Contents

[5.3] Information Overload Paralysis

1. Operational Definition: A cognitive state where an analyst is presented with such a volume of data or alerts that they become unable to process any of it effectively, leading to delayed or absent responses.

2. Main Metric & Algorithm:

- **Metric:** Alert Volume-to-Response Ratio (AVRR). Formula: `AVRR = (Number of Alerts Acknowledged or Closed) / (Total Number of Alerts Presented) per analyst per hour.`.

- **Pseudocode:**

  python

  ```
  def calculate_avrr(events, analyst_id, time_window_hours=1):
      # Get all events for the analyst and the time window
      start_time = now() - timedelta(hours=time_window_hours)
      analyst_events = get_events(assigned_to=analyst_id, start_time=start_time)

      total_alerts = len(analyst_events)
      if total_alerts == 0:
          return 1.0  # No alerts is 100% processing

      # Count alerts that were acted upon (acknowledged or closed)
      acted_alerts = len([e for e in analyst_events if e.status in ['in_progress', 'closed']

      return acted_alerts / total_alerts
  ```

- **Alert Threshold:** `AVRR < 0.3` (The analyst is acting on fewer than 30% of the alerts they receive in an hour).

3. Digital Data Sources (Algorithm Input):

- **SIEM (Splunk/Elasticsearch):** Primary source for raw event volume. Query: `index=sec_events assigned_to=$analyst_id` over a rolling time window.
- **SOAR/Ticketing System:** To determine the status (`new`, `in_progress`, `closed`) of each alert presented to the analyst.

4. Human-to-Human Audit Protocol: Observe an analyst's workstation during a peak period. Note visible signs of overwhelm (e.g., rapidly switching windows without focus, excessive sighing). Follow up with a question: "When the queue looks like this, what's your strategy for deciding what to work on first?" A response of "I don't know" or "I just pick one" indicates paralysis.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement and tune SIEM correlation rules to aggregate related low-fidelity alerts into single, higher-fidelity meta-alerts, reducing the total number of items in the queue.

- **Human/Organizational Mitigation:** Provide training on triage techniques and “first principles” for cutting through noise during overwhelming events.
- **Process Mitigation:** Establish a clear escalation protocol where an analyst can formally declare “overload”, triggering support from other team members or a shift lead.