1. **Project Title & Version Control**

   Simulated SOC Incident Response & Analysis

   Version Control

- Lab Version: Version 1.0
- Date: 06/17/2025
- Change Log: N/A

2. **Project Summary** This project aims to provide a realistic, hands-on experience for developing Security Operations Center (SOC) incident response skills. It involves setting up a simulated enterprise network, detecting and investigating a simulated attack, and employing containment and remediation strategies alongside extensive documentation to aid future incident response readiness.

3. **Problem Statement / Use Case** Cyber attacks are increasingly sophisticated, requiring well-trained Security Operations Center (SOC) analysts to respond effectively. This project prepares prospective analysts by offering a realistic scenario to practice their skills in a controlled, simulated environment.

4. **Goals and Objectives**

   - Develop technical incident response skills
   - Learn to configure, manage, and respond to alerts within a Security Information and Event Management (SIEM) platform
   - Provide extensive, realistic practice in investigating and mitigating cyber attacks

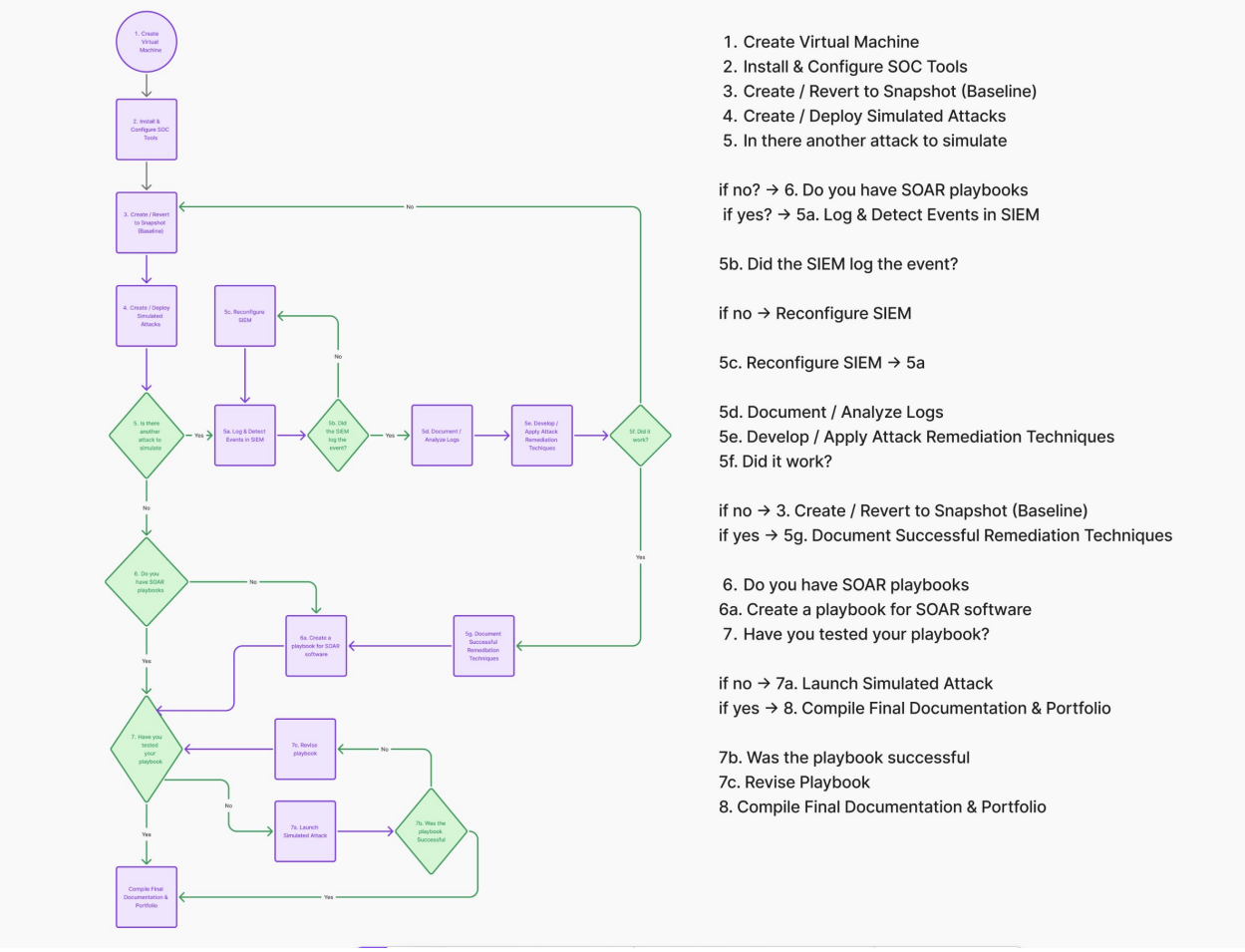
5. **Key Features / Functions**

    - Simulating a realistic enterprise attack
    - Security event detection, triaging, and investigating attacks
    - Implementing containment and remediation strategies
    - Collaborative incident response with extensive documentation
    - Simulated attacks and malware testing, including: Brute Force Authentication, Phish-Based Compromise with Malicious Payload, Privilege Escalation, Lateral Movement, Command-and-Control Communication, Malicious File / Ransomware Simulation, Data Exfiltration Attempt, Port Scanning and Network Discovery, Fileless or PowerShell Attacks, and a Malware Analysis Component

6. **Tech Stack and Tools**

    - Security Information and Event Management (SIEM) (Splunk or Elastic SIEM)
    - Network packet capture with Wireshark
    - Linux and Windows event logging
    - SOAR (Security orchestration and automated response scripting) Software

7. **Architecture / Workflow Diagram** Diagram depicting the simulated enterprise network, attack vectors, incident response process, and containment strategies (full image attached separately).



8. **Timeline / Weekly Milestone**
    - Week 1: Lab Setup
