Contents

[2.8] Weekend/Holiday Security Lapses

1. Operational Definition: A systemic reduction in security posture, monitoring vigilance, and response readiness during weekends and organizational holidays, often due to skeletal staffing.

2. Main Metric & Algorithm:

- **Metric:** Weekend Mean Time to Respond (W-MTTR). Compare to Weekly MTTR. Formula: `W-MTTR = MTTR_weekend - MTTR_weekday`.
- **Pseudocode:**

  python

  ```
  def calculate_wmttr(incidents):
      """
      incidents: List of incidents with ['detection_time', 'containment_time', 'is_weekend']
      """
      weekday_times = []
      weekend_times = []

      for inc in incidents:
          if inc.containment_time: # Ensure incident was contained
              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
  ```

- **Alert Threshold:** `W-MTTR > 4` (Average response time is more than 4 hours slower on weekends).

3. Digital Data Sources (Algorithm Input):

- **SOAR / Ticketing (ServiceNow):** `incident` table. Fields: `opened_at`, `closed_at`. Use `opened_at` to determine weekday/weekend.
- **XDR / EDR (CrowdStrike, SentinelOne):** `detections` API. Field: `status`, `last_update` to calculate containment time.

4. Human-to-Human Audit Protocol: Review the on-call roster and incident reports from the last three weekends/holidays: "How many analysts were on call? What was the SLA for initial response? Were there any incidents where the response time exceeded SLA?" Interview on-call staff about their workload and stress during these periods.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Enhance automated containment playbooks to act more aggressively during weekends to compensate for slower human response (e.g., automatically isolate endpoints exhibiting certain high-confidence threats).
- **Human/Organizational Mitigation:** Implement a follow-the-sun model or hire dedicated weekend staff. Offer premium compensation for on-call weekends to ensure engagement.
- **Process Mitigation:** Define and communicate clear, separate SLAs for weekends/holidays. Conduct quarterly tabletop exercises that simulate a major incident starting on a holiday.