

Contents

[8.1] Proiezione dell'ombra su attaccanti	1
---	---

[8.1] Proiezione dell'ombra su attaccanti

1. Definizione Operativa: Un meccanismo di difesa psicologica in cui un individuo o un gruppo attribuisce i propri impulsi, intenzioni e tratti inaccettabili o negativi (la loro “Ombra”) esclusivamente ad attaccanti esterni, creando un punto cieco alle minacce interne e favorendo una mentalità “noi vs loro” che indebolisce la difesa olistica.

2. Metrica Principale & Algoritmo:

- **Metrica:** Rapporto Proiezione-verso-Minaccia-Interna (PITR). Formula: $PITR = \frac{\text{(Menzioni di attribuzione esterna nei rapporti di incidente)}}{\text{(Menzioni di fattori interni nei rapporti di incidente)}}$.

- **Pseudocodice:**

```
def calculate_pitr(incident_reports, start_date, end_date):  
    """  
    incident_reports: Collezione di documenti di rapporto post-incidente  
    """  
  
    # 1. Elenchi di Parole Chiave NLP  
    external_keywords = ['hacker', 'nation-state', 'esterno', 'cybercriminale', 'loro', 'c  
    internal_keywords = ['misconfiguration', 'errore', 'dipendente', 'insider', 'processo  
  
    total_external_mentions = 0  
    total_internal_mentions = 0  
  
    for report in incident_reports:  
        if start_date <= report.date <= end_date:  
            text = report.title + " " + report.root_cause_analysis  
            # 2. Conteggio delle occorrenze di parole chiave (semplice approccio bag-of-wo  
            external_count = count_keywords(text, external_keywords)  
            internal_count = count_keywords(text, internal_keywords)  
  
            total_external_mentions += external_count  
            total_internal_mentions += internal_count  
  
            # 3. Calcola PITR, evita divisione per zero  
            if total_internal_mentions > 0:  
                PITR = total_external_mentions / total_internal_mentions  
            else:  
                PITR = total_external_mentions # Se non vengono citate fattori interni, il rappo  
    return PITR
```

- **Soglia di Allerta:** $PITR > 3.0$ (Le minacce esterne sono menzionate 3 volte più spesso dei fattori interni nell'analisi della causa radice)

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

- **Piattaforma di Gestione degli Incidenti (Jira, ServiceNow):** Campi: `post_mortem_report`, `root_cause_analysis`, `title`.
- **Elaborazione del Testo NLP:** Un semplice contatore di parole chiave o un modello di analisi del sentimento/tema più sofisticato addestrato per identificare il linguaggio di attribuzione.

4. Protocollo di Audit Umano-Umano: Un terzo indipendente neutrale (ad es., un revisore o consulente esterno) rivede un campione di rapporti di incidente e conduce interviste con gli autori del rapporto. Utilizzano questionari strutturati: “Quali prove ti hanno portato a concludere che la minaccia era principalmente esterna? Quanto bene hai indagato sui potenziali fattori interni che hanno contribuito?” L’obiettivo è identificare le assunzioni e le narrazioni non contestate.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Configura il sistema di gestione degli incidenti per richiedere un campo obbligatorio nell’analisi della causa radice che deve elencare almeno un potenziale fattore di processo interno o umano che avrebbe potuto contribuire all’impatto dell’incidente, anche se esterno.
- **Mitigazione Umana/Organizzativa:** Condurre una formazione sui bias cognitivi e sui meccanismi di difesa per il team di risposta agli incidenti, con focus specifico sul concetto di Ombra di Jung e come si manifesta nella cybersecurity.
- **Mitigazione del Processo:** Integrare un passaggio obbligatorio di “Red Team” o “Avvocato del Diavolo” nel processo di revisione degli incidenti, in cui il ruolo di un individuo designato è argomentare contro la narrativa prevalente e proporre ipotesi alternative di causa interna.