

Contents

[1.2] Diffusion of responsibility in hierarchical structures	1
--	---

[1.2] Diffusion of responsibility in hierarchical structures

1. Operational Definition: A psychological state where individuals in a hierarchical chain assume someone else is responsible for a security action or decision, leading to critical tasks being overlooked or delayed.

2. Main Metric & Algorithm:

- **Metric:** Task Bounce Rate (TBR). Formula: $TBR = (\text{Number of tickets reassigned more than } n \text{ times}) / (\text{Total number of tickets})$.

- **Pseudocode:**

```
python

def calculate_tbr(tickets, start_date, end_date, max_reassignments=2):
    """
    tickets: List of ticket objects from a ticketing system
    """
    filtered_tickets = [t for t in tickets if start_date <= t.created_date <= end_date]

    bounced_tickets_count = 0
    for ticket in filtered_tickets:
        # Get the assignment history from the ticket's timeline/audit log
        assignment_events = get_assignment_history(ticket)
        if len(assignment_events) > max_reassignments:
            bounced_tickets_count += 1

    total_tickets = len(filtered_tickets)
    TBR = bounced_tickets_count / total_tickets if total_tickets > 0 else 0
    return TBR
```

- **Alert Threshold:** $TBR > 0.15$ (Over 15% of tickets are reassigned more than twice)

3. Digital Data Sources (Algorithm Input):

- **Ticketing System API (Jira, ServiceNow):** Fields: `ticket_id`, `created_date`, `audit_log` (containing history of assignee changes).

4. Human-to-Human Audit Protocol: Interview team members using a critical incident technique: “Describe a recent security task that was delayed. Walk me through who was assigned what and the communication that happened. Were you waiting for someone else to take action?” Look for patterns of assumption and unclear ownership.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Configure ticketing system escalations to automatically alert a manager if a ticket is reassigned more than n times within a set period.
- **Human/Organizational Mitigation:** Define and communicate RACI (Responsible, Accountable, Consulted, Informed) charts for common security processes and incident types.

- **Process Mitigation:** Implement a daily “ticket huddle” where the team reviews open tickets with ambiguous ownership and explicitly assigns a single responsible owner.