# Contents



## [6.5] Effetto Spettatore nella Risposta agli Incidenti

**1. Definizione Operativa:** Il fenomeno in cui gli individui sono meno propensi a intraprendere azioni durante un'emergenza (ad es. un incidente di sicurezza) quando altri sono presenti. Questo si manifesta come un ritardo nella risposta iniziale o nell'escalation di un incidente perché ogni osservatore presume che qualcun altro lo gestirà.

**2. Metrica Principale & Algoritmo:**

- **Metrica:** Tempo di Prima Risposta (FRT). Formula: `Tempo tra la creazione dell'incidente e la prima azione significativa intrapresa da qualsiasi membro del team`.
- **Pseudocodice:**

```
def calculate_frt(incidents):
    frt_list = []
    for incident in incidents:
        # Ottenere tutte le azioni per questo incidente, ordinate per tempo
        actions = get_actions(incident.id)
        first_action_time = actions[0].timestamp if actions else None
        if first_action_time:
            response_time = first_action_time - incident.created_time
            frt_list.append(response_time)
    return np.median(frt_list) # Usare mediana per evitare distorsione da outlier
```

- **Soglia di Allarme:** `FRT > 15 (minuti)` per incidenti di alta severità.

**3. Fonti Dati Digitali (Input Algoritmo):**

- **SOAR/Ticketing (ServiceNow, Jira):** Tabella degli Incidenti. Campi: `number`, `sys_created_on`, `state`.
- **Log di Audit SOAR/Ticketing:** Campi: `tablename`, `recordkey`, `fieldname`, `sys_created_on`. (Per trovare il primo cambio di stato o commento dopo la creazione dell'incidente).

**4. Protocollo di Audit Umano-a-Umano:** Durante un esercizio di simulazione o una revisione post-incidente di un caso reale, chiedi al team: "Quando l'avviso è arrivato per la prima volta, qual era il tuo processo di pensiero? L'hai visto? Hai presumo che una persona specifica o il lead del turno lo gestirebbe? C'è stata esitazione nell'essere il primo a impegnarsi?"

**5. Azioni di Mitigazione Consigliate:**

- **Mitigazione Tecnica/Digitale:** Configurare le regole di avviso per pagare direttamente l'analista on-call principale (ad es. tramite PagerDuty/VictorOps) per avvisi critici, bypassando un canale condiviso e assegnando la proprietà immediatamente.
- **Mitigazione Umana/Organizzativa:** Implementare e praticare un protocollo formale di "Prima Risposta" per ogni turno, designando chi ci si aspetta che effettui il triage di qualsiasi avviso di alta severità in arrivo.

- **Mitigazione del Processo:** Creare una cultura di “See Something, Say Something” in cui qualsiasi analista che noti un avviso non azionato, anche se non assegnato a loro, sia autorizzato e si aspetti di almeno assegnarlo alla persona corretta o portarlo in attenzione nel chat del team.