Contents

[5.5] Vulnerabilità di cambio di contesto

1. Definizione operativa: Gli errori di sicurezza specifici che si verificano nel periodo di transizione *tra* compiti, dove le risorse cognitive si riallocano, portando a dettagli persi o scorciatoie procedurali. Questo è il *risultato* del degrado descritto in 5.4.

2. Metrica principale e algoritmo:

- **Metrica:** Tasso di errore post-cambio (PSER). Formula: `PSER = (Numero di errori commessi su un avviso entro M minuti dal cambio da un avviso precedente) / (Numero totale di avvisi elaborati dopo un cambio)`.
- **Pseudocodice:**

```
def calculate_pser(events, analyst_id, time_window_minutes=5):
    # Ottenere il log eventi dell'analista, ordinato per tempo
    analyst_events = get_events(assigned_to=analyst_id, sort='timestamp')
    error_count = 0
    total_switched_alerts = 0

    for i in range(1, len(analyst_events)):
        prev_event = analyst_events[i-1]
        current_event = analyst_events[i]

        # Verificare se l'analista è passato a un avviso diverso
        if current_event.alert_id != prev_event.alert_id:
            total_switched_alerts += 1
            # Verificare un errore (ad es. classificazione errata) sul nuovo avviso entro
            subsequent_events = get_events_for_alert(current_event.alert_id, within_minute
            if any(e.action == 'misclassified' for e in subsequent_events):
                error_count += 1

    return error_count / total_switched_alerts if total_switched_alerts > 0 else 0
```

- **Soglia di avviso:** `PSER > 0.15` (Più del 15% dei cambi di contesto portano a un errore misurabile).

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

- **Log di audit SOAR/SIEM:** Come in 5.4, per tracciare i cambi di compito.
- **Sistema Ticketing & Rapporti di incidenti:** Per identificare gli errori (ad es. ticket riapertini a causa di classificazione iniziale errata, report post-mortem che citano errori dell'analista). Ciò richiede un sistema di tagging "errore" definito.

4. Protocollo di audit uomo-uomo: Durante una riunione del team, eseguire una retrospettiva su un incidente recente che ha coinvolto un passo falso iniziale. Chiedere al team: "Cosa stava succedendo appena prima che questo avviso arrivasse? Stava qualcuno lavorando su qualcos'altro di complesso?" Ciò può aiutare a identificare se un cambio di contesto è stato un fattore contribuente.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Progettare i playbook SOAR per includere una "lista di controllo di contesto" obbligatoria che appare quando un analista apre per la prima volta un avviso ad alta severità, forzando un momento di concentrazione.
- **Mitigazione umana/organizzativa:** Incoraggiare un rituale di "pausa di 30 secondi" per gli analisti prima di iniziare un'investigazione nuova per reimpostare mentalmente.
- **Mitigazione dei processi:** Istituire un processo di peer-review per la classificazione iniziale di tutti gli avvisi ad alta severità per catturare gli errori introdotti dal rapido cambio di contesto.