Contents

[6.3] Diffusion of Responsibility

1. Operational Definition: A socio-psychological phenomenon where individuals are less likely to take action or feel responsible for a task when they believe others are also responsible. In a SOC, this manifests as critical alerts or tasks remaining in an unassigned state for prolonged periods or being repeatedly reassigned without action.

2. Main Metric & Algorithm:

- **Metric:** Unassigned Critical Alert Duration (UCAD). Formula: `Time between alert creation and assignment to an individual owner`.
- **Pseudocode:**

  python

  ```
  def calculate_ucad(alerts, severity='critical'):
      unassigned_critical_alerts = [a for a in alerts if a.severity == severity and a.owner
      total_duration = 0
      for alert in unassigned_critical_alerts:
          time_unassigned = alert.time_now - alert.created_time
          total_duration += time_unassigned
      # Return average hours unassigned
      return total_duration / len(unassigned_critical_alerts) if unassigned_critical_alerts
  ```

- **Alert Threshold:** `UCAD > 4 (hours)` for critical severity alerts.

3. Digital Data Sources (Algorithm Input):

- **SIEM (Splunk/Elasticsearch):** Alert index. Fields: `signature` (e.g., "Critical Vulnerability Detected"), `severity`, `created_time`, `owner`.
- **SOAR/Ticketing (ServiceNow, Jira):** Task/Incident tables. Fields: `state` (e.g., "New", "Assigned"), `assignment_group`, `assigned_to`, `sys_created_on`.

4. Human-to-Human Audit Protocol: During a team meeting, present a list of all alerts that were unassigned for more than the threshold (4 hours) in the last week. Ask the team: "What was the process for assigning these? Was it unclear who was responsible? Did everyone assume someone else would pick it up?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Configure the SOAR platform to auto-assign new critical alerts to a specific on-call analyst or a primary/secondary rotation, eliminating the unassigned state.
- **Human/Organizational Mitigation:** Clearly define and document RACI (Responsible, Accountable, Consulted, Informed) charts for different alert types and incident response procedures.
- **Process Mitigation:** Implement a daily "unassigned audit" ritual where the shift lead reviews all unassigned items older than 1 hour and explicitly assigns them, verbally confirming acceptance.