Contents

[2.6] Temporal Exhaustion Patterns

1. Operational Definition: A state of diminished cognitive capacity and security vigilance that predictably occurs at certain times during a work period (e.g., just before a break, end of a long shift), leading to an increase in errors.

2. Main Metric & Algorithm:

- **Metric:** Exhaustion Error Rate (EER). Formula: `EER = N_errors_last_hour / N_errors_total`.

- **Pseudocode:**

  python

  ```python
  def calculate_eer(events, shift_start, shift_duration_hours):
      """
      events: List of error/incident objects with a timestamp.
      Example: SIEM alerts falsely closed, failed login attempts from SOC analysts, deployme
      """
      total_errors = len(events)
      # Get errors from the last hour of the shift
      errors_last_hour = [e for e in events if e.timestamp > (shift_start + shift_duration_h

      if total_errors > 0:
          EER = len(errors_last_hour) / total_errors
      else:
          EER = 0

      return EER
  ```

- **Alert Threshold:** `EER > 0.3` (More than 30% of errors occur in the last hour of a shift).

3. Digital Data Sources (Algorithm Input):

- **SIEM (Splunk, Elastic):** Query for (`event_type="alert" AND status="closed" AND resolution="false_positive"`) by analyst, grouped by hour of their shift.
- **Access Logs:** `vpn` or `bastion_host` logs for failed login attempts by SOC analysts, grouped by time of day.
- **CI/CD Logs:** Failed pipeline runs or rollbacks, analyzed by the time of day they were initiated.

4. Human-to-Human Audit Protocol: Anonymous survey to analysts: "On a scale of 1-5, how does your concentration and attention to detail feel in the last hour of your shift compared to the first hour?" Correlate responses with the quantitative metric.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement a "fatigue detection" rule in the SOAR platform that automatically escalates all alerts from the last hour of a shift to a secondary analyst for

peer review.

- **Human/Organizational Mitigation:** Mandate a fresh-eyes review for critical changes or alert closures proposed in the last hour of a shift. Adjust shift patterns to avoid long, uninterrupted periods on high-intensity tasks.
- **Process Mitigation:** Schedule critical maintenance and complex tasks outside of known exhaustion windows. Institute mandatory micro-breaks every 90 minutes.