Contents

[5.5] Context Switching Vulnerabilities

1. Operational Definition: The specific security errors that occur in the transition period *between* tasks, where cognitive resources are reallocating, leading to missed details or procedural shortcuts. This is the *result* of the degradation described in 5.4.

2. Main Metric & Algorithm:

- **Metric:** Post-Switch Error Rate (PSER). Formula: `PSER = (Number of errors made on an alert within M minutes of switching from a previous alert) / (Total number of alerts worked on after a switch)`.
- **Pseudocode:**

  python

  ```
  def calculate_pser(events, analyst_id, time_window_minutes=5):
      # Get analyst's event log, ordered by time
      analyst_events = get_events(assigned_to=analyst_id, sort='timestamp')
      error_count = 0
      total_switched_alerts = 0

      for i in range(1, len(analyst_events)):
          prev_event = analyst_events[i-1]
          current_event = analyst_events[i]

          # Check if the analyst switched to a different alert
          if current_event.alert_id != prev_event.alert_id:
              total_switched_alerts += 1
              # Check for an error (e.g., wrong classification) on the new alert within time
              subsequent_events = get_events_for_alert(current_event.alert_id, within_minute
              if any(e.action == 'misclassified' for e in subsequent_events):
                  error_count += 1

      return error_count / total_switched_alerts if total_switched_alerts > 0 else 0
  ```

- **Alert Threshold:** `PSER > 0.15` (More than 15% of context switches lead to a measurable error).

3. Digital Data Sources (Algorithm Input):

- **SOAR/SIEM Audit Logs:** As in 5.4, to track task switching.
- **Ticketing System & Incident Reports:** To identify errors (e.g., tickets reopened due to incorrect initial classification, post-mortem reports citing analyst error). This requires a defined "error" tagging system.

4. Human-to-Human Audit Protocol: During a team meeting, perform a retrospective on a recent incident that involved an initial misstep. Ask the team: "What was happening right before

this alert came in? Was anyone working on something else complex?" This can help identify if a context switch was a contributing factor.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Design SOAR playbooks to include a mandatory "context checklist" that pops up when an analyst first opens a high-severity alert, forcing a moment of focus.
- **Human/Organizational Mitigation:** Encourage a "30-second pause" ritual for analysts before beginning a new investigation to mentally reset.
- **Process Mitigation:** Institute a peer-review process for the initial classification of all high-severity alerts to catch errors introduced by rapid context switching.