Contents

[2.3] Accettazione del Rischio Guidata dai Deadline

1. Definizione Operativa: Uno stato cognitivo in cui la pressione percepita di un deadline imminente causa al personale della sicurezza di eludere consapevolmente o scorciatoiare i protocolli di sicurezza per rispettare la timeline, accettando così un livello di rischio più elevato.

2. Metrica Principale e Algoritmo:

- **Metrica:** Tasso di Accettazione del Rischio per Deadline (DRAR). Formula: `DRAR = N_protocol_bypass / N_deadline_tasks`.
- **Pseudocodice:**

  python

  ```
  def calculate_drar(tasks, start_date, end_date):
      """
      tasks: Lista di oggetti task con campi: ['deadline', 'completed_at', 'security_checks_
      """
      bypass_count = 0
      total_deadline_tasks = 0

      for task in tasks:
          if task.deadline is not None and task.completed_at between start_date and end_date
              total_deadline_tasks += 1
              if task.security_checks_bypassed > 0: # Assumendo che sia un conteggio o un fl
                  bypass_count += 1

      if total_deadline_tasks > 0:
          DRAR = bypass_count / total_deadline_tasks
      else:
          DRAR = 0

      return DRAR
  ```

- **Soglia di Allarme:** `DRAR > 0.1` (ovvero, più del 10% dei compiti vicini a un deadline comportano bypass della sicurezza).

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

- **API di Gestione Progettuale (Jira, Asana):** Endpoint `issues` o `tasks`. Campi: `due_date`, `updated_at`, `status`, `labels` (es. `#security_waiver`).
- **Log della Pipeline CI/CD (Jenkins, GitLab):** Indice `pipeline_runs`. Campi: `duration`, `end_time`, `success`, `variables` (es. `SKIP_TESTS=true`).
- **Sistema di Controllo Versione (Git):** Messaggi di commit contenenti parole chiave come "hotfix", "bypass", "skip".

4. Protocollo di Audit da Persona a Persona: Condurre interviste retrospettive dopo un rilascio importante o un deadline di progetto: "Eri consapevole dei requisiti di sicurezza per il

compito X? Quali compromessi hai sentito di dover fare per rispettare il deadline? Hai formalmente documentato l'accettazione del rischio?" Incrociare le risposte con i log dei cambiamenti.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare guardrail automatizzati nelle pipeline CI/CD che impediscono di bypassare i passaggi di sicurezza critici (es. SAST, rilevamento segreti) senza approvazione obbligatoria e registrata da un responsabile di sicurezza separato.
- **Mitigazione Umana/Organizzativa:** Incorporare "pressione di programmazione" come fattore di rischio formale nelle sessioni di pianificazione progettuale e threat modeling. Addestrare i manager a riconoscere e mitigare questa pressione.
- **Mitigazione dei Processi:** Istituire una procedura formale e snella di accettazione del rischio che deve essere completata e registrata prima che qualsiasi controllo di sicurezza possa essere bypassato, creando responsabilità e una pista di audit.