Contents

[2.9] Finestre di Sfruttamento del Cambio di Turno

1. Definizione Operativa: Un tipo specifico di vulnerabilità temporale causato dall'attrito intrinseco, dalla distrazione e dal potenziale di miscomunicazione durante il periodo di passaggio tra due turni di sicurezza, portando agli allarmi di essere mancati o agli incidenti di essere gestiti male.

2. Metrica Principale e Algoritmo:

- **Metrica:** Tasso di Perdita del Cambio di Turno (SCDR). Formula: `SCDR = N_alerts_during_change / N_alerts_total (per la stessa gravità)`.
- **Pseudocodice:**

  python

  ```
  def calculate_scdr(alerts, shift_change_start, shift_change_duration_minutes):
      """
      alerts: Lista di oggetti allarme con ['timestamp', 'severity', 'status']
      """
      total_alerts = len(alerts)
      dropped_during_change = 0

      change_end = shift_change_start + timedelta(minutes=shift_change_duration_minutes)

      for alert in alerts:
          # Verificare se l'allarme è arrivato durante la finestra di cambio e non è stato r
          if shift_change_start <= alert.timestamp <= change_end:
              if alert.status == "new" or alert.status == "closed" and alert.resolution_note
                  dropped_during_change += 1

      if total_alerts > 0:
          SCDR = dropped_during_change / total_alerts
      else:
          SCDR = 0

      return SCDR
  ```

- **Soglia di Allarme:** `SCDR > 0.15` (Oltre il 15% degli allarmi che arrivano durante il cambio di turno non sono gestiti adeguatamente).

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

- **SIEM (Splunk ES):** Indice `notable_events`. Campi: `_time`, `status`, `owner`.
- **SOAR (Phantom, XSOAR):** `playbook_runs` per vedere se gli allarmi attivati durante il cambio di turno sono stati elaborati più tardi degli altri.

4. Protocollo di Audit da Persona a Persona: Osservare direttamente un cambio di turno. Successivamente, intervistare sia l'analista in arrivo che quello in partenza: "Quali allarmi erano

aperti? Sono stati tutti discussi? C'era confusione sulla proprietà o sui prossimi passi?" Esaminare le note di passaggio nel sistema di ticketing.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare una "modalità di passaggio" tecnica nel dashboard SOC che assegna automaticamente tutti gli allarmi non riconosciuti ad alta gravità al responsabile del turno in arrivo 30 minuti prima della fine di un turno.
- **Mitigazione Umana/Organizzativa:** Obbligare una sovrapposizione minima di 30 minuti tra turni dedicati esclusivamente al processo di passaggio. Usare un modello di passaggio standardizzato.
- **Mitigazione dei Processi:** Formalizzare la "regola dei due uomini" per gli allarmi critici durante il cambio di turno: sia l'analista in arrivo che quello in partenza devono verbalmente confermare lo stato e il piano d'azione per qualsiasi allarme di gravità "alta" o "critica" prima che il cambio di turno sia considerato completo.