Contents

[1.10] Crisis Authority Escalation

1. Operational Definition: During a confirmed or perceived security crisis, the automatic and often unquestioned transfer of decision-making authority to the highest-ranking individual present, potentially bypassing established incident response protocols and expert advice.

2. Main Metric & Algorithm:

- **Metric:** Protocol Bypass Frequency during Incidents (PBFI). Formula: `PBFI = Count(protocol_deviations) / N_major_incidents`.
- **Pseudocode:**

  python

  ```
  def calculate_pbfi(incident_reports, comms_data, start_date, end_date):
      major_incidents = query_incidents(severity=['high', 'critical'], date_range=(start_dat
      deviation_count = 0

      for incident in major_incidents:
          # Analyze IR playbook steps vs. actual actions taken
          planned_steps = get_playbook_steps(incident.type)
          actual_actions = get_incident_actions(incident.id)

          # Check for commands from executives that bypassed playbook steps
          exec_comms = get_incident_comms(incident.id, from_users=get_executives())
          for comm in exec_comms:
              if comm.command not in planned_steps:
                  deviation_count += 1
                  break # Count one deviation per incident

      PBFI = deviation_count / len(major_incidents) if major_incidents else 0
      return PBFI
  ```

- **Alert Threshold:** `PBFI > 0.2` (i.e., playbooks are bypassed in more than 20% of major incidents).

3. Digital Data Sources (Algorithm Input):

- **SOAR/Incident Management Platform API:** Incident logs, assigned playbooks, and action timelines.
- **Communication Platform API (Slack, Teams):** Channels dedicated to major incidents, to analyze command and decision flow.
- **HRIS API:** To identify users with executive roles.

4. Human-To-Human Audit Protocol: During post-incident reviews (blameless postmortems), explicitly ask: "Were all actions taken in accordance with our runbooks? If not, what was the reason? Was a decision made to deviate by someone based on their seniority rather than the protocol?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement technical "circuit breakers" in SOAR playbooks that require a documented reason and a second opinion for critical deviations.
- **Human/Organizational Mitigation:** Conduct crisis simulation exercises where an executive is present but the Incident Commander role is clearly assigned to a trained expert. Debrief the chain of command.
- **Process Mitigation:** Formalize the role of "Incident Commander" in the IR policy, vesting them with clear authority to execute the playbook during an incident, with pre-approved backing from leadership.