Contents

[7.7] Visione Tunnel Indotta da Stress 1

[7.7] Visione Tunnel Indotta da Stress

1. Definizione Operativa: Un restringimento cognitivo dell'attenzione sotto stress, in cui un analista si concentra eccessivamente su un aspetto singolo di una minaccia mentre manca di spunti contestuali più ampi o di eventi correlati, potenzialmente portando a una diagnosi errata dell'incidente.

2. Metrica Principale e Algoritmo:

- **Metrica: Punteggio di Punto Cieco Contestuale (CBS)**. Formula: `CBS = 1 - (N_correlated_events_linked / N_total_correlated_events)`.
- **Pseudocodice:**

  python

  ```
  def calculate_cbs(incident_id):
      # Ottenere l'avviso/evento primario dell'incidente
      primary_event = get_primary_event(incident_id)

      # Utilizzare le regole di correlazione SIEM per trovare eventi comunemente correlati (
      correlated_events = query_siem(f'search NOT incident_id:{incident_id} AND (src_ip:{pri

      # Verificare le note di indagine dell'incidente per menzioni di questi eventi correlat
      investigation_notes = get_incident_notes(incident_id)
      events_linked = 0
      for event in correlated_events:
          if event.id in investigation_notes:
              events_linked += 1

      total_correlated = len(correlated_events)
      if total_correlated > 0:
          cbs = 1 - (events_linked / total_correlated)
      else:
          cbs = 0
      return cbs
  ```

- **Soglia di Allerta:** `CBS > 0.8` per un incidente **critico** (analista ha mancato più dell'80% degli eventi correlati).

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

- **SIEM (es. Splunk ES):** Dati del modello `Incident_Review`, `notable_events`.
- **API del Sistema di Ticketing (es. ServiceNow SecOps):** `incident_id`, `work_notes`.

4. Protocollo di Audit Umano-Umano: Durante una revisione post-incidente, presentare l'analista con la cronologia completa degli eventi correlati e chiedere: "Vedendo questa immagine completa, avresti investigato diversamente?" "Cosa ti ha impedito di vedere questi altri eventi durante l'incidente?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Migliorare gli strumenti SIEM e SOAR per suggerire e visualizzare automaticamente gli eventi potenzialmente correlati durante un'indagine.
- **Mitigazione Umana/Organizzativa:** Formazione incrociata degli analisti su diversi domini tecnologici per allargare la loro prospettiva.
- **Mitigazione di Processo:** Rendere obbligatorio un meeting "step-back" 30 minuti in un'esercitazione di risposta agli incidenti critici per rivedere l'ipotesi e assicurare che il team non sia bloccato su una singola traccia.