Contents

[4.6] Conformità Eccessiva Guidata dalla Colpa

1. Definizione Operativa: Una controriezione a un precedente fallimento di sicurezza o errore, portando a un'aderenza eccessivamente rigida ai protocolli, che può ostacolare l'efficienza operativa, creare attrito inutile e causare affaticamento degli avvisi da segnalazione eccessiva.

2. Metrica Principale e Algoritmo:

- **Metrica:** Procedural Friction Index (PFI). Formula: `PFI = (N_richieste_rifiutate + N_richieste_escalate) / N_richieste_totali`.
- **Pseudocodice:**

  python

  ```
  def calculate_pfi(access_logs, ticketing_system, team_id):
      """
      access_logs: Log di richieste di accesso (es. al sistema IAM)
      ticketing_system: Ticket per richieste di accesso o eccezioni di sicurezza
      """
      # Ottenere tutte le richieste di accesso effettuate dal team
      team_requests = query_requests(team_id)

      # Contare le richieste che sono state rifiutate o hanno richiesto un'escalation per l'
      rejected_or_escalated = [r for r in team_requests if r['status'] in ['rejected', 'esca

      pfi = len(rejected_or_escalated) / len(team_requests) if team_requests else 0
      return pfi
  ```

- **Soglia di Allarme:** `PFI > 0.4` (Oltre il 40% delle richieste sono rifiutate o richiedono escalation, indicando un'applicazione eccessivamente rigorosa).

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

- **Log del Sistema IAM:** (es. Azure AD, Okta) API per controllare i log di richiesta e approvazione di accesso.
- **Sistema di Ticketing (ServiceNow):** API per interrogare la cronologia del flusso di lavoro dei ticket di richiesta di accesso.

4. Protocollo di Audit Umano-su-Umano: Intervistare i membri del team dallo sviluppo e altri gruppi interni: "Come descriveresti il processo di ottenimento dell'accesso necessario o delle eccezioni dal team di sicurezza? Sembra collaborativo o avversariale?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare un sistema di accesso Just-In-Time (JIT) per ridurre la necessità di privilegi permanenti e eccezioni permanenti.
- **Mitigazione Umana/Organizzativa:** Fornire formazione al personale di sicurezza sul processo decisionale basato sul rischio piuttosto che sulla conformità binaria. Promuovere la collaborazione tra la sicurezza e altri team.

- **Mitigazione del Processo:** Rivedere e aggiornare le politiche di controllo dell'accesso per assicurare che siano allineate alle esigenze aziendali e non inutilmente restrittive.
