

Contents

[7.6] Fawn Response Overcompliance	1
--	---

[7.6] Fawn Response Overcompliance

1. Operational Definition: A stress-induced response to appease authority figures or systems by following procedures to an excessive, unthinking degree, often bypassing critical thinking and leading to errors (e.g., approving a risky request from a superior without scrutiny).

2. Main Metric & Algorithm:

- **Metric: Blind Approval Rate (BAR).** Formula: $BAR = \frac{N_approvals_with_short_review}{N_total_approvals}$.

- **Pseudocode:**

```
python

def calculate_bar(employee_id, start_date, end_date):
    # Get all approval actions performed by the employee (e.g., access requests, firewall
    approvals = query_iam_system(employee_id, start_date, end_date)

    blind_approvals = 0
    for approval in approvals:
        # Define "short review" as less than 60 seconds between request and approval
        review_time = approval.approval_time - approval.request_time
        if review_time < timedelta(seconds=60):
            blind_approvals += 1

    total_approvals = len(approvals)
    if total_approvals > 0:
        bar = blind_approvals / total_approvals
    else:
        bar = 0
    return bar
```

- **Alert Threshold:** $BAR > 0.3$ (30% of approvals are done in under 60 seconds).

3. Digital Data Sources (Algorithm Input):

- **Identity and Access Management (IAM) System API** (e.g., SailPoint, Okta Work-flows): approver, request_time, decision_time, decision.
- **Privileged Access Management (PAM) System Logs.**

4. Human-To-Human Audit Protocol: Sample audit of approved requests. In an interview, present a recent, approved request and ask: “Can you talk me through the factors you considered before approving this?” “Did you feel any pressure to approve this quickly?”

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement a mandatory 2-minute “cooling-off” period for all high-risk approvals. Require a mandatory comment field for any approval.

- **Human/Organizational Mitigation:** Training on assertiveness and security governance. Reinforce that the security team's authority to deny requests is supported by leadership.
- **Process Mitigation:** Introduce a “four-eyes” principle for approvals coming from high-authority figures.