Contents

[5.4] Degradazione del multitasking

1. Definizione operativa: Il costo delle prestazioni e l'aumento del tasso di errore associati al cambio frequente tra diversi compiti di sicurezza (ad es. monitoraggio, investigazione, reporting), che impedisce una concentrazione profonda su alcun singolo compito.

2. Metrica principale e algoritmo:

- **Metrica:** Frequenza di cambio di contesto (CSF). Formula: `CSF = (Numero di ID avviso/ticket distinti su cui ha lavorato un analista) / (Tempo totale del turno in ore)`.
- **Pseudocodice:**

```
def calculate_csf(events, analyst_id, shift_start, shift_end):
    # Ottenere tutti gli eventi per l'analista durante il turno
    shift_events = get_events(assigned_to=analyst_id, start_time=shift_start, end_time=shi

    # Estrarre gli ID univoci di avviso/ticket con cui è stata effettuata un'interazione
    unique_worked_items = set()
    for event in shift_events:
        if event.action in ['acknowledge', 'investigate', 'update', 'close']:
            unique_worked_items.add(event.alert_id)

    shift_duration_hours = (shift_end - shift_start).total_seconds() / 3600

    return len(unique_worked_items) / shift_duration_hours
```

- **Soglia di avviso:** `CSF > 8` (L'analista passa il contesto più di 8 volte all'ora in media).

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

- **Log di audit SIEM/SOAR:** La fonte definitiva per le interazioni utente. Query dei log per `user=$analyst_id` e filtrare per azioni come `alert_acknowledge`, `ticket_update`, `investigation_start`. Campi: `timestamp`, `user`, `action`, `object_id`.

4. Protocollo di audit uomo-uomo: Intervistare l'analista: "Quanti incidenti o compiti diversi stai generalmente giocolando contemporaneamente?" e "Con che frequenza sei interrotto da nuovi avvisi, chat o chiamate mentre lavori su qualcos'altro?" Numeri alti e frustrati si correlano con CSF alto.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Configurare le code di avvisi per essere assegnate ai ruoli, non ai singoli, permettendo a un analista di concentrarsi su un'investigazione approfondita mentre altri gestiscono il triage in arrivo.
- **Mitigazione umana/organizzativa:** Implementare "focus block" nel programma del turno dove gli analisti non ricevono nuovi avvisi e possono lavorare ininterrottamente su investigazioni complesse.

- **Mitigazione dei processi:** Creare un protocollo del team dove le interruzioni non urgenti (messaggi Slack, domande) vengono indirizzate a un ruolo “help” dedicato o a un canale invece di direttamente agli analisti in lavoro profondo.