# Category 5: Cognitive Overload Vulnerabilities

## Contents



This directory contains detailed implementation schemas for all 10 indicators in the Cognitive Overload vulnerability category.

## Overview

Cognitive overload vulnerabilities exploit limitations in human information processing, attention, working memory, and decision-making capacity under high cognitive load.

## Indicators

1. [**5.1**] **Alert fatigue desensitization** - MCAR (Missed Critical Alert Rate) tracking
2. [**5.2**] **Decision Fatigue Errors** - Decision quality degradation over time
3. [**5.3**] **Information Overload Paralysis** - Response delays with increasing event volume
4. [**5.4**] **Multitasking Degradation** - Performance decline with concurrent tasks
5. [**5.5**] **Context Switching Vulnerabilities** - Error rates during task transitions
6. [**5.6**] **Cognitive Tunneling** - Fixation on single threats while missing others
7. [**5.7**] **Working Memory Overflow** - Capacity exceeded in complex scenarios
8. [**5.8**] **Attention Residue Effects** - Performance impacts from incomplete task switches
9. [**5.9**] **Mental Model Mismatch** - System understanding gaps
10. [**5.10**] **Mental Model Confusion** - Contradictory mental models causing errors

## Implementation Schema

Each indicator file follows the **OFTLISRV** framework with emphasis on cognitive load metrics.

## Key Metrics

### Missed Critical Alert Rate (MCAR)

```
MCAR = N_missed / N_total_critical
```

Alert threshold: MCAR $> 0.05$ (5% miss rate)

### Decision Quality Index

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

Measures accuracy and efficiency under cognitive load.

### Cognitive Load Score

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

## Key Data Sources

- **SIEM**: Alert volume, acknowledgment times, false positive rates
- **Ticketing**: Issue complexity, resolution quality, reopened tickets
- **User Activity**: Application switches, concurrent sessions, task duration
- **Communication**: Email/Slack volume, response times
- **Incident Data**: Error patterns, missed detections

## Detection Approach

### Alert Fatigue Detection

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

MCAR = missed_count / total_critical
```

### Working Memory Overflow

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

## Baseline Establishment

Cognitive indicators require: - Individual analyst baselines (performance varies significantly) - Normal alert volume per shift - Typical task complexity distribution - Context switch frequency baselines

## Common Event Types

- `alert_generated` → 5.1 (when volume exceeds capacity)
- `decision_made` → 5.2 (tracked for quality over time)
- `task_switch` → 5.5, 5.8 (context switching)
- `multiple_incidents` → 5.4, 5.7 (concurrent load)
- `complex_scenario` → 5.6, 5.10 (tunneling, confusion)

## Risk Levels

- **Low** (0-0.33): Cognitive load within capacity, high performance
- **Medium** (0.34-0.66): Approaching capacity limits, some degradation
- **High** (0.67-1.00): Overload state, significant performance decline

## Mitigation Strategies

### Technical Mitigations

- ML-based alert triage to reduce volume
- Automated false positive suppression
- Alert aggregation and deduplication
- Workflow automation for routine tasks

### Organizational Mitigations

- Task rotation to reduce fatigue
- Shift schedules that account for cognitive limits

- Training on decision-making under stress
- Regular breaks during high-alert periods

### Process Mitigations

- Weekly SIEM tuning to reduce noise
- Complexity scoring for ticket assignment
- Maximum concurrent incident limits
- Formal handoff protocols during overload

## Related Resources

- **Dense Foundation**: `/foundation docs/core/en-US/` - Cognitive load formalization
- **Pattern Detector**: `/src/detectors.py` - Alert fatigue algorithm
- **Dashboard**: `/dashboard/soc/` - Cognitive load visualization
- **Research**: Human factors in cybersecurity decision-making