Contents

[5.6] Cognitive Tunneling

1. Operational Definition: An intense focus on a single, often narrow, aspect of a security incident at the expense of a broader, more holistic view, causing the analyst to miss peripheral but critical information.

2. Main Metric & Algorithm:

- **Metric:** Investigation Breadth Index (IBI). Formula: `IBI = (Number of unique data sources queried per investigation) / (Duration of investigation in hours)`. A very low IBI suggests a narrow, tunnel-vision approach.
- **Pseudocode:**

  python

  ```
  def calculate_ibi(investigation_sessions):
      # investigation_sessions: a list of sessions, each containing 'start_time', 'end_time'
      ibi_scores = []
      for session in investigation_sessions:
          duration_hours = (session.end_time - session.start_time).total_seconds() / 3600
          unique_data_sources = set(session.data_sources_queried)
          ibi = len(unique_data_sources) / duration_hours
          ibi_scores.append(ibi)
      return np.median(ibi_scores)  # Use median to avoid skew from very short/long sessions
  ```

- **Alert Threshold:** `IBI < 0.8` (The analyst is querying fewer than one unique data source per hour on average during an investigation).

3. Digital Data Sources (Algorithm Input):

- **SIEM Query Logs:** The primary source. Query: `index=siem_audit user=$analyst_id action=search` to see which indexes/sourcetypes they are searching.
- **EDR/Network Tool Logs:** Audit logs from tools like CrowdStrike, Splunk UEBA, or Corelight to capture queries made directly to those platforms.
- **Ticketing System:** To get the timeframe of an investigation (from alert creation to resolution).

4. Human-to-Human Audit Protocol: Present an analyst with a complex incident case study. Ask them to verbalize their thought process and investigation plan. An auditor should listen for a narrow, linear approach (e.g., "I would look at the firewall logs and that's it") versus a broad one (e.g., "I'd check EDR, then netflow, then see if the user was phished…").

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Develop and promote pre-built investigation dashboards in the SIEM that automatically surface correlated data from multiple sources (e.g., endpoint, network, identity) for a given alert.

- **Human/Organizational Mitigation:** Training based on the "kill chain" or "MITRE ATT&CK" frameworks to encourage analysts to think broadly about the stages of an attack and the associated data sources.
- **Process Mitigation:** Incorporate a mandatory "peer bounce" step in the investigation process for critical incidents, where the analyst must briefly explain their findings and approach to a colleague to uncover potential blind spots.