Project Planning Document

Date: 12 March 2025
Team ID: PNT2025TMID02719
Project Name: Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age Maximum Marks: 8 Marks

Team Details

S.no	Name	College	Contact
1	Maaj Bairagdar	DYP-ATU	maajbairagdar3365@gmail.com
2	Bilal Mirje	DYP-ATU	mirjebilal7@gmail.com
3	MohamadAyan Desai	DYP-ATU	ayan2004desai@gmail.com

Institution: DY Patil Agriculture and Technical University, Talsande

1. INTRODUCTION

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

1.2 Team ID:
PNT2025TMID02719

1.3 Maximum Marks:
8 Marks

2. PRODUCT BACKLOG, SPRINT SCHEDULE, AND ESTIMATION (4 Marks)

Sprint-1: Identifying Cybersecurity Risks

Sprint	Functional Requirement (Epic)	USN	User Story	Story Points	Priority	Team Member
Sprint-1	Identifying Cybersecurity Risks	USN-1	As a security researcher, I can detect and classify various cyber threats, including malware, phishing, and ransomware.	4	High	Maaj
Sprint-1	Identifying Cybersecurity Risks	USN-2	As a threat analyst, I can investigate recent cybersecurity breaches and document their consequences.	3	High	Ayan

Sprint-2: Digital Evidence Analysis & Security Response

Sprint	Functional Requirement (Epic)	USN	User Story	Story Points	Priority	Team Member
Sprint-2	Digital Evidence Analysis & Security Response	USN-3	As an incident handler, I can examine system logs to extract valuable security insights.	4	High	Bilal

Sprint-2	Digital Evidence Analysis & Security Response	USN-4	As a forensic investigator, I can trace attack sources using digital forensic tools.	3	Medium	Maaj

Sprint-3: Secure Data Handling & Access Control

Sprint	Functional Requirement (Epic)	USN	User Story	Story Points	Priority	Team Member
Sprint-3	Secure Data Handling & Access Control	USN-5	As a security architect, I can implement encryption techniques (AES, RSA) to protect confidential data.	4	High	Ayan
Sprint-3	Secure Data Handling & Access Control	USN-6	As a software developer, I can integrate multi-factor authentication (MFA) into an application.	3	Medium	Bilal

Sprint-4: Network Traffic Monitoring & Anomaly Detection

Sprint	Functional Requirement (Epic)	USN	User Story	Story Points	Priority	Team Member
Sprint-4	Network Traffic Monitoring & Anomaly Detection	USN-7	As a network analyst, I can capture and analyze network packets using Wireshark.	3	Medium	Maaj
Sprint-4	Network Traffic Monitoring & Anomaly Detection	USN-8	As a cybersecurity trainer, I can develop awareness materials on social engineering attacks.	3	High	Bilal

Sprint-5: Cybersecurity Awareness & Preventive Measures

Sprint	Functional Requirement (Epic)	USN	User Story	Story Points	Priority	Team Member
Sprint-5	Cybersecurity Awareness & Preventive Measures	USN-9	As a security educator, I can design training resources focused on best security practices.	3	High	Ayan
Sprint-5	Cybersecurity Awareness & Preventive Measures	USN-10	As a general user, I can learn how to safeguard my personal data against cyber threats.	2	Medium	Maaj

---

3. PROJECT TRACKER, VELOCITY & BURNDOWN CHART (4 Marks)

Sprint Tracker

Sprint	Total Story Points	Duration	Sprint Start Date	Sprint End Date (Planned)	Story Points Completed (as on Planned End Date)	Sprint Release Date (Actual)
Sprint-1	7	4 Days	Feb 22, 2025	Feb 25, 2025	7	Feb 25, 2025
Sprint-2	7	4 Days	Feb 26, 2025	Feb 29, 2025	7	Feb 29, 2025
Sprint-3	7	3 Days	Mar 3, 2025	Mar 3, 2025	7	Mar 5, 2025
Sprint-4	6	3 Days	Mar 4, 2025	Mar 5, 2025	6	Mar 5, 2025
Sprint-5	5	3 Days	Mar 7, 2025	Mar 12, 2025	5	Mar 12, 2025

Velocity Calculation

Velocity = Total Story Points Completed / Number of Sprints
= (7 + 7 + 7 + 6 + 5) / 5

= 32 / 5 ≈ 6.4 story points per sprint

CONCLUSION

This project systematically identifies, analyzes, and mitigates cybersecurity threats through a structured sprint approach. By integrating automated tools and manual verification, it enhances accuracy and minimizes risks. The sprint tracker and velocity analysis ensure efficient progress in securing systems. Real-time monitoring, forensic investigations, and encryption techniques strengthen overall security. Future improvements can focus on AI-driven threat detection and enhanced security awareness programs. This framework provides a solid foundation for building resilient cybersecurity solutions in an evolving digital landscape.