Categoria 1: Vulnerabilità basate sull'Autorità

Contents

Questa directory contiene schemi di implementazione dettagliati per tutti i 10 indicatori nella categoria di vulnerabilità basata sull'Autorità.

Panoramica

Le vulnerabilità basate sull'autorità sfruttano le tendenze umane a conformarsi alle figure di autorità percepite, a bypassare la sicurezza per superiori e a deferire la responsabilità all'interno di strutture gerarchiche.

Indicatori

1. **[1.1] Conformità incondizionata all'autorità apparente** - Monitoraggio dei modelli di conformità con modelli di dominio dell'autorità
2. **[1.2] Diffusione della responsabilità in strutture gerarchiche** - Tracciamento delle transizioni di proprietà dei ticket
3. **[1.3] Suscettibilità all'impersonificazione della figura di autorità** - Correlazione dei fallimenti SPF/DKIM con interazioni utente

4. [**1.4**] **Bypass della sicurezza per comodità del superiore** - Tassi di concessione di eccezioni durante la presenza di dirigenti
5. [**1.5**] **Paura della contraddizione nelle decisioni di sicurezza** - Analisi linguistica per marcatori di urgenza
6. [**1.6**] **Deferenza della sicurezza della gerarchia di stato** - Profondità della gerarchia organizzativa come fattore di ponderazione
7. [**1.7**] **Reclami di autorità del gergo tecnico** - Densità del gergo che supera i baseline del dominio
8. [**1.8**] **Normalizzazione dell'eccezione esecutiva** - Conteggio cumulativo del bypass su finestre scorrevoli
9. [**1.9**] **Prova sociale basata sull'autorità** - Analisi grafica sui cascate di conformità
10. [**1.10**] **Escalation dell'autorità in crisi** - Monitoraggio migliorato durante livelli di minaccia elevati

Schema di implementazione

Ogni file di indicatore segue il framework **OFTLISRV**:

- **O** - Osservabili: Quali modelli comportamentali rilevare
- **F** - Fonti dati: Quali log/API interrogare (AD, email, PAM, SIEM)
- **T** - Temporalità: Finestre temporali, soglie di persistenza, funzioni di decadimento
- **L** - Logica di rilevamento: Formule che combinano metodi deterministici + statistici
- **I** - Interdipendenze: Correlazioni bayesiane con altri indicatori
- **S** - Soglie: Livelli di gravità degli avvisi (verde/giallo/rosso)
- **R** - Risposte: Azioni di mitigazione consigliate
- **V** - Convalida: Protocolli di audit umani

Fonti dati chiave

- **Active Directory**: Log di autenticazione, eventi di escalation dei privilegi
- **Gateway di posta**: Intestazioni dei messaggi, verifica SPF/DKIM, domini mittente
- **Sistemi PAM**: Richieste di accesso privilegiato, catene di approvazione
- **SIEM**: Correlazione di eventi tra le fonti
- **Sistemi di ticketing**: Trasferimenti di proprietà degli incidenti

Approccio al rilevamento

Funzione del tasso di conformità

```
C_r = N_eseguiti / N_richiesti
```

Dove le richieste provengono da modelli di authority_domain.

Legittimità dell'autorità bayesiana

```
P(legittimo|fattori) = P(fattori|legittimo) × P(legittimo) / P(fattori)
```

Fattori: time_of_day, request_pattern, verification_attempted

Stabilimento del baseline

Gli indicatori di autorità richiedono un periodo di baseline di 30 giorni per stabilire: - Tassi di conformità normali per utente/dipartimento - Modelli di richiesta di eccezione tipici - Modelli di comunicazione esecutiva legittimi

Tipi di evento comuni

Eventi che attivano indicatori basati sull'autorità: - `authority_request` → 1.1, 1.3, 1.9 - `approval_chain_modification` → 1.2 - `executive_exception_granted` → 1.4, 1.8 - `technical_override` → 1.7

Livelli di rischio

- **Basso** (0-0.33): Modelli di conformità gerarchica normali
- **Medio** (0.34-0.66): Conformità elevata senza verifica
- **Alto** (0.67-1.00): Sfruttamento sistematico dell'autorità rilevato

Risorse correlate

- **Fondamento denso**: `/foundation docs/core/it-IT/` - Sezione su vulnerabilità di autorità
- **Regole di correlazione**: `/src/correlation-rules/cpf_authority_detection.spl`
- **Dashboard**: `/dashboard/soc/` - Visualizzazione in tempo reale
- **Simulatore**: `/dashboard/simulator/` - Generazione di eventi di test