Contents

[5.8] Attention Residue Effects

1. Operational Definition: The negative impact on performance when switching from Task A to Task B, where cognitive resources are still partially occupied by the previous task, reducing focus and effectiveness on the new task.

2. Main Metric & Algorithm:

- **Metric:** Time-to-Focus (TTF). Formula: `TTF = (Time between first opening a new alert and performing the first meaningful, unique investigative action on it)`. High TTF suggests attention residue from a previous task.
- **Pseudocode:**

  python

```
def calculate_ttf(events, alert_id):
    # Get events for this alert, sorted by time
    alert_events = get_events_for_alert(alert_id)
    open_time = None
    first_action_time = None

    for event in alert_events:
        if event.action == 'open' or event.action == 'assign':
            open_time = event.timestamp
        # Define what constitutes a "meaningful investigative action"
        if open_time and event.action in ['query_edr', 'run_yara', 'check_dns']:
            first_action_time = event.timestamp
            break

    if open_time and first_action_time:
        return (first_action_time - open_time).total_seconds() / 60  # Return time in minu
    else:
        return None  # Data incomplete
```

- **Alert Threshold:** `TTF > 15 (minutes)` for high-severity alerts. The analyst is taking over 15 minutes to begin meaningful work on a critical alert.

3. Digital Data Sources (Algorithm Input):

- **SOAR/SIEM Audit Logs:** To get the precise timestamp when an alert was assigned/opened by an analyst.
- **Various Tool Audit Logs (EDR, DNS, etc.):** To get the timestamp of the first investigative action taken on the alert, which may occur outside the SIEM.

4. Human-to-Human Audit Protocol: Ask an analyst to describe what they do in the first 5 minutes after picking up a new high-severity ticket. A vague or hesitant answer may indicate a lack of a clear protocol, exacerbating attention residue. Compare this with their measured TTF.

5. **Recommended Mitigation Actions:**

   - **Technical/Digital Mitigation:** Implement a “handover” protocol in the ticketing system where the previous analyst must leave a brief, structured summary of the alert’s context to reduce the cognitive load on the next analyst.
   - **Human/Organizational Mitigation:** Encourage analysts to perform a brief “closure ritual” (e.g., writing one sentence on next steps) before switching tasks to mentally compartmentalize the previous work.
   - **Process Mitigation:** Standardize the first 5 steps for investigating any new alert (e.g., 1. Check EDR, 2. Enrich IP, 3. Check auth logs). This reduces the decision load when starting a new task.