Contents

[5.8] Effetti del residuo di attenzione

1. Definizione operativa: L'impatto negativo sulle prestazioni nel passaggio da Compito A a Compito B, dove le risorse cognitive sono ancora parzialmente occupate dal compito precedente, riducendo la concentrazione e l'efficacia sul nuovo compito.

2. Metrica principale e algoritmo:

- **Metrica:** Tempo per focalizzazione (TTF). Formula: `TTF = (Tempo tra l'apertura iniziale di un nuovo avviso e l'esecuzione della prima azione di investigazione significativa e unica su di esso)`. Un TTF elevato suggerisce residuo di attenzione da un compito precedente.
- **Pseudocodice:**

```
def calculate_ttf(events, alert_id):
    # Ottenere gli eventi per questo avviso, ordinati per tempo
    alert_events = get_events_for_alert(alert_id)
    open_time = None
    first_action_time = None

    for event in alert_events:
        if event.action == 'open' or event.action == 'assign':
            open_time = event.timestamp
        # Definisci cosa costituisce un'"azione di investigazione significativa"
        if open_time and event.action in ['query_edr', 'run_yara', 'check_dns']:
            first_action_time = event.timestamp
            break

    if open_time and first_action_time:
        return (first_action_time - open_time).total_seconds() / 60  # Restituisci il temp
    else:
        return None  # Dati incompleti
```

- **Soglia di avviso:** `TTF > 15 (minuti)` per avvisi ad alta severità. L'analista impiega più di 15 minuti per iniziare il lavoro significativo su un avviso critico.

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

- **Log di audit SOAR/SIEM:** Per ottenere il timestamp preciso quando un avviso è stato assegnato/aperto da un analista.
- **Vari log di audit degli strumenti (EDR, DNS, ecc.):** Per ottenere il timestamp della prima azione di investigazione eseguita sull'avviso, che può verificarsi al di fuori del SIEM.

4. Protocollo di audit uomo-uomo: Chiedere a un analista di descrivere cosa fa nei primi 5 minuti dopo aver preso un nuovo ticket ad alta severità. Una risposta vaga o esitante può indicare la mancanza di un protocollo chiaro, esacerbando il residuo di attenzione. Confronta questo con il loro TTF misurato.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Implementare un protocollo di "handover" nel sistema di ticketing dove l'analista precedente deve lasciare un breve riassunto strutturato del contesto dell'avviso per ridurre il carico cognitivo sull'analista successivo.
- **Mitigazione umana/organizzativa:** Incoraggiare gli analisti a eseguire un breve "rituale di chiusura" (ad es. scrivere una frase sui prossimi passi) prima di passare a un altro compito per compartimentalizzare mentalmente il lavoro precedente.
- **Mitigazione dei processi:** Standardizzare i primi 5 passi per investigare qualsiasi nuovo avviso (ad es. 1. Controllare EDR, 2. Arricchire IP, 3. Controllare i log di autenticazione). Ciò riduce il carico decisionale quando si inizia un nuovo compito.