Contents

[5.7] Working Memory Overflow

1. Operational Definition: The point at which the volume of information an analyst is trying to mentally track exceeds the capacity of their working memory (~7±2 items), leading to forgotten details, repeated queries, and inconsistent reasoning.

2. Main Metric & Algorithm:

- **Metric:** Information Redundancy Rate (IRR). Formula: `IRR = (Number of repeated queries for the same information within a single investigation session) / (Total number of queries in the session)`.
- **Pseudocode:**

  python

  ```
  def calculate_irr(investigation_session):
      # investigation_session: a list of search queries made by an analyst for a single aler
      total_queries = len(investigation_session)
      unique_queries = set()
      redundant_count = 0

      for query in investigation_session:
          normalized_query = normalize_query(query)  # Remove timestamps, user-specific bits
          if normalized_query in unique_queries:
              redundant_count += 1
          else:
              unique_queries.add(normalized_query)

      return redundant_count / total_queries
  ```

- **Alert Threshold:** `IRR > 0.1` (More than 10% of an analyst's queries are repeats of information they've already retrieved).

3. Digital Data Sources (Algorithm Input):

- **SIEM Query Logs:** Essential for this metric. Requires logging the full text of search queries executed by users. Query: `index=siem_audit user=$analyst_id sourcetype=search` and group by `alert_id`.

4. Human-to-Human Audit Protocol: Shadow an analyst during a complex investigation. Note if they frequently say things like "Wait, what was that IP again?" or "I already looked that up but I forgot." Observe if they use notepads or sticky notes excessively to compensate for memory limitations.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Encourage and train analysts to use the SIEM's built-in investigation notebook or session-tracking features to offload information from their mind.

- **Human/Organizational Mitigation:** Teach analysts to use structured note-taking frameworks (e.g., the SOARA model) to externalize their working memory.
- **Process Mitigation:** Design investigation playbooks to include steps for documenting key findings (IPs, hashes, usernames) in a dedicated section of the ticket as they are discovered, creating a shared "external brain."