Contents

[4.2] Anger-Induced Risk Taking

1. Operational Definition: A state where heightened anger leads security personnel to bypass protocols, make hasty decisions, or engage in aggressive retaliation against perceived threats, thereby increasing system instability and creating new attack surfaces.

2. Main Metric & Algorithm:

- **Metric:** Anger-Induced Action Ratio (AIAR). Formula: `AIAR = N_rapid_high_severity_actions / N_total_high_severity_actions`.
- **Pseudocode:**

  python

  ```
  def calculate_aiar(actions_log, user_id, time_window='1h'):
      """
      actions_log: List of dicts with keys ['user', 'action_type', 'severity', 'timestamp',
      """
      # Filter for the specific user's high-severity actions (e.g., block IP, quarantine dev
      user_actions = [a for a in actions_log if a['user'] == user_id and a['severity'] == 'h

      # Define a threshold for a "rapid" action (e.g., < 2 minutes from alert to action sugg
      rapid_action_threshold = 120  # seconds

      # Count actions performed faster than the threshold
      rapid_actions = [a for a in user_actions if a['time_to_execute'] < rapid_action_thresh

      # Calculate the ratio
      aiar = len(rapid_actions) / len(user_actions) if user_actions else 0
      return aiar
  ```

- **Alert Threshold:** `AIAR > 0.3` (More than 30% of high-sev actions are performed with minimal deliberation).

3. Digital Data Sources (Algorithm Input):

- **SOAR Platform Logs:** (e.g., Splunk Phantom, Cortex XSOAR) API to fetch playbook execution logs, including `user`, `action_name`, `start_time`, `end_time`, and severity tags from the triggering alert.
- **SIEM/Syslog:** Authentication and command logs from critical systems (e.g., firewall admin logs, EDR console logs) to capture manual, out-of-band actions.

4. Human-to-Human Audit Protocol: Conduct a confidential, anonymous survey with scenario-based questions: "You receive a taunting message from an attacker on a critical system. What is your first instinct?" and provide multiple-choice answers. Follow up in 1-on-1 interviews after critical incidents to discuss the decision-making process and emotional state.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement a "cool-down" mandatory delay for high-impact SOAR playbooks, requiring a second analyst approval for execution within the first 5 minutes.
- **Human/Organizational Mitigation:** Integrate de-escalation and emotional regulation techniques into security training. Establish a buddy system for peer review during high-tension incidents.
- **Process Mitigation:** Create a post-incident review checklist that explicitly includes analyzing the emotional state of responders and its impact on decisions.