Category 4: Affective Vulnerabilities

Contents

This directory contains detailed implementation schemas for all 10 indicators in the Affective (Emotional) vulnerability category.

Overview

Affective vulnerabilities exploit emotional states—fear, excitement, trust, curiosity—to manipulate security decisions and bypass rational threat assessment.

Indicators

1. [**4.1**] **Fear Paralysis** - Panic preventing effective response
2. [**4.2**] **Excitement-Induced Carelessness** - Positive emotions reducing vigilance
3. [**4.3**] **Trust Exploitation** - Misplaced trust in attackers
4. [**4.4**] **Emotional Contagion** - Spread of emotional states affecting teams
5. [**4.5**] **Curiosity Exploitation** - Using curiosity to trigger risky behaviors
6. [**4.6**] **Anger-Driven Decisions** - Hostility leading to poor choices
7. [**4.7**] **Hope/Optimism Bias** - Underestimating threats due to wishful thinking
8. [**4.8**] **Sadness-Induced Passivity** - Low mood reducing security engagement
9. [**4.9**] **Empathy Exploitation** - Using sympathy to manipulate compliance
10. [**4.10**] **Emotional Exhaustion** - Depletion of emotional resources

Implementation Schema

Each indicator follows the **OFTLISRV** framework with emotional state detection.

Key Metrics

Emotional Arousal Score

`EAS = Sentiment_polarity × Sentiment_intensity`

Range: [-1, 1], where extremes indicate vulnerability.

Fear Response Index

`FRI = Response_delay × Error_rate × Escalation_frequency`

Trust Exploitation Score

`TES = Successful_social_engineering / Total_attempts`

Key Data Sources

- **Email/Communication**: Sentiment analysis of messages
- **Phishing Simulations**: Click rates, reporting rates
- **SIEM**: Unusual access patterns during emotional events
- **Incident Data**: Response quality during high-emotion periods
- **HR Systems**: Organizational events (layoffs, acquisitions)
- **External**: News sentiment about company

Detection Approach

Sentiment Analysis

```
from sentiment_analyzer import analyze
```

```
# Analyze email/slack messages
sentiment = analyze(message_text)

if sentiment.polarity < -0.5:  # Strong negative
    flag_emotional_state(user, 'fear/sadness')
elif sentiment.polarity > 0.5:  # Strong positive
    flag_emotional_state(user, 'excitement/optimism')
```

Fear Detection Markers

- Keywords: urgent, critical, breach, attack, lawsuit
- Unusual escalation patterns
- After-hours activity spikes
- Rapid decision-making without verification

Excitement Detection Markers

- Keywords: opportunity, exclusive, reward, winner
- Reduced verification steps
- Policy exceptions for "special" cases

Baseline Establishment

Affective indicators require: - 60-day baseline of normal sentiment patterns - Individual emotional response patterns - Organizational emotional climate - Correlation with external events

Common Event Types

- `phishing_clicked` → 4.3, 4.5, 4.9 (trust, curiosity, empathy)
- `crisis_event` → 4.1 (fear paralysis)
- `good_news` → 4.2, 4.7 (excitement, optimism)
- `major_incident` → 4.4, 4.10 (contagion, exhaustion)
- `conflict_detected` → 4.6 (anger)

Risk Levels

- **Low** (0-0.33): Emotional stability, rational decision-making
- **Medium** (0.34-0.66): Emotional influence, some impairment
- **High** (0.67-1.00): Strong emotional state, significant vulnerability

Mitigation Strategies

Technical

- Enhanced monitoring during organizational stress
- Automatic verification for emotionally-charged requests
- Circuit breakers for rapid decisions

Organizational

- Emotional intelligence training
- Mental health support resources
- Transparent communication during crises
- Celebration protocols that maintain security awareness

Process

- Mandatory cooling-off period for high-emotion decisions
- Buddy system for verification during stress
- Debriefing after emotional incidents

Related Resources

- **Dense Foundation**: `/foundation docs/core/en-US/` - Affective vulnerability models
- **Pattern Examples**: `/docs/cpf_pattern_examples_list.md`
- **Dashboard**: `/dashboard/soc/` - Emotional state indicators