Contents

[6.5] Bystander Effect in Incident Response

1. Operational Definition: The phenomenon where individuals are less likely to take action during an emergency (e.g., a security incident) when other people are present. This manifests as a delay in the initial response or escalation of an incident because each observer assumes someone else will handle it.

2. Main Metric & Algorithm:

- **Metric:** First Response Time (FRT). Formula: `Time between incident creation and the first meaningful action taken by any team member`.
- **Pseudocode:**

  python

  ```
  def calculate_frt(incidents):
      frt_list = []
      for incident in incidents:
          # Get all actions for this incident, sorted by time
          actions = get_actions(incident.id)
          first_action_time = actions[0].timestamp if actions else None
          if first_action_time:
              response_time = first_action_time - incident.created_time
              frt_list.append(response_time)
      return np.median(frt_list) # Use median to avoid skew from outliers
  ```

- **Alert Threshold:** `FRT > 15 (minutes)` for high-severity incidents.

3. Digital Data Sources (Algorithm Input):

- **SOAR/Ticketing (ServiceNow, Jira):** Incident table. Fields: `number`, `sys_created_on`, `state`.
- **SOAR/Ticketing Audit Logs:** Fields: `tablename`, `recordkey`, `fieldname`, `sys_created_on`. (To find the first state change or comment after incident creation).

4. Human-to-Human Audit Protocol: During a tabletop exercise or a post-incident review of a real case, ask the team: “When the alert first came in, what was your thought process? Did you see it? Did you assume a specific person or the shift lead would handle it? Was there any hesitation to be the first to engage?”

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Configure alerting rules to page the primary on-call analyst directly (e.g., via PagerDuty/VictorOps) for critical alerts, bypassing a shared channel and assigning clear ownership immediately.
- **Human/Organizational Mitigation:** Implement and practice a formal “First Responder” protocol for every shift, designating who is expected to triage any new incoming high-severity alert.

- **Process Mitigation:** Create a culture of “See Something, Say Something” where any analyst who notices an unactioned alert, even if not assigned to them, is empowered and expected to at least assign it to the correct person or bring it up in the team chat.