Contents

[4.1] Paralisi Decisionale Basata sulla Paura

1. Definizione Operativa: Uno stato di spegnimento cognitivo e inazione comportamentale innescato da paura o ansia intensa associata a una minaccia di sicurezza, impedendo a un analista di eseguire procedure di risposta critiche.

2. Metrica Principale e Algoritmo:

- **Metrica:** Fear-based Decision Paralysis Rate (FDPR). Formula: `FDPR = (Numero di incidenti senza azioni nonostante alta fiducia) / (Numero totale di incidenti ad alta fiducia)`.
- **Pseudocodice:**

  python

```
def calculate_fdpr(incident_logs, comms_logs, confidence_threshold=0.8):
    """
    incident_logs: da SIEM/SOAR, con azioni degli analisti
    comms_logs: da chat/email, per valutare il sentimento
    """
    # 1. Identificare incidenti ad alta fiducia (es. confidence score da ML model > thresh
    high_confidence_incidents = [i for i in incident_logs if i.confidence_score >= confide

    paralyzed_count = 0
    for incident in high_confidence_incidents:
        # 2. Verificare se nessuna azione decisiva è stata intrapresa entro una finestra c
        actions_taken = get_actions_for_incident(incident.id, incident.created_time + time
        decisive_actions = [a for a in actions_taken if a.type in ['contain', 'isolate', '

        # 3. Controllare le comunicazioni per indicatori di paura se nessuna azione è stat
        if len(decisive_actions) == 0:
            relevant_comms = get_comms_for_incident(comms_logs, incident.id)
            # Usare analisi del sentimento o corrispondenza di parole chiave su paura/ansi
            if contains_fear_indicators(relevant_comms):
                paralyzed_count += 1

    # 4. Calcolare FDPR
    total_high_conf = len(high_confidence_incidents)
    FDPR = paralyzed_count / total_high_conf if total_high_conf > 0 else 0
    return FDPR
```

- **Soglia di Allarme:** `FDPR > 0.15` (Paralisi si verifica in >15% degli incidenti ad alta fiducia)

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

- **API SIEM/SOAR:** Per log degli incidenti, confidence score e timeline delle azioni.

- **API Piattaforme di Comunicazione (Slack, Teams):** Per accedere ai dati di canale/messaggio correlati agli ID degli incidenti per analisi del sentimento.
- **Modello NLP (Natural Language Processing):** Modello pre-allenato per analisi del sentimento (es. rilevamento di ansia, paura) o un elenco di parole chiave (`"panico"`, `"non so cosa fare"`, `"spaventato"`, `"sopraffatto"`).

4. Protocollo di Audit Umano-su-Umano: Durante esercizi di tavolo o debriefing di team rosso, usare domande guidate: "Quando l'[evento critico simulato] si è verificato, descrivi cosa sentivi. Cosa ti passava per la mente nei primi minuti? Cosa ti ha impedito di intraprendere azioni immediate?" Cercare segnali verbali e non verbali di risposta di congelamento.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare script "panic button" nella piattaforma SOAR che, quando attivati, eseguono un playbook di contenimento standardizzato per automatizzare i passi di risposta iniziale e rompere la paralisi.
- **Mitigazione Umana/Organizzativa:** Integrare formazione di inoculazione dello stress negli esercizi di tavolo, simulando deliberatamente scenari ad alta pressione in un ambiente controllato per costruire resilienza.
- **Mitigazione del Processo:** Progettare playbook di risposta agli incidenti con alberi decisionali binari molto semplici per i primi 15 minuti (es. "Se X, allora eseguire Script di Contenimento A. Se Y, allora chiamare immediatamente il Supervisore.") per ridurre il carico cognitivo durante una crisi.