Contents

[4.7] Anxiety-Triggered Mistakes

1. Operational Definition: A state of high anxiety that impairs cognitive function, leading to procedural errors, misconfigurations, and clumsy execution during security-critical tasks.

2. Main Metric & Algorithm:

- **Metric:** Anxiety-Induced Error Rate (AIER). Formula: `AIER = N_errors_during_high_anxiety / N_total_errors`. *We proxy "high anxiety" periods via high-severity incident counts.*
- **Pseudocode:**

  python

  ```
  def calculate_aier(error_log, incident_log, time_window='1h'):
      """
      error_log: Logs of configuration errors, failed login bursts, failed script runs.
      incident_log: List of security incidents with severity and time.
      """
      # Identify time bins with active HIGH or CRITICAL severity incidents
      high_stress_windows = get_high_severity_incident_windows(incident_log)

      total_errors = len(error_log)
      errors_in_stress = 0

      for error in error_log:
          # Check if this error occurred during a high-stress window
          if is_during_window(error['time'], high_stress_windows):
              errors_in_stress += 1

      aier = errors_in_stress / total_errors if total_errors else 0
      return aier
  ```

- **Alert Threshold:** `AIER > 0.6` (Over 60% of errors occur during high-anxiety periods).

3. Digital Data Sources (Algorithm Input):

- **SIEM/Syslog:** Logs for authentication failures, configuration management errors, script execution failures.
- **Ticketing System (Jira):** API to fetch incident data, including `severity` and `start_time`/`end_time`.

4. Human-to-Human Audit Protocol: During a low-stress period, interview analysts about recent high-severity incidents: "How did you feel during the incident? Can you walk me through your actions? Do you recall making any mistakes under pressure?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement automated sanity checks and pre-commit checks for critical commands to catch errors before they are executed.

- **Human/Organizational Mitigation:** Introduce mindfulness and stress-management training into the SOC. Ensure adequate staffing and break schedules during major incidents.
- **Process Mitigation:** Develop and practice high-fidelity runbooks and playbooks for common high-stress scenarios to reduce cognitive load.