Contents

[7.10] Recovery Period Vulnerabilities

1. Operational Definition: The increased susceptibility to errors and lapses in judgment immediately following a period of high stress or a critical incident, due to cognitive depletion and the body's effort to restore homeostasis, creating a window of vulnerability.

2. Main Metric & Algorithm:

- **Metric: Post-Incident Error Rate (PIER)**. Formula: `PIER = N_errors / N_actions` for `N_hours` after incident resolution.
- **Pseudocode:**

  python

```
def calculate_pier(employee_id, incident_end_time, observation_hours=8):
    start_window = incident_end_time
    end_window = incident_end_time + timedelta(hours=observation_hours)

    # Get all actions performed by the analyst in the recovery window
    actions = query_soar_logs(employee_id, start_window, end_window)

    errors = 0
    for action in actions:
        # Define an error (e.g., failed script run, misconfigured rule, approval without c
        if action.status == "Failed" or action.comment == "":
            errors += 1

    total_actions = len(actions)
    if total_actions > 0:
        pier = errors / total_actions
    else:
        pier = 0
    return pier
```

- **Alert Threshold:** `PIER > 0.25` (25% of actions in the 8 hours post-incident are erroneous).

3. Digital Data Sources (Algorithm Input):

- **SOAR Platform:** `playbook_execution_logs.status`, `timestamp`, `user`.
- **Ticketing System:** `issue.updates` (for comments), `user`, `timestamp`.

4. Human-To-Human Audit Protocol: Targeted audit of work done in the hours after a major incident. Informal check-in by a manager: "How are you feeling after that last incident? Would it be helpful to hand over some of your routine tasks for the rest of the day?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement a system that automatically flags actions taken by analysts who were just involved in a critical incident for secondary review.

- **Human/Organizational Mitigation:** Formalize a “recovery period” policy, offering analysts light-duty tasks, a shortened shift, or time off after a major incident response.
- **Process Mitigation:** Mandate a handover procedure where an analyst coming off a high-stress incident must brief their replacement and is explicitly relieved of duty for a defined period.