Contents

[7.5] Paralisi da Risposta di Blocco

1. Definizione Operativa: Uno stato indotto da stress di sovraccarico cognitivo e indecisione in cui un analista è incapace di iniziare o continuare un'azione di risposta di sicurezza, spesso durante un incidente critico, portando a ritardi pericolosi.

2. Metrica Principale e Algoritmo:

- **Metrica: Ritardo nella Risposta agli Incidenti (IRL)**. Formula: `IRL = timestamp(first_action) - timestamp(incident_detection)`.
- **Pseudocodice:**

  python

  ```
  def calculate_irl(incident_id):
      # Ottenere il tempo di creazione dell'incidente da SOAR/SIEM
      incident = query_incident_db(incident_id)
      detection_time = incident.created_time

      # Ottenere il timestamp della prima azione significativa (es. riconoscimento dell'avvi
      first_action_log = query_soar_playbook_logs(incident_id).first()
      if first_action_log:
          action_time = first_action_log.timestamp
          irl = action_time - detection_time
          return irl  # in minuti
      else:
          return None  # Nessuna azione intrapresa
  ```

- **Soglia di Allerta:** `IRL > 15` minuti per un incidente di gravità **critica**.

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

- **Piattaforma SOAR (es. Splunk Phantom, XSOAR):** `incident_id`, `created_time`, `playbook_execution_logs`.
- **SIEM (es. Elastic SIEM):** `event.ingested`, `event.kind:alert`.

4. Protocollo di Audit Umano-Umano: Eseguire simulazioni da tavolo e misurare il tempo fino alla prima risposta. Condurre un'intervista di revisione post-incidente: "Cosa stava passando per la tua mente nei primi minuti dopo l'attivazione dell'avviso?" "C'era qualcosa di poco chiaro o confuso sulla procedura?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare e rendere obbligatorio l'uso di playbook SOAR che forniscono guida passo-passo, riducendo il carico cognitivo necessario per decidere cosa fare per primo.
- **Mitigazione Umana/Organizzativa:** Formazione di inoculazione dello stress attraverso esercitazioni realistiche e ad alta fedeltà.

- **Mitigazione di Processo:** Definire e fare drills su un chiaro protocollo “primi 5 minuti” per diversi tipi di incidenti. Istituire un sistema di coppie in cui due analisti sono assegnati a rispondere agli incidenti critici.