**Create the Flowchart in Lucidchart**

**Workflow Steps to Include:**

1. **Monitor SIEM:**
   * Inputs: Alerts from Splunk/SolarWinds.
   * Action: Analyst validates the alert.
2. **Log Incident:**
   * Inputs: Validated incident details.
   * Action: Enter incident data into the tracker.
3. **Triage and Classification:**
   * Inputs: Incident details.
   * Action: Assign severity level.
   * Decision Point: If severity is "High" or "Critical," escalate to Manager.
4. **Containment:**
   * Inputs: Manager’s escalation instructions.
   * Actions:
     + Isolate affected systems.
     + Block malicious IPs.
     + Disable compromised accounts.
5. **Mitigation:**
   * Inputs: Tools and methods (CrowdStrike, OpenVAS).
   * Actions:
     + Remove malware.
     + Apply patches or updates.
6. **Recovery:**
   * Inputs: Backups and testing tools.
   * Actions:
     + Restore data/systems.
     + Test functionality.
7. **Post-Incident Reporting:**
   * Inputs: Incident details and actions taken.
   * Actions:
     + Create report.
     + Submit for review.
8. **Process Improvement:**
   * Inputs: Lessons learned.
   * Actions:
     + Identify gaps.
     + Update processes or tools.