Contents

[5.7] Overflow della memoria di lavoro

1. Definizione operativa: Il punto in cui il volume di informazioni che un analista sta cercando di tracciare mentalmente supera la capacità della loro memoria di lavoro (~7±2 elementi), portando a dettagli dimenticati, query ripetute e ragionamento incoerente.

2. Metrica principale e algoritmo:

- **Metrica:** Tasso di ridondanza delle informazioni (IRR). Formula: `IRR = (Numero di query ripetute per le stesse informazioni all'interno di una singola sessione di investigazione) / (Numero totale di query nella sessione)`.
- **Pseudocodice:**

```
def calculate_irr(investigation_session):
    # investigation_session: una lista di query di ricerca effettuate da un analista per u
    total_queries = len(investigation_session)
    unique_queries = set()
    redundant_count = 0

    for query in investigation_session:
        normalized_query = normalize_query(query)  # Rimuovi timestamp, bit specifici del
        if normalized_query in unique_queries:
            redundant_count += 1
        else:
            unique_queries.add(normalized_query)

    return redundant_count / total_queries
```

- **Soglia di avviso:** `IRR > 0.1` (Più del 10% delle query di un analista sono ripetizioni di informazioni che hanno già recuperato).

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

- **Log di query SIEM:** Essenziale per questa metrica. Richiede la registrazione del testo completo delle query di ricerca eseguite dagli utenti. Query: `index=siem_audit user=$analyst_id sourcetype=search` e raggruppa per `alert_id`.

4. Protocollo di audit uomo-uomo: Sorvegliare un analista durante un'investigazione complessa. Annotare se frequentemente dicono cose come "Aspetta, quale era quell'IP?" o "Ho già cercato questo ma l'ho dimenticato." Osservare se utilizzano eccessivamente blocchi note o post-it per compensare le limitazioni della memoria.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Incoraggiare e addestrare gli analisti a usare le funzioni di notebook di investigazione integrate del SIEM o le funzioni di tracciamento della sessione per scaricare le informazioni dalla loro mente.

- **Mitigazione umana/organizzativa:** Insegnare agli analisti a usare framework di nota strutturata (ad es. il modello SOARA) per esternalizzare la loro memoria di lavoro.
- **Mitigazione dei processi:** Progettare i playbook di investigazione per includere i passaggi di documentazione dei risultati chiave (IP, hash, nomi utente) in una sezione dedicata del ticket mentre vengono scoperti, creando un "cervello esterno" condiviso.