Contents

[3.3] Social Proof Manipulation

1. Operational Definition: The tendency of individuals to adopt the actions or behaviors of a group, even if those actions violate security policies, because they perceive the behavior as correct or normal based on its prevalence.

2. Main Metric & Algorithm:

- **Metric: Deviant Practice Prevalence (DPP).** Formula: `DPP = U_deviant / U_total`, where `U_deviant` is the number of users engaging in a specific insecure practice and `U_total` is the total number of users in a peer group.
- **Pseudocode:**

  python

```
def calculate_dpp(logs, peer_groups, insecure_action_patterns):
    """
    logs: Consolidated logs from various sources showing user actions.
    peer_groups: A mapping of users to their teams/departments.
    insecure_action_patterns: A list of regex or patterns defining the insecure behavior (
    """
    dpp_results = {}
    for group, users in peer_groups.items():
        total_users = len(users)
        deviant_users = set()

        for user in users:
            user_actions = get_actions(logs, user, period='30d')
            # Check if user performed any of the defined insecure actions
            if any(action_matches_pattern(action, insecure_action_patterns) for action in
                deviant_users.add(user)

        dpp = len(deviant_users) / total_users
        dpp_results[group] = dpp
    return dpp_results
```

- **Alert Threshold:** `DPP > 0.4` (Over 40% of a peer group engages in the practice).

3. Digital Data Sources (Algorithm Input):

- **Proxy/Firewall Logs (e.g., Zscaler, Palo Alto):** To detect visits to unauthorized cloud storage or websites. Fields: `user`, `url`, `category`.
- **Endpoint DLP Logs (e.g., Microsoft Purview, Symantec DLP):** To detect unauthorized file transfers. Fields: `user`, `file_name`, `action` (e.g., `upload`, `copy`), `destination`.
- **Cloud Access Security Broker (CASB) Logs (e.g., Netskope, McAfee MVISION):** To detect shadow IT usage. Fields: `user`, `app_name`, `activity`.

4. Human-to-Human Audit Protocol: Distribute an anonymous survey to departments: "Approximately what percentage of your colleagues do you think use [X insecure method, e.g., personal email] to share work files?" Compare the perceived percentage with the DPP metric calculated from logs. A high correlation confirms the bias is active.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Use CASB or DLP tools to automatically block uploads to unauthorized services and redirect users to the organization's approved, secure alternative.
- **Human/Organizational Mitigation:** Leadership and security champions should publicly champion and recognize correct security behaviors to provide positive social proof.
- **Process Mitigation:** Clearly document and communicate the *actual* prevalence of secure behavior (e.g., "95% of the finance team uses the approved secure share tool correctly") to counteract false perceptions of deviant norms.