Contents

[7.5] Freeze Response Paralysis

1. Operational Definition: A stress-induced state of cognitive overload and indecision where an analyst is unable to initiate or continue a security response action, often during a critical incident, leading to dangerous delays.

2. Main Metric & Algorithm:

- **Metric: Incident Response Lag (IRL)**. Formula: `IRL = timestamp(first_action) - timestamp(incident_detection)`.
- **Pseudocode:**

  python

  ```
  def calculate_irl(incident_id):
      # Get the incident creation time from SOAR/SIEM
      incident = query_incident_db(incident_id)
      detection_time = incident.created_time

      # Get the timestamp of the first meaningful action (e.g., alert acknowledgement, scrip
      first_action_log = query_soar_playbook_logs(incident_id).first()
      if first_action_log:
          action_time = first_action_log.timestamp
          irl = action_time - detection_time
          return irl  # in minutes
      else:
          return None  # No action taken
  ```

- **Alert Threshold:** `IRL > 15` minutes for a **critical** severity incident.

3. Digital Data Sources (Algorithm Input):

- **SOAR Platform (e.g., Splunk Phantom, XSOAR):** `incident_id`, `created_time`, `playbook_execution_logs`.
- **SIEM (e.g., Elastic SIEM):** `event.ingested`, `event.kind:alert`.

4. Human-To-Human Audit Protocol: Run tabletop simulations and measure time to first response. Conduct a post-incident review interview: "What was going through your mind in the first minutes after the alert sounded?" "Was anything unclear or confusing about the procedure?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement and mandate the use of SOAR playbooks that provide step-by-step guidance, reducing the cognitive load required to decide what to do first.
- **Human/Organizational Mitigation:** Stress inoculation training through realistic, high-fidelity drills.
- **Process Mitigation:** Define and drill a clear "first 5 minutes" protocol for different incident types. Institute a buddy system where two analysts are assigned to respond to critical incidents.