Contents

[5.10] Confusione del modello mentale

1. Definizione operativa: Una situazione in cui un analista mantiene una comprensione interna scorretta o incompleta di come funziona un sistema, uno strumento o un attacco, portandoli a interpretare male i dati e trarre conclusioni erronee.

2. Metrica principale e algoritmo:

- **Metrica:** Tasso di invalidazione dell'ipotesi (HIR). Formula: `HIR = (Numero di volte che l'ipotesi iniziale di un analista su un avviso è provata errata dalle prove successive) / (Numero totale di avvisi in cui ha formato un'ipotesi)`.
- **Pseudocodice:**

```
def calculate_hir(tickets, analyst_id):
    # Ottenere i ticket dove l'analista era l'investigatore principale
    analyst_tickets = get_tickets(primary_analyst=analyst_id, has_initial_assessment=True)
    invalidation_count = 0

    for ticket in analyst_tickets:
        initial_hypothesis = ticket.initial_assessment  # ad es. "Questo è un FP"
        final_verdict = ticket.final_verdict           # ad es. "Positivo vero - Malware"
        if initial_hypothesis != final_verdict:
            invalidation_count += 1

    return invalidation_count / len(analyst_tickets)
```

- **Soglia di avviso:** `HIR > 0.4` (L'ipotesi iniziale dell'analista è errata più del 40% delle volte, indicando un modello mentale difettoso).

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

- **Sistema Ticketing (Jira/ServiceNow):** Richiede campi personalizzati `Initial Hypothesis` e `Final Verdict` da compilare dagli analisti e convalidati da un analista senior o da uno strumento automatizzato.

4. Protocollo di audit uomo-uomo: Durante una retrospettiva di incidenti, chiedere all'analista: "Percorri il tuo processo di pensiero quando hai visto questo avviso per la prima volta. Cosa pensavi stesse succedendo e perché?" Quindi confronta questo con le prove. Indaga per malintesi sulla funzionalità degli strumenti (ad es. "Pensavo che il firewall avrebbe bloccato questo") o sulle tecniche di attacco.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Implementare un wiki di "modello mentale" che documenti i sistemi comuni e gli attacchi, affrontando esplicitamente i malintesi frequenti.
- **Mitigazione umana/organizzativa:** Istituire un robusto programma di mentoring dove gli analisti junior regolarmente rivedono i casi con analisti senior per correggere e affinare i loro modelli mentali.

- **Mitigazione dei processi:** Creare una cultura di “post-mortem senza colpe” che si concentri sull’identificazione e la correzione dei modelli mentali difettosi piuttosto che l’assegnazione di colpa per gli errori.