

Contents

[10.6] Negazione del Rinoceronte Grigio	1
---	---

[10.6] Negazione del Rinoceronte Grigio

1. Definizione Operativa: Lo stato di ignorare consapevolmente o sottoprioritizzare una minaccia altamente probabile e ad alto impatto che è visibilmente in carica (un “Rinoceronte Grigio”). Misurato dall’intervallo di tempo tra l’identificazione della minaccia e l’azione di mitigazione.

2. Metrica Principale e Algoritmo:

- **Metrica:** Ritardo di Risposta per Rischi Critici (RLCR). Formula: $RLCR = \text{Data_Inizio_Mitigazione} - \text{Data_Identificazione_Rischio}$ (giorni).

- **Pseudocodice:**

python

```
def calculate_rlcrrisk_db):
    # Ottieni tutti i rischi ad alto impatto e alta probabilità che ora sono chiusi
    gray_rhino_risks = query_risks(impact='High', probability='High', status='Closed')
    total_lag = 0
    count = 0

    for risk in gray_rhino_risks:
        id_date = risk.identified_date
        mitigation_date = risk.mitigation_start_date

        if mitigation_date and id_date:
            lag = (mitigation_date - id_date).days
            total_lag += lag
            count += 1

    return total_lag / count if count > 0 else 0
```

- **Soglia di Avviso:** $RLCR > 180$ (giorni) (Sei mesi di ritardo nell’affrontare rischi critici noti).

3. Fonti Dati Digitali (Input dell’Algoritmo):

- **Registro dei Rischi / Piattaforma GRC:** (ad es. ServiceNow GRC, RSA Archer) campi: risk_id, description, impact, probability, identified_date, mitigation_start_date, status.

4. Protocollo di Audit Umano-Umano: Rivedi il registro dei rischi con il CISO e il consiglio. Per ogni rischio ad alto impatto e alta probabilità che è ancora aperto, chiedi: “Qual è il passo successivo specifico e più piccolo che stiamo intraprendendo per mitigare questo? Quale è la data per questo passo? Se non è una priorità, per favore giustifica perché il punteggio di impatto o probabilità è inesatto.”

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementa una dashboard che contrassegna automaticamente i rischi che soddisfano i criteri del “Rinoceronte Grigio” (Alto/Alto) e li evidenzia per la revisione della leadership senior.
- **Mitigazione Umana/Organizzativa:** Lega una parte dei bonus di performance dei dirigenti alla riduzione dell’RLCR per i rischi nel loro dominio.
- **Mitigazione dei Processi:** Istituisce una revisione trimestrale obbligatoria guidata dal CISO per tutti i rischi Alto/Alto, richiedendo un’accettazione formale o un piano di mitigazione dal proprietario aziendale responsabile.