**Documentation and Demo Phase**

Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age

Team Members:

1. Dhanraj Pawar
2. Kaushal Chougule
3. Athrav Pawar
4. Balaji Patil

**Documentation and Demonstration Phase Summary**

The Documentation and Demonstration Phase marks the final stage of the project lifecycle. This phase involves compiling essential documentation and conducting a presentation to exhibit the system’s functionality and efficiency.

**Objectives:**

* Record details of the system’s design, implementation, and testing.
* Develop a demonstration to highlight the system’s features.
* Ensure that all stakeholders are well-informed about system usage.

**Documentation**

The documentation offers a detailed account of the system, including its structure, development, and testing. Key components include:

**1. User Guide**

The user guide provides step-by-step instructions for utilizing the system.

* **Sections:**
  1. **Introduction:** Overview of the system and its purpose.
  2. **Installation Guide:** Instructions for installing and setting up the system.
  3. **Usage Guide:** How to use system features (e.g., vulnerability scanning, log analysis).
  4. **Troubleshooting:** Solutions to common issues.

**2. Technical Documentation**

The technical documentation provides in-depth information on system architecture and implementation.

* **Sections:**
  1. **System Architecture:** Overview of system components, including frontend, backend, and database.
  2. **Workflows:** Detailed workflows for vulnerability assessment, threat detection, and incident management.
  3. **Code Reference:** Documentation on system code, including APIs and scripts.
  4. **Test Cases:** Functional and performance test cases.

**3. Incident Management Plan**

The incident management plan outlines the procedures to follow in case of a cyber incident.

* **Sections:**
  1. **Incident Identification:** Methods for detecting cybersecurity threats.
  2. **Response Procedures:** Steps to mitigate and address an incident.
  3. **Post-Incident Review:** Steps to assess and document lessons learned after an incident.

**Demonstration**

The demonstration highlights the system’s features and capabilities. Below is the structured demo plan:

**1. Demo Overview**

* **Objective:** Showcase system functionality to stakeholders.
* **Audience:** Project sponsors, team members, and end-users.
* **Duration:** 30 minutes.

**2. Demo Agenda**

* **Introduction (5 minutes):**
  + Overview of project objectives.
  + Brief explanation of system features.
* **Vulnerability Assessment Demo (10 minutes):**
  + Demonstrate vulnerability scanning using Nessus.
  + Show how to interpret results and prioritize risks.
* **Threat Monitoring Demo (10 minutes):**
  + Demonstrate SIEM log monitoring for unusual activity.
  + Show how to analyze and escalate potential threats.
* **Incident Response Demo (5 minutes):**
  + Analyze phishing emails for Indicators of Compromise (IOCs).
  + Generate an incident report and suggest remediation measures.
* **Q&A Session (5 minutes):**
  + Address stakeholder queries.

**Deliverables**

1. **User Guide:**
   * Comprehensive instructions for system use.
2. **Technical Documentation:**
   * Detailed records of system architecture, workflows, and coding elements.
3. **Incident Management Plan:**
   * A structured response plan for handling cyber incidents.
4. **Demo Script:**
   * Step-by-step outline of the demonstration process.

**Next Steps**

1. **Deployment:**
   * Implement the system in the production environment.
2. **Training:**
   * Provide user training for effective system utilization.
3. **Ongoing Maintenance:**
   * Ensure continued system support and performance monitoring.