# Contents

**[10.5] Cecità dei Cigni Neri** . . . . . 1

## [10.5] Cecità dei Cigni Neri

**1. Definizione Operativa:** L'incapacità di un'organizzazione di riconoscere o prepararsi per eventi estremi, ad alto impatto che sono statisticamente rari ma si trovano al di fuori del regno delle aspettative regolari. Misurato dalla mancanza di preparazione per scenari ad alto impatto e bassa probabilità.

**2. Metrica Principale e Algoritmo:**

- **Metrica:** Indice di Preparazione del Cigno Nero (BSPI). Questo è un punteggio composito (0-100) basato su una checklist di attività di preparazione. Formula: `BSPI = (Somma_Punteggi_Ponderati / Punteggio_Totale_Possibile) * 100`.
- **Pseudocodice:**

  python

  ```
  def calculate_bspi(preparedness_checklist):
      total_score = 0
      max_possible = 0

      for item in preparedness_checklist:
          # item ha: 'question', 'weight', 'score' (0-5)
          total_score += item['score'] * item['weight']
          max_possible += 5 * item['weight'] # assumendo punteggio massimo di 5 per elemento

      if max_possible == 0:
          return 0
      bspi = (total_score / max_possible) * 100
      return bspi
  ```

- **Soglia di Avviso:** `BSPI < 50` (Meno del 50% di preparazione per eventi estremi).

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

- **Piattaforma GRC:** Modulo di questionario o checklist in cui il team del CISO risponde e assegna punteggi a elementi come: "Abbiamo un playbook per uno zero-day nella nostra VPN primaria?" oppure "Abbiamo testato il ripristino dai backup dopo un attacco ransomware sul server di backup stesso?".

**4. Protocollo di Audit Umano-Umano:** Conduci una sessione di war-gaming facilitata con la leadership senior. Presenta uno scenario plausibile ma estremo (ad es. "Un attore statale ha compromesso i nostri server di compilazione e ha spedito software infetto a tutti i clienti"). Valuta la risposta non per la perfezione tecnica, ma per l'esistenza di qualsiasi piano e il processo decisionale.

**5. Azioni di Mitigazione Consigliate:**

- **Mitigazione Tecnica/Digitale:** Isola e proteggi rigorosamente i beni gioiello della corona con controlli estremi, assumendo che altre difese possano fallire.

- **Mitigazione Umana/Organizzativa:** Nomina un individuo senior come "Avvocato del Diavolo" il cui ruolo è sfidare le ipotesi e proporre scenari peggiori durante le riunioni di pianificazione.
- **Mitigazione dei Processi:** Integra uno scenario "cigno nero" nel programma annuale di test della risposta agli incidenti per testare la capacità di resilienza e improvvisazione dell'organizzazione.