# Contents

## [2.7] Time-of-Day Vulnerability Windows

**1. Operational Definition:** Predictable periods of reduced security monitoring or responsiveness that occur at the same time each day (e.g., during shift changes, lunch hours), creating recurring attack opportunities.

**2. Main Metric & Algorithm:**

- **Metric:** Recurring Gap Score (RGS). Formula: `RGS = (N_incidents_during_window / N_hours_in_window) / (N_incidents_outside / N_hours_outside)`.
- **Pseudocode:**

  python

```
def calculate_rgs(incidents, start_time, end_time, analysis_period_days):
    """
    incidents: List of incidents with timestamps.
    window: e.g., ('11:00', '13:00') for lunch window, or ('08:50', '09:10') for shift cha
    """
    window_incidents = 0
    outside_incidents = 0
    total_hours_in_window = (end_time - start_time).hours * analysis_period_days
    total_hours_outside = (24 * analysis_period_days) - total_hours_in_window

    for incident in incidents:
        if start_time <= incident.time.time() <= end_time:
            window_incidents += 1
        else:
            outside_incidents += 1

    # Calculate incident rates per hour
    rate_in_window = window_incidents / total_hours_in_window
    rate_outside = outside_incidents / total_hours_outside

    if rate_outside > 0:
        RGS = rate_in_window / rate_outside
    else:
        RGS = float('inf') # Handle division by zero

    return RGS
```

- **Alert Threshold:** `RGS > 1.5` (Incident rate during the window is 50% higher than the baseline rate).

**3. Digital Data Sources (Algorithm Input):**

- **SIEM (Splunk, Elastic):** `notable_events` or `incidents` index. Query for `| bucket _time span=1h | stats count by _time`.
- **SOAR / Ticketing (ServiceNow):** `incident` table. Fields: `opened_at`.
- **Active Directory Logs:** `4768` (Kerberos TGS requested) or `4624` (logon) events, looking for spikes during off-hours.

**4. Human-to-Human Audit Protocol:** Review the shift handover procedure: "Is there a documented 15-minute overlap period? Is there a process for monitoring during lunch breaks? Who is formally responsible for coverage during these times?" Observe a handover.

**5. Recommended Mitigation Actions:**

- **Technical/Digital Mitigation:** Configure automated playbooks to trigger higher severity or additional notifications for alerts detected during known vulnerability windows.
- **Human/Organizational Mitigation:** Implement mandatory overlapping shifts to ensure continuous coverage. Create a formal "lunch cover" rotation within the team.
- **Process Mitigation:** Document and enforce a strict shift handover protocol that includes a verbal briefing and a review of open high-severity alerts. Schedule critical system patches outside of these windows.