Categoria 5: Vulnerabilità di sovraccarico cognitivo

Contents

Questa directory contiene schemi di implementazione dettagliati per tutti i 10 indicatori nella categoria di vulnerabilità Cognitive Overload.

Panoramica

Le vulnerabilità da sovraccarico cognitivo sfruttano i limiti dell'elaborazione delle informazioni umane, dell'attenzione, della memoria di lavoro e della capacità decisionale sotto alto carico cognitivo.

Indicatori

1. [**5.1**] **Desensibilizzazione da affaticamento degli avvisi** - Tracciamento MCAR (Missed Critical Alert Rate)
2. [**5.2**] **Errori di affaticamento decisionale** - Degradazione della qualità decisionale nel tempo
3. [**5.3**] **Paralisi da sovraccarico informativo** - Ritardi nella risposta con aumento del volume di eventi
4. [**5.4**] **Degradazione del multitasking** - Declino delle prestazioni con attività concorrenti
5. [**5.5**] **Vulnerabilità di cambio di contesto** - Tassi di errore durante le transizioni di attività
6. [**5.6**] **Tunneling cognitivo** - Fissazione su minacce singole mentre si trascurano altre
7. [**5.7**] **Overflow della memoria di lavoro** - Capacità superata in scenari complessi
8. [**5.8**] **Effetti del residuo di attenzione** - Impatti sulle prestazioni da passaggi di attività incompleti
9. [**5.9**] **Disallineamento del modello mentale** - Lacune nella comprensione del sistema
10. [**5.10**] **Confusione del modello mentale** - Modelli mentali contraddittori che causano errori

Schema di implementazione

Ogni file indicatore segue il framework **OFTLISRV** con enfasi sulle metriche di carico cognitivo.

Metriche chiave

Tasso di avvisi critici mancati (MCAR)

```
MCAR = N_missed / N_total_critical
```

Soglia di avviso: MCAR > 0.05 (tasso di mancanza del 5%)

Indice di qualità decisionale

```
DQI = (Correct_decisions / Total_decisions) × (1 / Avg_decision_time)
```

Misura accuratezza ed efficienza sotto carico cognitivo.

Punteggio di carico cognitivo

```
CLS = w ×Alert_volume + w ×Task_complexity + w ×Context_switches
```

Fonti dati principali

- **SIEM**: Volume di avvisi, tempi di riconoscimento, tassi di falsi positivi
- **Ticketing**: Complessità delle problematiche, qualità della risoluzione, ticket riapertini
- **Attività dell'utente**: Cambi di applicazione, sessioni concorrenti, durata dell'attività
- **Comunicazione**: Volume di email/Slack, tempi di risposta
- **Dati degli incidenti**: Pattern di errore, rilevamenti mancati

Approccio di rilevamento

Rilevamento dell'affaticamento degli avvisi

```
missed_count = alerts.filter(
    status='closed' AND
    resolution='false_positive' OR
    status='expired'
).count()

MCAR = missed_count / total_critical
```

Overflow della memoria di lavoro

```
WM_capacity = 7 ± 2 items  # Legge di Miller
Current_load = Active_alerts + Open_tickets + Concurrent_tasks
Overflow = Current_load > (WM_capacity × Expertise_factor)
```

Stabilimento della linea di base

Gli indicatori cognitivi richiedono: - Linee di base individuali per analisti (le prestazioni variano significativamente) - Volume di avvisi normale per turno - Distribuzione tipica della complessità dei compiti - Linee di base della frequenza di cambio di contesto

Tipi di eventi comuni

- `alert_generated` → 5.1 (quando il volume supera la capacità)
- `decision_made` → 5.2 (tracciato per la qualità nel tempo)
- `task_switch` → 5.5, 5.8 (cambio di contesto)
- `multiple_incidents` → 5.4, 5.7 (carico concorrente)
- `complex_scenario` → 5.6, 5.10 (tunneling, confusione)

Livelli di rischio

- **Basso** (0-0.33): Carico cognitivo entro la capacità, alte prestazioni
- **Medio** (0.34-0.66): Avvicinamento ai limiti di capacità, degradazione parziale
- **Alto** (0.67-1.00): Stato di sovraccarico, declino significativo delle prestazioni

Strategie di mitigazione

Mitigazioni tecniche

- Triage degli avvisi basato su ML per ridurre il volume
- Soppressione automatica dei falsi positivi
- Aggregazione e deduplicazione degli avvisi
- Automazione del flusso di lavoro per attività di routine

Mitigazioni organizzative

- Rotazione dei compiti per ridurre l'affaticamento
- Programmi di turni che tengono conto dei limiti cognitivi
- Formazione sul processo decisionale sotto stress
- Pause regolari durante periodi ad alto numero di avvisi

Mitigazioni dei processi

- Sintonizzazione settimanale di SIEM per ridurre il rumore
- Scoring della complessità per l'assegnazione dei ticket
- Limiti massimi di incidenti concorrenti
- Protocolli formali di passaggio durante il sovraccarico

Risorse correlate

- **Documentazione di base**: `/foundation docs/core/it-IT/` - Formalizzazione del carico cognitivo
- **Pattern Detector**: `/src/detectors.py` - Algoritmo di affaticamento degli avvisi
- **Dashboard**: `/dashboard/soc/` - Visualizzazione del carico cognitivo
- **Ricerca**: Fattori umani nel processo decisionale sulla cybersicurezza