Category 8: Unconscious Process Vulnerabilities

Contents

This directory contains detailed implementation schemas for all 10 indicators in the Unconscious Process vulnerability category.

Overview

Unconscious process vulnerabilities exploit automatic behaviors, implicit biases, habitual patterns, and cognitive processes operating below conscious awareness.

Indicators

1. [**8.1**] **Automaticity Exploitation** - Leveraging automatic response patterns
2. [**8.2**] **Implicit Bias Effects** - Unconscious prejudices affecting decisions
3. [**8.3**] **Habitual Behavior Exploitation** - Targeting routine behaviors
4. [**8.4**] **Priming Effects** - Unconscious influence from prior exposure
5. [**8.5**] **Anchoring Bias** - Over-reliance on first piece of information
6. [**8.6**] **Confirmation Bias** - Seeking information confirming existing beliefs
7. [**8.7**] **Availability Heuristic** - Overweighting easily recalled information
8. [**8.8**] **Recognition Heuristic** - Trusting familiar patterns over analysis
9. [**8.9**] **Affect Heuristic** - Using emotions as shortcuts for decisions
10. [**8.10**] **Unconscious Defense Mechanisms** - Denial, projection, rationalization

Implementation Schema

Each indicator follows the **OFTLISRV** framework with focus on detecting unconscious patterns.

Key Metrics

Automaticity Score

```
AS = Response_speed / Verification_depth
```

High score indicates automatic response without conscious processing.

Implicit Bias Index

```
IBI = (Decisions_favoring_group_A - Decisions_favoring_group_B) / Total_decisions
```

Confirmation Bias Score

```
CBS = Info_supporting_hypothesis / (Info_supporting + Info_contradicting)
```

Score > 0.7 indicates strong confirmation bias.

Key Data Sources

- **SIEM**: Response patterns, click-through rates, decision speed
- **Email**: Interaction patterns with different sender types
- **Incident Data**: Investigation breadth, alternative hypotheses considered
- **Ticketing**: Resolution patterns, information gathering behaviors
- **Audit Logs**: System interaction patterns revealing habits

Detection Approach

Automaticity Detection

```
# Identify automatic responses
response_time = calculate_response_time(event)

if response_time < (baseline_time * 0.5):
    # Too fast - likely automatic
    verification_depth = analyze_verification_steps(event)

    if verification_depth < minimum_required:
        flag_automaticity_risk(user_id)
```

Confirmation Bias Detection

```
# Track information gathering in investigations
investigation = get_investigation(incident_id)

supporting_evidence = count_evidence_type('supporting')
contradicting_evidence = count_evidence_type('contradicting')

bias_ratio = supporting_evidence / (supporting_evidence + contradicting_evidence)

if bias_ratio > 0.7:  # Heavily one-sided
    flag_confirmation_bias(analyst_id)
```

Habit Pattern Recognition

```
# Identify repeated behavioral sequences
user_actions = get_action_sequence(user_id, window=30_days)

# Find repeating patterns
patterns = find_frequent_sequences(user_actions, min_frequency=10)

for pattern in patterns:
    if pattern.variation < 0.1:  # Highly consistent = habitual
        flag_habit_exploitation_risk(user_id, pattern)
```

Baseline Establishment

Unconscious process indicators require: - 90-day behavioral pattern baseline - Decision-making process documentation - Individual cognitive bias profiles - Organizational investigation norms

Common Event Types

- `rapid_response` → 8.1, 8.8 (automaticity, recognition)
- `investigation_incomplete` → 8.6, 8.7 (confirmation, availability)
- `familiar_pattern` → 8.3, 8.8 (habit, recognition)
- `initial_anchor_set` → 8.5 (anchoring)

- `prior_exposure` → 8.4 (priming)

Risk Levels

- **Low** (0-0.33): Conscious deliberation, bias awareness
- **Medium** (0.34-0.66): Some automatic processing, manageable bias
- **High** (0.67-1.00): Heavily automatic, strong unconscious influence

Mitigation Strategies

Awareness

- Bias awareness training
- Cognitive bias flashcards
- Regular bias reflection exercises
- Peer bias identification

Structural

- Mandatory verification steps
- Automated bias detection alerts
- Decision review by independent party
- Diverse investigation teams

Process

- Checklist-based investigations
- Devil's advocate requirements
- Alternative hypothesis documentation
- Blind analysis techniques

Related Resources

- **Dense Foundation**: `/foundation docs/core/en-US/` - Unconscious process models
- **Kahneman's Thinking Fast and Slow**: Theoretical foundation
- **Dashboard**: `/dashboard/soc/` - Bias indicator visualization
- **Research**: Cognitive biases in cybersecurity