Contents

[5.6] Tunneling cognitivo

1. Definizione operativa: Un'intensa concentrazione su un singolo aspetto, spesso ristretto, di un incidente di sicurezza a spese di una visione più olistica e ampia, causando all'analista di trascurare informazioni periferiche ma critiche.

2. Metrica principale e algoritmo:

- **Metrica:** Indice di ampiezza dell'investigazione (IBI). Formula: `IBI = (Numero di fonti dati uniche interrogate per investigazione) / (Durata dell'investigazione in ore)`. Un IBI molto basso suggerisce un approccio tunnel-vision ristretto.
- **Pseudocodice:**

```
def calculate_ibi(investigation_sessions):
    # investigation_sessions: una lista di sessioni, ognuna contiene 'start_time', 'end_t
    ibi_scores = []
    for session in investigation_sessions:
        duration_hours = (session.end_time - session.start_time).total_seconds() / 3600
        unique_data_sources = set(session.data_sources_queried)
        ibi = len(unique_data_sources) / duration_hours
        ibi_scores.append(ibi)
    return np.median(ibi_scores)  # Usa la mediana per evitare distorsioni da sessioni mo
```

- **Soglia di avviso:** `IBI < 0.8` (L'analista interroga meno di una fonte dati unica per ora in media durante un'investigazione).

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

- **Log di query SIEM:** La fonte primaria. Query: `index=siem_audit user=$analyst_id action=search` per vedere quali indici/sourcetype stanno cercando.
- **Log degli strumenti EDR/Network:** Log di audit da strumenti come CrowdStrike, Splunk UEBA, o Corelight per catturare le query effettuate direttamente a queste piattaforme.
- **Sistema Ticketing:** Per ottenere il periodo di tempo di un'investigazione (dalla creazione dell'avviso alla risoluzione).

4. Protocollo di audit uomo-uomo: Presentare a un analista uno studio di caso di incidente complesso. Chiedere loro di verbalizzare il loro processo di pensiero e piano di investigazione. Un auditor dovrebbe ascoltare un approccio ristretto e lineare (ad es. "Guarderei i log del firewall e basta") rispetto a uno ampio (ad es. "Controllerei EDR, poi netflow, poi vedrei se l'utente è stato phishing…").

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Sviluppare e promuovere dashboard di investigazione pre-costruite nel SIEM che automaticamente affiorano dati correlati da più fonti (ad es. endpoint, network, identità) per un dato avviso.

- **Mitigazione umana/organizzativa:** Formazione basata su framework “kill chain” o “MITRE ATT&CK” per incoraggiare gli analisti a pensare in modo ampio alle fasi di un attacco e alle fonti dati associate.
- **Mitigazione dei processi:** Incorporare un passo obbligatorio di “peer bounce” nel processo di investigazione per incidenti critici, dove l’analista deve brevemente spiegare le loro scoperte e approccio a un collega per scoprire punti ciechi potenziali.