Contents

[2.1] Urgency-induced security bypass

1. Operational Definition: The tendency for personnel to circumvent established security protocols when under perceived time pressure, significantly increasing the risk of error and introducing vulnerabilities.

2. Main Metric & Algorithm:

- **Metric:** Security Bypass Rate (SBR). Formula: `SBR = (Number of security procedure violations) / (Total number of opportunities for violation)`.
- **Pseudocode:**

  python

```
def calculate_sbr(access_logs, change_logs, start_date, end_date):
    """
    access_logs: Logs from secure systems
    change_logs: Logs from change management system
    """
    # 1. Identify "opportunities": High-impact actions performed (e.g., prod deployment, f
    all_actions = get_high_impact_actions(access_logs, change_logs, start_date, end_date)

    # 2. For each action, check if it violated procedure (no ticket, outside maintenance w
    violations = 0
    for action in all_actions:
        # Check if there's an approved change ticket for this action/time/system
        corresponding_ticket = find_change_ticket(action)
        if not corresponding_ticket or corresponding_ticket.status != 'approved':
            violations += 1

    total_actions = len(all_actions)
    SBR = violations / total_actions if total_actions > 0 else 0
    return SBR
```

- **Alert Threshold:** `SBR > 0.1` (Over 10% of high-impact actions bypass change control)

3. Digital Data Sources (Algorithm Input):

- **Change Management System API:** To get a list of approved changes (`ticket_id`, `approved_time`, `affected_systems`).
- **Infrastructure Logs (Git commits, CI/CD pipelines, Firewall/Admin logs):** To get a list of all actual high-impact actions performed (`action`, `timestamp`, `system`, `user`).

4. Human-to-Human Audit Protocol: Review a sample of recent high-impact changes. For each, interview the person who performed it and their manager: "What was the business driver for this change? Walk me through the change approval process for it." Corroborate the story with the change management system audit trail.

5. **Recommended Mitigation Actions:**

    - **Technical/Digital Mitigation:** Implement technical enforcement (e.g., deployment pipelines that require a valid change ticket number before executing) rather than relying on procedural controls.
    - **Human/Organizational Mitigation:** Foster a culture where meeting a deadline is not an acceptable justification for bypassing security, reinforced by leadership.
    - **Process Mitigation:** Introduce an expedited (but not skipped) emergency change process with mandatory post-implementation review to handle genuine urgency.