ogni strumento, con un conteggio delle caratteristiche
    """
    total_available_features = 0
    total_used_features = 0
    for tool in tool_audit_list:
        total_available_features += tool.total_features
        total_used_features += tool.used_features
    return total_used_features / total_available_features
```

- **Soglia di Allarme:** `TUS < 0.4` (Meno del 40% delle capacità dello strumento acquistato sono utilizzate).

3. Fonti Dati Digitali (Input Algoritmo):

- **API SIEM/SOAR/EDR:** Log di audit e endpoint di configurazione per verificare le caratteristiche abilitate rispetto alle caratteristiche disponibili.
- **CMDB:** Elenco degli strumenti di sicurezza posseduti e dei loro livelli di licenza (che spesso si mappano alle caratteristiche).
- **Strumenti di Gestione del Progetto:** Ticket relativi alla valutazione di nuovi strumenti rispetto ai ticket per il miglioramento dell'uso degli strumenti esistenti.

4. Protocollo di Audit Umano-a-Umano: In una riunione strategica, chiedi: "Nell'ultimo anno, cosa ci ha dato il più grande miglioramento di sicurezza: uno strumento nuovo che abbiamo acquistato, o un nuovo processo o caso d'uso che abbiamo implementato con uno strumento esistente?" Cataloga tutti i principali strumenti e chiedi al team di valutare onestamente il loro livello di utilizzo.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Prima di qualsiasi valutazione di nuovo strumento, richiedere una revisione formale della toolstack esistente per identificare se il bisogno può

essere soddisfatto migliorando l'uso delle capacità attuali.

- **Mitigazione Umana/Organizzativa:** Spostare la misura del successo per gli ingegneri di sicurezza da "valutati X nuovi strumenti" a "sbloccate Y nuove caratteristiche nella nostra piattaforma esistente".
- **Mitigazione del Processo:** Implementare un "modello di maturità di capacità" per ogni strumento principale. Definire cosa significa "utilizzo pieno" e creare una tabella di marcia per arrivarci prima di approvare nuovi acquisti.