Contents

[8.3] Repetition Compulsion Patterns 1

[8.3] Repetition Compulsion Patterns

1. Operational Definition: The unconscious tendency to repeat past security mistakes or procedural failures, often under similar circumstances (e.g., time of day, type of alert), despite awareness of the correct procedure.

2. Main Metric & Algorithm:

- **Metric:** Repeated Error Rate (RER). Formula: `RER = Count_of_Repeated_Error_Events / Total_Error_Events`.
- **Pseudocode:**

  python

```
def calculate_rer(analyst_id, start_date, end_date):
    # 1. Query all recorded error events from ticketing or SOAR playbook logs
    all_errors = query_errors(analyst_id, start_date, end_date)  # e.g., misclassified tic

    # 2. Cluster errors by type and context (e.g., same error type, similar time, similar
    repeated_errors = 0
    for error in all_errors:
        # Find similar past errors by the same analyst (e.g., within last 30 days)
        similar_past_errors = find_similar_errors(analyst_id, error, time_delta=30)
        if similar_past_errors:
            repeated_errors += 1

    # 3. Calculate ratio
    rer = repeated_errors / len(all_errors) if all_errors else 0
    return rer
```

- **Alert Threshold:** `RER > 0.3` (30% of errors are repeats of a previous mistake).

3. Digital Data Sources (Algorithm Input):

- **SOAR Platform:** Logs of playbook execution errors (fields `user`, `playbook_name`, `error_type`, `timestamp`, `asset_involved`).
- **Ticketing System:** Jira/ServiceNow API for tickets marked as “incorrectly classified” or “reopened” due to analyst error (fields `assignee`, `status`, `status_changes`, `comments`).
- **SIEM:** Logs of manual override actions that later proved to be incorrect.

4. Human-to-Human Audit Protocol: Review past incident reports involving the individual/team in a blameless post-mortem format. Ask: “We’ve seen a similar issue before. What was different about the context this time? What could we put in place to make the correct action more automatic or easier to remember next time?”

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement “just-in-time” training in SOAR playbooks; if a user fails a step, the system immediately offers a micro-training module on that specific action.

- **Human/Organizational Mitigation:** Integrate blameless post-mortems into the standard operating procedure to break the cycle of shame and repetition.
- **Process Mitigation:** Create and maintain a “common errors” checklist for specific high-stakes procedures to be consulted before finalizing an action.