Contents

[8.10] Logica dei Sogni negli Spazi Digitali

1. Definizione Operativa: L'applicazione di processi di pensiero irrazionali, associativi e simbolicamente distorti—caratteristici della fase REM—agli ambienti digitali e agli incidenti di sicurezza, portando a non sequitur, confabulazione e pensiero magico nella risoluzione dei problemi.

2. Metrica Principale & Algoritmo:

- **Metrica:** Densità di Associazione Irrazionale (IAD). Formula: `IAD = Conteggio_Connessioni_Illogiche / Connessioni_Totali_Effettuate`.
- **Pseudocodice:**

```
# Questa è una metrica altamente complessa che richiede NLP avanzato. Questo è uno schema
def calculate_iad(incident_id):
    # 1. Recupera tutta la documentazione e comunicazione per un incidente specifico
    incident_data = fetch_incident_data(incident_id)  # ticket, log chat, rapporto

    # 2. Usa NLP per estrarre relazioni causali e connessioni logiche asserite dagli anal
    extracted_connections = extract_causal_claims(incident_data)

    # 3. Valida queste connessioni rispetto a un grafo di conoscenza di TTP noti, infrast
    illogical_connections = 0
    for connection in extracted_connections:
        if not validate_connection(connection):  # es. contro MITRE ATT&CK, CMDB
            illogical_connections += 1

    # 4. Calcola la densità
    iad = illogical_connections / len(extracted_connections) if extracted_connections else
    return iad
```

- **Soglia di Allerta:** `IAD > 0.25` (Più del 25% dei collegamenti causali effettuati durante l'analisi dell'incidente sono illogici o non supportati dai fatti).

3. Fonti Dati Digitali (Input dell'Algoritmo):

- **Rapporti di Risposta agli Incidenti:** Analisi NLP del rapporto finale.
- **Piattaforme di Comunicazione:** Messaggi Teams/Slack durante l'incidente (anonimizzati).
- **Sistemi di Ticketing:** Ticket di incidente Jira/ServiceNow e note di indagine.

4. Protocollo di Audit Umano-Umano: Un investigatore senior rivede separatamente le prove e la cronologia di un incidente chiuso. Quindi intervista il team di analisi, chiedendo loro di ripercorrere il loro processo di ragionamento. L'auditor cerca salti nella logica, assunzioni trattate come fatti o spiegazioni che si basano sulla coincidenza piuttosto che su prove.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Sviluppare e utilizzare uno strumento di documentazione strutturato degli incidenti che costringa gli analisti a collegare le conclusioni a pezzi specifici di prove da log e sistemi.
- **Mitigazione Umana/Organizzativa:** Implementare un passaggio obbligatorio di "revisione paritaria" o "avvocato del diavolo" nel processo di analisi degli incidenti per sfidare le assunzioni e i gap logici.
- **Mitigazione del Processo:** Addestrare gli investigatori in tecniche analitiche strutturate (SAT) provenienti dall'analisi di intelligence, come l'Analisi delle Ipotesi Concorrenti (ACH), per contrastare la "logica dei sogni" intuitiva ma difettosa.