**Project Report:** Cybersecurity Risk Assessment and Mitigation Strategy Implementation for an E-Commerce Platform

**Introduction**

In today’s digital world, e-commerce platforms are increasingly targeted by sophisticated cyber threats. This report focuses on improving the cybersecurity posture of an e-commerce platform through a comprehensive risk assessment and implementation of best mitigation strategies. The issue like, rapid increase in threats to online retail systems, data breaches, phishing attacks, and unauthorized access to system, has raised concern to e-commerce businesses to protect their sensitive data and digital assets. Our teams aim to identify existing vulnerabilities, evaluate associated risks, and propose actionable solutions for an e-commerce platform to enhance their security posture. The report outlines the complete project plan, scope, Gantt chart with interdependence, risk assessment and change management processes. The report also presents the use of industry standard tools such as GitHub for version control and Jira for team collaboration.

**Project Plan Document: Cybersecurity Risk Assessment and Mitigation Strategy Implementation for an E-Commerce Platform**

1. **Project Scope Statement**

Objective: To conduct a comprehensive cybersecurity risk assessment and mitigate cybersecurity risks in an e-commerce platform by identifying vulnerabilities, prioritizing threats, and implementing effective actionable measures.

**In-Scope Activities**

* Identification of cybersecurity risks through scans and assessment.
* Developing and implementing mitigation control such as MFA, firewalls, and encryption.
* Identifying threats such as malware, phishing, DDoS attacks, and insider threats.
* Use of GitHub for version control
* Use of Jira for team collaboration and project tracking
* Delivering a final report and presentation.

**Out-of-Scope Activities:**

* Physical security audits and controls.
* Applying hardware-based solutions in addition to software setups.
* Redesign of the e-commerce platform infrastructure.
* Ongoing monitoring and maintenance after project completion.

**Deliverables**

* Risk Assessment Report
* Mitigation Strategy Plan
* Gantt Chart with timeline phases including (Planning, Assessment, Mitigation, Monitoring.)
* Screenshots of GitHub and Jira usage.

1. **Gantt Chart with Interdependencies**

The Gantt chart below outlines the project timeline, tasks, duration and interdependencies to ensure timely project delivery and manage interrelated task effectively.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Phase | Task | Start Date | End Date | Duration | Dependency |
| T1 | Planning | Define scope and objectives | 01/06/2025 | 02/06/2025 | 2 days | - |
| T2 | Planning | Assign roles and responsibilities | 03/06/2025 | 04/06/2025 | 2 days | T1 |
| T3 | Planning | Select tools (GitHub, Jira) | 05/06/2025 | 07/06/2025 | 3 days | T2 |
| T4 | Risk Assessment | Perform vulnerability scanning | 08/06/2025 | 11/06/2025 | 4 days | T3 |
| T5 | Risk Assessment | Conduct threat modelling and analysis | 12/06/2025 | 15/06/2025 | 4 days | T4 |
| T6 | Risk Assessment | Prioritize identified risks | 16/06/2025 | 21/06/2025 | 6 days | T5 |
| T7 | Mitigation | Implement Multi-Factor Authentication (MFA) | 22/06/2025 | 26/06/2025 | 5 days | T6 |
| T8 | Mitigation | Update and configure firewall rules | 27/06/2025 | 01/07/2025 | 5 days | T7 |
| T9 | Mitigation | Conduct cybersecurity training for employees | 02/07/2025 | 05/07/2025 | 4 days | T8 |
| T10 | Monitoring | Set up continuous threat detection tools | 06/07/2025 | 12/07/2025 | 7 days | T9 |
| T11 | Monitoring | Test incident response procedures | 13/07/2025 | 19/07/2025 | 7 days | T10 |

Table-1: Gantt Chart with interdependencies

The following visual representation of the Gantt chart provides a clearer timeline and task flow with visible dependencies and duration.

Figure-1: Visual Gantt chart