

Contents

[7.1] Compromissione da Stress Acuto	1
--	---

[7.1] Compromissione da Stress Acuto

1. Definizione Operativa: Un deterioramento temporaneo nelle capacità cognitive e motorie causato dalla risposta neuroendocrina a un incidente di sicurezza immediato e ad alto rischio, manifestandosi come rallentamento del tempo di reazione, lapsi di memoria e tremori fisici.

2. Metrica Principale e Algoritmo:

- **Metrica:** Degradazione delle Prestazioni Indotta da Stress (SIPD). Formula: SIPD = (Tempo medio di completamento del compito durante gli incidenti) / (Tempo medio di completamento del compito durante periodi calmi).

- **Pseudocodice:**

```
python
```

```
def calculate_sipd(task_logs, incident_periods):  
    """  
        task_logs: Registri di compiti routine e ripetitivi (es. esecuzione query standard, tr  
        incident_periods: Elenco dei tempi di inizio/fine per gli incidenti significativi  
    """  
    # 1. Calcolare il tempo medio del compito durante i periodi di incidente  
    tasks_during_incidents = []  
    for period in incident_periods:  
        period_tasks = [t for t in task_logs if period.start <= t.timestamp <= period.end]  
        tasks_during_incidents.extend(period_tasks)  
  
    avg_time_during_incident = calculate_avg_task_time(tasks_during_incidents)  
  
    # 2. Calcolare il tempo medio del compito durante periodi calmi (es. 1 settimana prima  
    calm_period_tasks = get_tasks_from_calm_period(task_logs, incident_periods)  
    avg_time_calm = calculate_avg_task_time(calm_period_tasks)  
  
    # 3. Calcolare il rapporto SIPD  
    if avg_time_calm > 0:  
        SIPD = avg_time_during_incident / avg_time_calm  
    else:  
        SIPD = 1 # Nessun deterioramento se nessuna baseline  
    return SIPD
```

- **Soglia di Allerta:** SIPD > 1.5 (Le prestazioni del compito sono 50% più lente durante incidenti ad alto stress)

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

- **Registri della Piattaforma SOAR:** Timestamp per l'inizio e il completamento dei passaggi del playbook automatizzato o manuale.
- **API del Sistema di Ticketing:** Metriche di tempo per riconoscere e risolvere i ticket.

- **Dichiarazioni di Incidente:** Un registro di quando gli incidenti significativi sono stati formalmente dichiarati e risolti.
- 4. Protocollo di Audit Umano-Umano:** Simulare un incidente altamente realistico e stressante in un ambiente di training. Utilizzare sensori biometrici (variabilità della frequenza cardiaca, risposta cutanea galvanica) per misurare i livelli di stress e correlarli con le metriche di prestazioni su compiti standardizzati (es. tempo per contenere una violazione simulata). Fare un debriefing successivo sui sentimenti soggettivi di compromissione.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Progettare i playbook SOAR per incidenti ad alta gravità in modo che abbiano più passaggi automatizzati e meno compiti manuali e soggetti a errori, riducendo il carico cognitivo sull'analista compromesso.
- **Mitigazione Umana/Organizzativa:** Introdurre un “sistema a coppie” durante gli incidenti significativi, accoppiando un risponditore primario stressato con un analista secondario il cui ruolo è verificare i comandi, fornire una guida calma ed eseguire compiti su istruzione.
- **Mitigazione di Processo:** Rendere obbligatorio l’uso di checklist scritte per le azioni critiche durante un incidente dichiarato. L’atto fisico di spuntare una casella può aiutare a focalizzare una mente stressata e prevenire lapsi di memoria o passaggi saltati.