Contents

[2.8] Lacune della Sicurezza nei Weekend/Giorni Festivi

1. Definizione Operativa: Una riduzione sistematica della postura di sicurezza, della vigilanza del monitoraggio e della prontezza di risposta durante i fine settimana e i giorni festivi organizzativi, spesso dovuta a uno staffing scheletrico.

2. Metrica Principale e Algoritmo:

- **Metrica:** Tempo Medio di Risposta nel Fine Settimana (W-MTTR). Confrontare con MTTR Settimanale. Formula: `W-MTTR = MTTR_weekend - MTTR_weekday`.
- **Pseudocodice:**

  python

  ```
  def calculate_wmttr(incidents):
      """
      incidents: Lista di incidenti con ['detection_time', 'containment_time', 'is_weekend']
      """
      weekday_times = []
      weekend_times = []

      for inc in incidents:
          if inc.containment_time: # Assicurare che l'incidente sia stato contenuto
              response_time = (inc.containment_time - inc.detection_time).total_seconds() /
              if inc.is_weekend:
                  weekend_times.append(response_time)
              else:
                  weekday_times.append(response_time)

      mttr_weekday = sum(weekday_times) / len(weekday_times) if weekday_times else 0
      mttr_weekend = sum(weekend_times) / len(weekend_times) if weekend_times else 0

      W_MTTR_delta = mttr_weekend - mttr_weekday
      return W_MTTR_delta
  ```

- **Soglia di Allarme:** `W-MTTR > 4` (Il tempo di risposta medio è più di 4 ore più lento nei fine settimana).

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

- **SOAR / Ticketing (ServiceNow):** Tabella `incident`. Campi: `opened_at`, `closed_at`. Usare `opened_at` per determinare se giorno feriale/fine settimana.
- **XDR / EDR (CrowdStrike, SentinelOne):** API `detections`. Campo: `status`, `last_update` per calcolare il tempo di contenimento.

4. Protocollo di Audit da Persona a Persona: Esaminare il roster di reperibilità e i rapporti di incidenti degli ultimi tre fine settimana/giorni festivi: "Quanti analisti erano di reperibilità? Quale era l'SLA per la risposta iniziale? Ci sono stati incidenti in cui il tempo di risposta ha

superato l'SLA?" Intervistare lo staff di reperibilità sul loro carico di lavoro e lo stress durante questi periodi.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Potenziare i playbook di contenimento automatizzato per agire più aggressivamente durante i fine settimana per compensare la risposta umana più lenta (es. isolare automaticamente gli endpoint che mostrano determinate minacce ad alta fiducia).
- **Mitigazione Umana/Organizzativa:** Implementare un modello follow-the-sun o assumere personale dedicato per il fine settimana. Offrire compensi premium per la reperibilità nei fine settimana per garantire l'impegno.
- **Mitigazione dei Processi:** Definire e comunicare SLA chiari e separati per i fine settimana/giorni festivi. Condurre esercitazioni trimestrali di tabletop che simulano un importante incidente che inizia in una festa.