Contents

[2.5] Sconto Iperbolico delle Minacce Future

1. Definizione Operativa: La tendenza cognitiva in cui il costo percepito di affrontare una minaccia potenziale futura è pesato come più significativo del costo futuro reale e scontato di una violazione, portando al differimento perpetuo delle azioni di mitigazione.

2. Metrica Principale e Algoritmo:

- **Metrica:** Indice di Differimento della Mitigazione (MDI). Formula: `MDI = (N_vulns_deferred / N_vulns_identified) * Average_Deferral_Time`.
- **Pseudocodice:**

  python

  ```
  def calculate_mdi(vulnerabilities):
      """
      vulnerabilities: Lista di oggetti vuln con campi: ['vuln_id', 'discovery_date', 'risk_
      """
      deferred_vulns = []
      total_vulns = len(vulnerabilities)

      for vuln in vulnerabilities:
          if vuln.planned_remediation_date and vuln.actual_remediation_date:
              # Se rimediato più tardi del previsto, è stato differito
              if vuln.actual_remediation_date > vuln.planned_remediation_date:
                  deferral_time = (vuln.actual_remediation_date - vuln.planned_remediation_d
                  deferred_vulns.append(deferral_time)

      if total_vulns > 0 and len(deferred_vulns) > 0:
          deferral_rate = len(deferred_vulns) / total_vulns
          avg_deferral_time = sum(deferred_vulns) / len(deferred_vulns)
          MDI = deferral_rate * avg_deferral_time
      else:
          MDI = 0

      return MDI
  ```

- **Soglia di Allarme:** `MDI > 7` (es. un pattern dove il 10% delle vuln sono differite di una media di 70 giorni, o il 20% di 35 giorni).

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

- **Piattaforma di Gestione delle Vulnerabilità (Qualys, Tenable):** API `vulnerabilities`. Campi: `discovered`, `severity`, `planned_remediation_date`, `remediated`.
- **Sistema di Ticketing (Jira, ServiceNow):** `issues` di tipo 'Risk Acceptance'. Campi: `created`, `risk_assessment.expiry_date`.

4. Protocollo di Audit da Persona a Persona: Esaminare i moduli di accettazione del rischio e i verbali delle riunioni dell'ultimo trimestre: "Qual era la logica per accettare questo rischio? È stata effettuata un'analisi costi-benefici che ha confrontato il costo della mitigazione ora vs. la potenziale perdita futura? Questo risultato è stato differito prima?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Configurare la piattaforma VM per escalare e riassegnare automaticamente le vulnerabilità la cui data di rimediazione pianificata è stata superata senza azione.
- **Mitigazione Umana/Organizzativa:** Addestrare i responsabili dei rischi su appropriate tecniche di valutazione quantitativa dei rischi, forzando una valutazione numerica del costo futuro.
- **Mitigazione dei Processi:** Implementare una politica in cui qualsiasi differimento di una vulnerabilità "alta" o "critica" richiede accettazione formale e vincolata dal tempo firmata da un responsabile dell'unità aziendale, con revisioni trimestrali obbligatorie.