Category 7: Stress Response Vulnerabilities

Contents

This directory contains detailed implementation schemas for all 10 indicators in the Stress Response vulnerability category.

Overview

Stress response vulnerabilities exploit physiological and psychological reactions to acute and chronic stressors, leading to degraded security decision-making.

Indicators

1. [**7.1**] **Acute Stress Response** - Fight/flight/freeze reactions impacting decisions
2. [**7.2**] **Chronic Stress Accumulation** - Long-term stress degrading performance
3. [**7.3**] **Crisis Paralysis** - Decision-making shutdown under extreme pressure
4. [**7.4**] **Panic-Driven Actions** - Impulsive decisions without proper evaluation
5. [**7.5**] **Burnout Indicators** - Exhaustion leading to security lapses
6. [**7.6**] **Stress-Induced Tunnel Vision** - Narrowed focus missing peripheral threats
7. [**7.7**] **Hypervigilance Fatigue** - Excessive alertness leading to exhaustion
8. [**7.8**] **Learned Helplessness** - Giving up on security due to repeated failures
9. [**7.9**] **Crisis Overreaction** - Disproportionate response to minor events
10. [**7.10**] **Post-Incident Stress** - Performance degradation after major incidents

Implementation Schema

Each indicator follows the **OFTLISRV** framework with physiological and behavioral stress markers.

Key Metrics

Acute Stress Score

```
ASS = w ×Incident_severity + w ×Time_pressure + w ×Decision_load
```

Threshold: ASS $>$ 0.7 indicates acute stress state.

Burnout Index

```
BI = (Alert_volume × Incident_frequency) / (Recovery_time × Support_available)
```

Decision Quality Under Stress

```
DQUS = Correct_decisions_stress / Correct_decisions_baseline
```

Key Data Sources

- **SIEM**: Incident volume, severity distribution, resolution times
- **Ticketing**: Workload metrics, overtime hours, ticket backlog
- **HR Systems**: Vacation usage, sick days, tenure
- **Communication**: Sentiment analysis in tickets/emails
- **Incident Response**: Major incident frequency, post-mortem data

Detection Approach

Burnout Detection

```
# Calculate burnout indicators
alert_rate = count_alerts(window=7_days) / 7
```

```
incident_load = count_critical_incidents(window=30_days)
recovery_time = hours_off_duty / hours_on_duty

burnout_score = (alert_rate × incident_load) / recovery_time

if burnout_score > threshold:
    flag_burnout_risk(analyst_id)
```

Acute Stress Markers

- Response time degradation (>2x baseline)
- Error rate increase (>3x baseline)
- Abbreviated ticket notes
- Escalation rate increase
- Help-seeking behavior

Baseline Establishment

Stress indicators require: - 90-day performance baseline per analyst - Normal workload patterns - Historical incident impact data - Individual stress response patterns

Common Event Types

- `major_incident` → 7.1, 7.4, 7.10
- `continuous_alerts` → 7.2, 7.5, 7.7
- `overwhelming_scenario` → 7.3, 7.6
- `repeated_failures` → 7.8
- `minor_event_overreaction` → 7.9

Risk Levels

- **Low** (0-0.33): Normal stress levels, performance maintained
- **Medium** (0.34-0.66): Elevated stress, some performance impact
- **High** (0.67-1.00): Acute/chronic stress, significant degradation

Mitigation Strategies

Immediate (Acute Stress)

- Activate backup analyst for critical decisions
- Implement mandatory breaks
- Provide decision support tools
- Escalation to senior staff

Long-term (Chronic Stress/Burnout)

- Workload redistribution

- Mandatory time off
- Training on stress management
- Organizational culture changes
- Staffing adjustments

Preventive

- Regular rotation between high/low stress roles
- Wellness programs
- Post-incident debriefings
- Stress resilience training

Related Resources

- **Dense Foundation**: `/foundation docs/core/en-US/` - Stress response formalization
- **Pattern Detector**: `/src/detectors.py` - Burnout detection algorithm
- **Dashboard**: `/dashboard/soc/` - Stress indicator visualization
- **Research**: Occupational stress in cybersecurity