Category 1: Authority-Based Vulnerabilities

Contents

Overview **1**

Indicators **1**

Implementation Schema **2**

Key Data Sources **2**

Detection Approach **2**
Compliance Rate Function 2
Bayesian Authority Legitimacy 2

Baseline Establishment **3**

Common Event Types **3**

Risk Levels **3**

Related Resources **3**

This directory contains detailed implementation schemas for all 10 indicators in the Authority-Based vulnerability category.

Overview

Authority-based vulnerabilities exploit human tendencies to comply with perceived authority figures, bypass security for superiors, and defer responsibility within hierarchical structures.

Indicators

1. **[1.1] Unquestioning compliance with apparent authority** - Monitoring compliance patterns with authority-domain patterns
2. **[1.2] Diffusion of responsibility in hierarchical structures** - Tracking ticket ownership transitions
3. **[1.3] Authority Figure Impersonation Susceptibility** - Correlating SPF/DKIM failures with user interactions

4. **[1.4] Bypassing Security for Superior's Convenience** - Exception grant rates during executive presence
5. **[1.5] Fear of Contradiction in Security Decisions** - Linguistic analysis for urgency markers
6. **[1.6] Status Hierarchy Security Deference** - Organizational hierarchy depth as weighting factor
7. **[1.7] Technical Jargon Authority Claims** - Jargon density exceeding domain baselines
8. **[1.8] Executive Exception Normalization** - Cumulative bypass count over rolling windows
9. **[1.9] Authority-Based Social Proof** - Graph analysis on compliance cascades
10. **[1.10] Crisis Authority Escalation** - Enhanced monitoring during elevated threat levels

Implementation Schema

Each indicator file follows the **OFTLISRV** framework:

- **O** - Observables: What behavioral patterns to detect
- **F** - Data Sources: Which logs/APIs to query (AD, email, PAM, SIEM)
- **T** - Temporality: Time windows, persistence thresholds, decay functions
- **L** - Detection Logic: Formulas combining deterministic + statistical methods
- **I** - Interdependencies: Bayesian correlations with other indicators
- **S** - Thresholds: Alert severity levels (green/yellow/red)
- **R** - Responses: Recommended mitigation actions
- **V** - Validation: Human audit protocols

Key Data Sources

- **Active Directory**: Authentication logs, privilege escalation events
- **Email Gateway**: Message headers, SPF/DKIM verification, sender domains
- **PAM Systems**: Privileged access requests, approval chains
- **SIEM**: Correlation of events across sources
- **Ticketing Systems**: Incident ownership transfers

Detection Approach

Compliance Rate Function

```
C_r = N_executed / N_requested
```

Where requests originate from authority_domain patterns.

Bayesian Authority Legitimacy

```
P(legitimate|factors) = P(factors|legitimate) × P(legitimate) / P(factors)
```

Factors: time_of_day, request_pattern, verification_attempted

Baseline Establishment

Authority indicators require 30-day baseline period to establish: - Normal compliance rates per user/department - Typical exception request patterns - Legitimate executive communication patterns

Common Event Types

Events that trigger authority-based indicators: - `authority_request` → 1.1, 1.3, 1.9 - `approval_chain_modification` → 1.2 - `executive_exception_granted` → 1.4, 1.8 - `technical_override` → 1.7

Risk Levels

- **Low** (0-0.33): Normal hierarchical compliance patterns
- **Medium** (0.34-0.66): Elevated compliance without verification
- **High** (0.67-1.00): Systematic authority exploitation detected

Related Resources

- **Dense Foundation**: `/foundation docs/core/en-US/` - Section on Authority vulnerabilities
- **Correlation Rules**: `/src/correlation-rules/cpf_authority_detection.spl`
- **Dashboard**: `/dashboard/soc/` - Real-time visualization
- **Simulator**: `/dashboard/simulator/` - Test event generation