Contents

[5.9] Errori indotti dalla complessità 1

[5.9] Errori indotti dalla complessità

1. Definizione operativa: Errori commessi non a causa di una mancanza di conoscenza, ma a causa della complessità schiacciante degli strumenti, delle procedure o dell'attacco stesso, portando a configurazione scorretta, analisi difettosa o passi persi.

2. Metrica principale e algoritmo:

- **Metrica:** Indice di deviazione della procedura (PDI). Formula: `PDI = (Numero di passi saltati o fuori ordine in un processo documentato) / (Numero totale di passi nel processo)`. Misurato confrontando le azioni dell'analista a un playbook noto.
- **Pseudocodice:**

```
def calculate_pdi(analyst_actions, playbook_steps):
    # analyst_actions: lista ordinata di azioni intraprese (ad es. dal log di audit SOAR)
    # playbook_steps: lista ordinata di passaggi attesi

    # Questo è un complesso problema di allineamento di sequenza. Un proxy più semplice è
    skipped_steps = set(playbook_steps) - set(analyst_actions)
    return len(skipped_steps) / len(playbook_steps)
```

- **Soglia di avviso:** `PDI > 0.2` (L'analista sta saltando più del 20% dei passi consigliati in un playbook standard).

3. Fonti di dati digitali (Input dell'algoritmo):

- **Piattaforma SOAR:** La fonte ideale se i playbook sono automatizzati e i passi sono registrati. SOAR può direttamente registrare gli eventi `playbook_step_skipped` o `step_completed`.
- **Audit manuali:** Per i playbook non automatizzati, ciò richiede una revisione manuale delle note di investigazione rispetto a una lista di controllo.

4. Protocollo di audit uomo-uomo: Condurre un esercizio da tavolo con uno scenario complesso. Avere l'analista verbalizzare le loro azioni mentre un auditor li controlla rispetto al playbook ufficiale di risposta agli incidenti. Annotare quali passi sono saltati, fatti fuori ordine o fatti in modo errato a causa della confusione.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Dove possibile, automatizzare i passaggi più complessi e soggetti a errori di un playbook all'interno di un SOAR, riducendo il carico cognitivo sull'analista.
- **Mitigazione umana/organizzativa:** Fornire formazione regolare su procedure complesse usando simulazioni realistiche, focalizzandosi sul *perché* dietro ogni passaggio per aiutare la comprensione e il ricordo.
- **Mitigazione dei processi:** Semplificare e snellire i playbook. Suddividere le procedure complesse in sub-procedure più piccole e gestibili con chiari checkpoint.