Contents

[1.9] Authority-Based Social Proof

1. Operational Definition: The tendency of individuals to adopt insecure behaviors because they observe authority figures or a perceived majority of their peers engaging in those same behaviors, assuming it must be acceptable.

2. Main Metric & Algorithm:

- **Metric:** Insecure Practice Adoption Latency (IPAL). Formula: `IPAL = Average time between an authority figure's observed insecure action and its first replication by a subordinate`.
- **Pseudocode:**

  python

```
# This is complex and may require analyzing sequences of events.
def calculate_ipal(log_data, hr_org_chart, start_date, end_date):
    # 1. Define a list of insecure actions (e.g., 'disable_av', 'use_unsanctioned_cloud_ap
    insecure_actions = [...]

    # 2. Find these actions performed by managers/directors/VPs
    authority_events = query_events(users=get_authority_users(hr_org_chart), actions=insec

    replication_times = []
    # 3. For each authority event, check if their direct reports performed the same actio
    for auth_event in authority_events:
        reports = get_direct_reports(auth_event.user, hr_org_chart)
        for report in reports:
            report_events = query_events(users=[report], actions=[auth_event.action], date
            if report_events:
                time_delta = report_events[0].time - auth_event.time
                replication_times.append(time_delta)

    IPAL = sum(replication_times, timedelta(0)) / len(replication_times) if replication_ti
    return IPAL
```

- **Alert Threshold:** A statistically significant (`p < 0.05`) correlation between an authority's insecure action and subsequent similar actions by their team, with an average `IPAL < 7 days`.

3. Digital Data Sources (Algorithm Input):

- **EDR/Proxy/SIEM Logs:** To detect specific insecure actions (e.g., running unapproved software, accessing blocked sites).
- **HRIS API:** To obtain organizational hierarchy data (`manager_id`, `employee_id`).

4. Human-To-Human Audit Protocol: In focus groups, present a scenario: "Your manager often uses a personal Dropbox to share large files for work because it's 'faster.' What would you do?" Gauge the level of acceptance of this behavior.

5. **Recommended Mitigation Actions:**

   - **Technical/Digital Mitigation:** Apply technical controls uniformly. If a practice is insecure, the system should prevent it for everyone, regardless of role.
   - **Human/Organizational Mitigation:** Leaders must be held to a higher standard and act as role models for secure behavior. Publicly call out and correct insecure practices at all levels.
   - **Process Mitigation:** Create safe channels for employees to report insecure behaviors they observe in leadership without fear of reprisal.