Contents

[5.9] Complexity-Induced Errors

1. Operational Definition: Mistakes made not due to a lack of knowledge, but due to the overwhelming complexity of the tools, procedures, or attack itself, leading to incorrect configuration, flawed analysis, or missed steps.

2. Main Metric & Algorithm:

- **Metric:** Procedure Deviation Index (PDI). Formula: `PDI = (Number of skipped or out-of-order steps in a documented process) / (Total number of steps in the process)`. Measured by comparing analyst actions to a known playbook.
- **Pseudocode:**

  python

  ```
  def calculate_pdi(analyst_actions, playbook_steps):
      # analyst_actions: ordered list of actions taken (e.g., from SOAR audit log)
      # playbook_steps: ordered list of expected steps

      # This is a complex sequence alignment problem. A simpler proxy is:
      skipped_steps = set(playbook_steps) - set(analyst_actions)
      return len(skipped_steps) / len(playbook_steps)
  ```

- **Alert Threshold:** `PDI > 0.2` (The analyst is skipping more than 20% of the recommended steps in a standard playbook).

3. Digital Data Sources (Algorithm Input):

- **SOAR Platform:** The ideal source if playbooks are automated and steps are logged. The SOAR can directly log `playbook_step_skipped` or `step_completed` events.
- **Manual Audits:** For non-automated playbooks, this requires manual review of investigation notes against a checklist.

4. Human-to-Human Audit Protocol: Conduct a table-top exercise with a complex scenario. Have the analyst verbalize their actions while an auditor checks them off against the official incident response playbook. Note which steps are skipped, done out of order, or done incorrectly due to confusion.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Where possible, automate the most complex and error-prone steps of a playbook within a SOAR, reducing the cognitive burden on the analyst.
- **Human/Organizational Mitigation:** Provide regular training on complex procedures using realistic simulations, focusing on the *why* behind each step to aid understanding and recall.
- **Process Mitigation:** Simplify and streamline playbooks. Break complex procedures into smaller, more manageable sub-procedures with clear checkpoints.