Contents

[10.4] Allineamento del Modello Svizzero

1. Definizione Operativa: Uno stato in cui i buchi (lacune) in più livelli di difesa (tecnica, umana, processo) si allineano temporaneamente, consentendo a una minaccia di passare indenne. Questo viene misurato correlando i fallimenti in diversi domini di controllo.

2. Metrica Principale e Algoritmo:

- **Metrica:** Correlazione dei Fallimenti di Difesa (DFC). Formula: Per un dato incidente, `DFC = (Numero_Controlli_Falliti / Controlli_Totali_Rilevanti) * (1 / Tempo_Medio_Tra_Guasti)`. Un punteggio elevato indica che molti controlli hanno fallito in rapida successione.
- **Pseudocodice:**

  python

  ```
  def calculate_dfc(incident_id, controls_list):
      # Ottieni tutti gli eventi di fallimento del controllo correlati a questo incidente da
      control_failures = get_control_failures_for_incident(incident_id)

      num_failures = len(control_failures)
      total_relevant = len(controls_list) # ad es. tutti i controlli che dovrebbero aver fer

      # Calcola il tempo tra il primo e l'ultimo fallimento del controllo
      failure_times = sorted([f.time for f in control_failures])
      if num_failures > 1:
          time_window = (failure_times[-1] - failure_times[0]).total_seconds() / 60  # in mi
          mean_time_between = time_window / (num_failures - 1)
      else:
          mean_time_between = 0

      # Evita la divisione per zero
      if mean_time_between == 0:
          mean_time_between = 0.1

      dfc = (num_failures / total_relevant) * (1 / mean_time_between)
      return dfc
  ```

- **Soglia di Avviso:** `DFC > 1,0` (Rapporto elevato di controlli falliti in una finestra temporale molto breve).

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

- **SIEM:** Log da vari controlli di sicurezza (FW, EDR, Email Gateway, IAM) che mostrano messaggi `deny` o `alert` che sono stati bypassati.
- **Piattaforma GRC/Conformità:** (ad es. RSA Archer) per definire il `Controlli_Totali_Rilevanti` per un dato pattern di attacco.

4. Protocollo di Audit Umano-Umano: Durante una revisione post-incidente, usa una lavagna per mappare il percorso dell'attacco. Per ogni fase, chiedi: "Quale controllo era stato progettato per fermare questo? Perché ha fallito?" La mappa visuale mostrerà chiaramente l'"allineamento dei buchi" attraverso i livelli di difesa.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementa controlli che sono tecnicamente diversi (ad es. basati su firma + comportamentale) per ridurre la possibilità che un singolo difetto influenzi tutti i livelli.
- **Mitigazione Umana/Organizzativa:** Fornisci formazione incrociata agli operatori di controllo (ad es. team di rete, endpoint, cloud) per comprendere l'intera catena di difesa, non solo il loro silos.
- **Mitigazione dei Processi:** Rendi obbligatorie le revisioni di "difesa in profondità" per gli incidenti principali per identificare e correggere i fallimenti di controllo correlati.