Category 2: Temporal Vulnerabilities

Contents

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

Overview

Temporal vulnerabilities exploit time pressure, deadline stress, and urgency manipulation to induce security-degrading behaviors.

Indicators

1. [**2.1**] **Urgency-Induced Security Bypass** - Task completion time analysis under pressure
2. [**2.2**] **Time Pressure Decision Degradation** - Decision quality metrics vs deadline proximity

3. [**2.3**] **Deadline-Driven Risk Acceptance** - Exception requests correlated with project deadlines
4. [**2.4**] **After-Hours Security Fatigue** - Off-hours event patterns and error rates
5. [**2.5**] **Rushed Change Implementation** - Change control bypass during time constraints
6. [**2.6**] **Crisis Countdown Effect** - Behavior degradation as deadlines approach
7. [**2.7**] **Temporal Discounting of Security** - Hyperbolic discounting in security decisions
8. [**2.8**] **Weekend/Holiday Exploitation** - Reduced vigilance during off-peak periods
9. [**2.9**] **Shift Transition Vulnerability** - Incidents during handoff periods
10. [**2.10**] **Artificial Urgency Susceptibility** - Response to manufactured time pressure

Implementation Schema

Each indicator file follows the **OFTLISRV** framework for systematic operationalization.

Key Formulas

Urgency-Induced Bypass Rate

```
U_i = (Δt_normal - Δt_urgent) / Δt_normal
```

When U_i $>$ 0.5 (50% acceleration), security degradation is predictable.

Hyperbolic Discounting

```
V = A / (1 + k × D)
```

Where A = actual value, D = delay, k = discount rate (calibrated per org)

Key Data Sources

- **Project Management Systems**: Deadlines, milestone dates, sprint schedules
- **Change Management**: Change request timestamps, approval times
- **SIEM**: Event timestamps, after-hours activity
- **Ticketing**: Issue resolution times, SLA compliance
- **Email/Slack**: Urgency keywords, time pressure indicators

Detection Approach

Poisson Regression for Bypass Rate

```
 = e^(  +  ×pressure +  ×deadline_proximity)
```

Models expected bypass rate given temporal pressure.

Baseline Establishment

Temporal indicators require: - 60-day baseline for normal task completion times - Business hour patterns per department - Seasonal/cyclical deadline patterns - Shift schedule data

Common Event Types

- `urgent_request` → 2.1, 2.10
- `after_hours_access` → 2.4, 2.8
- `change_expedited` → 2.5, 2.6
- `shift_handoff` → 2.9
- `deadline_approaching` → 2.3, 2.7

Risk Levels

- **Low** (0-0.33): Normal time pressure, controls maintained
- **Medium** (0.34-0.66): Elevated time pressure, some control bypasses
- **High** (0.67-1.00): Extreme urgency, systematic security degradation

Mitigation Strategies

- Implement "security time budgets" in project planning
- Pre-authorize common urgent scenarios
- Enhanced monitoring during known deadline periods
- Automated validation for expedited changes

Related Resources

- **Dense Foundation**: `/foundation docs/core/en-US/` - Temporal vulnerability formalization
- **Implementation Guide**: `/docs/cpf_implementation_guide.md`
- **Dashboard**: `/dashboard/soc/` - Timeline visualization