Contents

[10.2] Fattori Scatenanti dei Fallimenti a Cascata 1

[10.2] Fattori Scatenanti dei Fallimenti a Cascata

1. Definizione Operativa: Uno stato in cui un fallimento in un sistema o processo avvia una sequenza di fallimenti nei sistemi interdipendenti, portando a un crollo della sicurezza su larga scala. Questo viene misurato dalla velocità e dalla portata della propagazione dell'incidente.

2. Metrica Principale e Algoritmo:

- **Metrica:** Tasso di Propagazione a Cascata (CPR). Formula: `CPR = (Numero_Sistemi_Colpiti / Sistemi_Totali_Interdipendenti) / Tempo_Contenimento (ore)`.
- **Pseudocodice:**

  python

  ```
  def calculate_cpr(incident_id, systems_list):
      # Ottieni il sistema iniziale dal primo avviso dell'incidente
      initial_alert = get_initial_alert(incident_id)
      initial_system = initial_alert.affected_system

      # Ottieni tutti i sistemi unici colpiti nella timeline dell'incidente
      timeline_alerts = get_incident_alerts(incident_id)
      affected_systems = set(alert.affected_system for alert in timeline_alerts)

      # Ottieni il tempo tra il primo avviso e la chiusura dell'incidente
      time_to_contain = timeline_alerts[-1].time - initial_alert.time

      # Calcola il rapporto di sistemi colpiti a sistemi totali interconnessi
      total_interconnected = get_interconnected_systems(initial_system, systems_list)
      propagation_ratio = len(affected_systems) / len(total_interconnected)

      # Evita la divisione per zero
      if time_to_contain.total_hours() == 0:
          time_to_contain_hours = 0.1
      else:
          time_to_contain_hours = time_to_contain.total_hours()

      cpr = propagation_ratio / time_to_contain_hours
      return cpr
  ```

- **Soglia di Avviso:** `CPR > 0,05` (cioè, più del 5% dei sistemi interconnessi sono interessati per ora di tempo di contenimento).

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

- **API CMDB:** (ad es. ServiceNow) per mappare le dipendenze dei sistemi (relazioni `depends_on`, `connected_to`).

- **SIEM/SOAR:** (ad es. Splunk ES, Splunk Phantom) per ottenere la timeline dell'incidente (campi `incident_id`, `alert_time`, `affected_system` da eventi notabili).

4. Protocollo di Audit Umano-Umano: Condotta un esercizio di tabletop o una retrospettiva su un incidente importante passato. Chiedi al team: "Descriveteci in dettaglio la sequenza dei fallimenti. Il compromesso di un sistema ha direttamente portato al compromesso di un altro? Con quale velocità si è verificata la propagazione, e cosa infine l'ha fermata?" L'obiettivo è mappare la catena dei fallimenti e identificare i singoli punti di guasto.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementa playbook di contenimento automatizzati nella piattaforma SOAR per isolare i sistemi compromessi sulla base di grafici delle dipendenze predefiniti.
- **Mitigazione Umana/Organizzativa:** Addestra i responditori di incidenti sul riconoscimento delle cascate e sulla prioritizzazione del contenimento, con focus sui "punti di costrizione" critici nell'architettura del sistema.
- **Mitigazione dei Processi:** Rendi obbligatorie le revisioni architettoniche per i nuovi sistemi per garantire che siano progettati con l'isolamento dei guasti in mente (ad es. bulkhead, interruttori automatici).