Contents

[1.4] Bypassing Security for Superior's Convenience

1. Operational Definition: The observed behavior where an employee disables or circumvents a security control (e.g., USB restrictions, application whitelisting) because a direct superior has requested they do so to complete a task more quickly.

2. Main Metric & Algorithm:

- **Metric:** Unauthorized Bypass Frequency (UBF). Formula: `UBF = Count(bypass_events) / Number_of_employees`.
- **Pseudocode:**

  python

```
def calculate_ubf(edr_logs, ticketing_system, start_date, end_date):
    # Query EDR for events where security controls were changed or disabled
    bypass_events = query_edr_events(
        action=['disable', 'bypass', 'override'],
        feature=['firewall', 'av', 'device_control'],
        date_range=(start_date, end_date)
    )

    # Enrich with ticketing data to find events without a valid, pre-approved ticket
    unauthorized_events = []
    for event in bypass_events:
        # Check if a ticket was approved for this action on this asset
        related_tickets = query_tickets(asset_id=event.asset_id, action_requested=event.ac
        approved_ticket_exists = any(t.status == 'approved' for t in related_tickets)
        if not approved_ticket_exists:
            unauthorized_events.append(event)

    total_employees = get_active_employee_count()
    UBF = len(unauthorized_events) / total_employees
    return UBF
```

- **Alert Threshold:** `UBF > 0.05` (i.e., more than 5% of the workforce has performed an unauthorized bypass in the period).

3. Digital Data Sources (Algorithm Input):

- **EDR/XDR Logs** (e.g., CrowdStrike, Microsoft Defender): Security control modification events.
- **Ticketing System API** (e.g., ServiceNow, Jira): To cross-reference changes with approved change requests.
- **Configuration Management Database (CMDB):** To get accurate asset-to-owner mapping.

4. Human-to-Human Audit Protocol: Interview team managers and their direct reports separately. Ask managers: “Have you ever asked your team to bypass a security policy to meet a deadline?” Ask employees: “Has your manager ever asked you to bypass a security control? How did you handle it?” Look for discrepancies and admitted instances.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement technical controls that require multi-person authorization (MFA/MofN) for critical security policy changes.
- **Human/Organizational Mitigation:** Leadership training on the operational risk of bypassing security and clear support from top management for employees who refuse unethical orders.
- **Process Mitigation:** Create and promote an expedited, legitimate process for requesting temporary security exceptions, reducing the perceived need for unauthorized bypasses.