    - Jul 7-8: Create virtual network lab (Linux, Windows, DMZ, firewall)
    - Jul 7-8: Install and configure SIEM (Splunk or Elastic)
    - Jul 9th: Install Wireshark on network monitoring node
    - Jul 7-10: Enable audit logging on Windows or Linux
    - Jul 10: Validate lab functionality with test logins
    -
    - Week 2: Research and Implement Attack Vectors
    - Jul 14th: Launch brute force attack (e.g., Hydra)
    - Jul 14th: Simulate phishing payload delivery (email or dropper)
    - Jul 14th: Emulate privilege escalation (e.g., mimikatz)
    - Jul 15th: Conduct lateral movement (e.g., PsExec)
    - Jul 15th: Create ransomware/malicious file activity
    - Jul 16th: Conduct network scanning (nmap)Jul 16th:
    - Jul 16th: Trigger fileless attack (PowerShell scripts)
    - Jul 17th: Confirm all attacks are logged in SIEM
    - Jul 17th: Develop Remediation Scripts and Playbook for each attack
    - Week 3: Investigate attacks and respond
    - Jul 21st: Identify IOCs in SIEM (hashes, IPs, file names)
    - Jul 21st: Triaging suspicious alerts
    - Jul 22nd: Investigate incident chain (kill chain mapping)
    - Jul 22nd: Perform containment (block IPs, isolate host)
    - Jul 23rd: Improve remediation scripts (restore, clean)
    - Jul 24th: Annotate SIEM logs with incident notes
    - Week 4: Perform forensics and produce incident report

- Jul 28th: Analyze endpoint logs (PowerShell, Sysmon)
- Jul 28th-29th: Reconstruct attacker timeline (TTPs)
- Jul 30th: Perform basic malware analysis (strings, behavior)
- Jul 30th: Write detailed incident report
- Jul 31st: Conduct project debrief & lessons learned

- Week 5-9: Research and Implementation of Cloud Based Chat Bot for AWS Certificate Training

- Week 10-12: Red vs Blue Capture The Flag Scenario

9. **Risks and Risk Mitigation**

    - Network configuration complexity: Implement fallback routines and snapshots
    - Security tool configuration inaccuracies: Use community standards and extensive testing
    - Limit attack scenarios: Develop multiple attack paths and vulnerabilities

10. **Evaluation Criteria**

- Successful containment and eradication of simulated attack
- Detailed and clear incident report
- Ability to identify attack indicators and actor motives

11. **Future Considerations**

- Expand to more realistic attack scenarios
- Implement automated incident response routines
- Integrate additional vulnerability scanning and forensics tools