Contents

[7.7] Stress-Induced Tunnel Vision

1. Operational Definition: A cognitive narrowing of attention under stress, where an analyst focuses excessively on a single aspect of a threat while missing larger contextual clues or correlated events, potentially leading to a misdiagnosis of the incident.

2. Main Metric & Algorithm:

- **Metric: Contextual Blind Spot Score (CBS)**. Formula: `CBS = 1 - (N_correlated_events_linked / N_total_correlated_events)`.
- **Pseudocode:**

  python

  ```
  def calculate_cbs(incident_id):
      # Get the primary alert/event of the incident
      primary_event = get_primary_event(incident_id)

      # Use SIEM correlation rules to find events that are commonly related (e.g., same sour
      correlated_events = query_siem(f'search NOT incident_id:{incident_id} AND (src_ip:{pri

      # Check the incident investigation notes for mentions of these correlated events
      investigation_notes = get_incident_notes(incident_id)
      events_linked = 0
      for event in correlated_events:
          if event.id in investigation_notes:
              events_linked += 1

      total_correlated = len(correlated_events)
      if total_correlated > 0:
          cbs = 1 - (events_linked / total_correlated)
      else:
          cbs = 0
      return cbs
  ```

- **Alert Threshold:** `CBS > 0.8` for a **critical** incident (analyst missed over 80% of correlated events).

3. Digital Data Sources (Algorithm Input):

- **SIEM (e.g., Splunk ES):** `Incident_Review` data model, `notable_events`.
- **Ticketing System API (e.g., ServiceNow SecOps):** `incident_id`, `work_notes`.

4. Human-To-Human Audit Protocol: During a post-incident review, present the analyst with the full timeline of correlated events and ask: "Seeing this full picture, would you have investigated differently?" "What prevented you from seeing these other events during the incident?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Enhance SIEM and SOAR tools to automatically suggest and visualize potentially correlated events during an investigation.
- **Human/Organizational Mitigation:** Cross-training analysts on different technology domains to broaden their perspective.
- **Process Mitigation:** Mandate a "step-back" meeting 30 minutes into a critical incident response to review the hypothesis and ensure the team isn't stuck on a single track.