Contents

[7.8] Cortisol-Impaired Memory

1. Operational Definition: The negative impact of chronic stress hormones on working memory and recall, leading to forgotten steps in procedures, missed details in alerts, or an inability to apply learned lessons from past incidents.

2. Main Metric & Algorithm:

- **Metric: Procedural Deviation Rate (PDR)**. Formula: `PDR = N_tasks_missing_steps / N_audited_tasks`.
- **Pseudocode:**

  python

```
def calculate_pdr(employee_id, start_date, end_date):
    # Get a sample of completed tasks (e.g., closed incidents)
    completed_tasks = query_soar_for_completed_tasks(employee_id, start_date, end_date)

    deviations = 0
    for task in completed_tasks:
        # Check playbook execution logs against the golden standard
        expected_steps = get_playbook_steps(task.playbook_id)
        executed_steps = get_executed_steps(task.incident_id)
        if expected_steps != executed_steps:  # Compare sets of required steps
            deviations += 1

    total_audited = len(completed_tasks)
    if total_audited > 0:
        pdr = deviations / total_audited
    else:
        pdr = 0
    return pdr
```

- **Alert Threshold:** `PDR > 0.15` (15% of audited tasks show missed critical steps).

3. Digital Data Sources (Algorithm Input):

- **SOAR Platform (e.g., XSOAR):** `playbook_id`, `task.executed_steps`, `incident.owner`.
- **CMDB / Procedure Database:** `standard_playbook.steps`.

4. Human-To-Human Audit Protocol: Direct observation or a "talk-through" method where the analyst explains how they would perform a routine procedure. "Can you walk me through the steps of the containment playbook for a phishing incident?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Integrate interactive checklists directly into the analyst's workflow within the SOAR or ticketing system to guide them step-by-step.

- **Human/Organizational Mitigation:** Implement a just-in-time micro-training system that delivers short, focused training modules based on recent errors.
- **Process Mitigation:** Simplify and standardize procedures. Encourage the use of personal wikis or notepads for analysts to jot down key learnings.