Contents

[3.10] Conflitti di Gestione della Reputazione 1

[3.10] Conflitti di Gestione della Reputazione

1. Definizione Operativa: Il conflitto che sorge quando un individuo deve scegliere tra l'adesione ai protocolli di sicurezza (ad esempio, segnalare un errore) e l'esecuzione di un'azione che protegge la sua reputazione personale o professionale (ad esempio, nascondere l'errore), spesso portando a rischi di sicurezza che vengono occultati.

2. Metrica Principale e Algoritmo:

- **Metrica: Tasso di Offuscamento degli Incidenti (IOR)**. Formula: `IOR = N_nascosto / N_totale_stimato`, dove `N_nascosto` è il numero di incidenti trovati attraverso mezzi forensici che non sono stati auto-segnalati.
- **Pseudocodice:**

  python

  ```
  # Questo algoritmo è intrinsecamente retrospettivo e probabilistico.
  def calculate_ior(reported_incidents, detected_incidents, period):
      """
      reported_incidents: Incidenti registrati tramite segnalazione ufficiale (ticketing).
      detected_incidents: Incidenti trovati tramite scansioni, audit, o segnalazioni esterne
      """
      # Trova gli incidenti che sono stati rilevati ma non segnalati
      hidden_incidents = set(detected_incidents) - set(reported_incidents)

      # Il vero totale è quello che abbiamo trovato tramite entrambi i canali
      estimated_total_incidents = set(reported_incidents) | set(detected_incidents)

      IOR = len(hidden_incidents) / len(estimated_total_incidents) if estimated_total_incide
      return IOR
  ```

- **Soglia di Allerta:** `IOR > 0.1` (Oltre il 10% degli incidenti non viene segnalato/nascosto).

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

- **Sistema di Ticketing (Jira, ServiceNow):** Fonte per `reported_incidents`. Campi: `incident_id`, `reporter`, `report_time`.
- **Log di Alert SIEM/SOC (Splunk, Elastic):** Fonte per `detected_incidents`. Campi: `alert_id`, `generation_time`, `severity`.
- **Log di Scansione delle Vulnerabilità (Qualys, Nessus):** Un'altra fonte per `detected_incidents`.

4. Protocollo di Audit Umano-Umano: Istituisci un processo formale di post-mortem blameless per tutti gli incidenti di sicurezza. La promessa esplicita di nessuna punizione per l'errore umano (tranne per l'intento malizioso) è fondamentale per scoprire le vere cause root e misurare il tasso di incidenti precedentemente nascosti.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementa controlli detective robusti (logging, monitoraggio, scansioni) che trovano automaticamente gli incidenti, riducendo l'opportunità di occultarli.
- **Mitigazione Umana/Organizzativa:** La leadership deve attivamente e ripetutamente promuovere una **cultura blameless**. Celebra e ricompensa i dipendenti che segnalano proattivamente i loro stessi errori o near-misses, inquadrandolo come un punto di forza che migliora la sicurezza organizzativa.
- **Mitigazione del Processo:** Formalizza il processo di post-mortem blameless. Assicurati che sia focalizzato sull'apprendimento e il miglioramento dei sistemi, non sull'assegnazione della colpa agli individui.