Contents

[5.3] Paralisi da sovraccarico informativo

1. Definizione operativa: Uno stato cognitivo in cui un analista è presentato con un tale volume di dati o avvisi da non riuscire a elaborare efficacemente nessuno di essi, portando a risposte ritardate o assenti.

2. Metrica principale e algoritmo:

- **Metrica:** Rapporto volume avvisi-risposta (AVRR). Formula: `AVRR = (Numero di avvisi riconosciuti o chiusi) / (Numero totale di avvisi presentati) per analista per ora.`.
- **Pseudocodice:**

```
def calculate_avrr(events, analyst_id, time_window_hours=1):
    # Ottenere tutti gli eventi per l'analista e la finestra temporale
    start_time = now() - timedelta(hours=time_window_hours)
    analyst_events = get_events(assigned_to=analyst_id, start_time=start_time)

    total_alerts = len(analyst_events)
    if total_alerts == 0:
        return 1.0  # Nessun avviso è il 100% di elaborazione

    # Contare gli avvisi su cui è stata agita un'azione (riconosciuti o chiusi)
    acted_alerts = len([e for e in analyst_events if e.status in ['in_progress', 'closed']

    return acted_alerts / total_alerts
```

- **Soglia di avviso:** `AVRR < 0.3` (L'analista agisce su meno del 30% degli avvisi che riceve in un'ora).

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

- **SIEM (Splunk/Elasticsearch):** Fonte primaria per il volume di eventi grezzo. Query: `index=sec_events assigned_to=$analyst_id` su una finestra temporale mobile.
- **Sistema SOAR/Ticketing:** Per determinare lo stato (`new`, `in_progress`, `closed`) di ogni avviso presentato all'analista.

4. Protocollo di audit uomo-uomo: Osservare una stazione di lavoro dell'analista durante un periodo di picco. Annotare i segni visibili di sopraffazione (ad es. passaggio rapido di finestre senza concentrazione, sospiri eccessivi). Seguire con una domanda: "Quando la coda assomiglia a questa, qual è la tua strategia per decidere cosa lavorare per primo?" Una risposta di "Non so" o "Semplicemente ne scelgo uno" indica paralisi.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Implementare e sintonizzare le regole di correlazione SIEM per aggregare avvisi a bassa fedeltà correlati in singoli meta-avvisi ad alta fedeltà, riducendo il numero totale di elementi nella coda.

- **Mitigazione umana/organizzativa:** Fornire formazione su tecniche di triage e "primi principi" per tagliare attraverso il rumore durante eventi travolgenti.
- **Mitigazione dei processi:** Stabilire un chiaro protocollo di escalation dove un analista può formalmente dichiarare "overload", attivando supporto da altri membri del team o da un shift lead.