# Contents



## [7.3] Aggressione da Risposta di Lotta

**1. Definizione Operativa:** Una risposta indotta da stress caratterizzata da interazioni ostili o eccessivamente forzate con sistemi, strumenti o colleghi, spesso portando a bypass procedurali, errori di configurazione o un ambiente di team tossico.

**2. Metrica Principale e Algoritmo:**

- **Metrica: Tasso di Interazione Aggressiva (AIR)**. Formula: `AIR = (N_aggressive_commands + N_hostile_messages) / N_total_interactions`.
- **Pseudocodice:**

  python

  ```
  def calculate_air(employee_id, start_date, end_date):
      # Interrogare la cronologia della riga di comando per pattern aggressivi (es. flag for
      cmd_logs = query_siem(index='linux_audit', search=f'user:{employee_id} (rm * -rf | kil
      n_aggressive_cmds = count(cmd_logs)

      # Interrogare le piattaforme di comunicazione per linguaggio ostile
      messages = query_teams_api(employee_id, start_date, end_date)
      hostile_keywords = ["idiot", "useless", "why bother", "broken", "fix it now", "dumb"]
      n_hostile_msgs = count_messages_containing(messages, hostile_keywords)

      # Ottenere il conteggio totale delle interazioni per la normalizzazione
      total_cmds = query_siem(index='linux_audit', search=f'user:{employee_id}', result_coun
      total_msgs = count(messages)
      total_interactions = total_cmds + total_msgs

      if total_interactions > 0:
          air = (n_aggressive_cmds + n_hostile_msgs) / total_interactions
      else:
          air = 0
      return air
  ```

- **Soglia di Allerta:** `AIR > 0.05` (5% delle interazioni sono aggressive) per un periodo di una settimana.

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

- **SIEM (es. Splunk):** Index `linux_audit` o `windows_events`, campi `user`, `command`.
- **API della Piattaforma di Comunicazione (es. API Microsoft Graph per Teams):** `sender`, `body`, `timestamp`.

**4. Protocollo di Audit Umano-Umano:** Osservazione del team lead e feedback anonimo a 360 gradi dai colleghi. Domande campione: "Hai osservato un collega che eludere i controlli di sicurezza per frustrazione?" "Qualcuno nel team usa linguaggio ostile o denigrante quando i sistemi falliscono?"

**5. Azioni di Mitigazione Consigliate:**

- **Mitigazione Tecnica/Digitale:** Implementare misure tecniche di sicurezza come la protezione `--no-preserve-root` sui comandi `rm` e richiedere l'approvazione doppia per le azioni critiche e distruttive.
- **Mitigazione Umana/Organizzativa:** Fornire formazione sulla risoluzione dei conflitti e sulla gestione dello stress. Promuovere una cultura di post-mortem incolpevole.
- **Mitigazione di Processo:** Introdurre un protocollo di "raffreddamento" in cui un analista frustrato può trasferire un compito a un collega senza penalità.