

Contents

[7.6] Overconformità da Risposta di Appeasement 1

[7.6] Overconformità da Risposta di Appeasement

1. Definizione Operativa: Una risposta indotta da stress per placciare figure di autorità o sistemi seguendo le procedure a un grado eccessivo e senza pensiero critico, spesso bypassando il pensiero critico e portando a errori (es. approvare una richiesta rischiosa da un superiore senza scrutinio).

2. Metrica Principale e Algoritmo:

- **Metrica: Tasso di Approvazione Cieca (BAR).** Formula: $BAR = \frac{N_approvals_with_short_review}{N_total_approvals}$.
- **Pseudocodice:**

python

```
def calculate_bar(employee_id, start_date, end_date):
    # Ottenere tutte le azioni di approvazione eseguite dall'impiegato (es. richieste di approvazione)
    approvals = query_iam_system(employee_id, start_date, end_date)

    blind_approvals = 0
    for approval in approvals:
        # Definire "revisione breve" come meno di 60 secondi tra la richiesta e l'approvazione
        review_time = approval.approval_time - approval.request_time
        if review_time < timedelta(seconds=60):
            blind_approvals += 1

    total_approvals = len(approvals)
    if total_approvals > 0:
        bar = blind_approvals / total_approvals
    else:
        bar = 0
    return bar
```

- **Soglia di Allerta:** $BAR > 0.3$ (30% delle approvazioni vengono fatte in meno di 60 secondi).

3. Fonti di Dati Digitali (Input dell'Algoritmo):

- **API del Sistema di Gestione dell'Identità e dell'Accesso (IAM)** (es. SailPoint, Okta Workflows): approver, request_time, decision_time, decision.
- **Registri del Sistema di Gestione dell'Accesso Privilegiato (PAM).**

4. Protocollo di Audit Umano-Umano: Audit campione delle richieste approvate. In un'intervista, presentare una richiesta approvata di recente e chiedere: “Puoi illustrarmi i fattori che hai considerato prima di approvare questa?” “Hai sentito qualche pressione nel fare questa approvazione rapidamente?”

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare un periodo “cooling-off” obbligatorio di 2

minuti per tutte le approvazioni ad alto rischio. Richiedere un campo di commento obbligatorio per qualsiasi approvazione.

- **Mitigazione Umana/Organizzativa:** Formazione sull'assertività e sulla governance della sicurezza. Rafforzare che l'autorità del team di sicurezza nel negare le richieste è supportata dalla leadership.
- **Mitigazione di Processo:** Introdurre il principio dei “quattro occhi” per le approvazioni provenienti da figure di elevata autorità.