Week 1: Planning and Architecture (Team Lead & All Members)

- **Day 1-2: Requirements Gathering and Refinement:**
  - Detailed discussion of existing DDoS protection system limitations.
  - Define specific goals for "Black Storm" (e.g., specific attack vectors to mitigate, performance targets).
  - Prioritize features based on risk and feasibility.
- **Day 3-4: Architecture Design:**
  - Develop a detailed architecture diagram, outlining all components and their interactions.
  - Select technologies and tools (e.g., programming languages, libraries, cloud services).
  - Define data flow and storage requirements.
- **Day 5: Threat Intelligence and Prediction Planning:**
  - Research and select threat intelligence feeds.
  - Outline the plan for anomaly detection and predictive analysis.
  - Assign tasks for week 2.
- **Day 6-7: Task Assignment and Environment Setup:**
  - Break down the architecture into specific tasks and assign them to team members.
  - Set up development environments, version control (e.g., Git), and communication tools (e.g., Slack, Teams).

Week 2: Core Defense Implementation (Defense Specialist, Software Engineer, Security Analyst)

- **Day 8-10: Multi-Layered Defense Implementation:**
  - Defense Specialist focuses on rate limiting, traffic filtering, and geo-blocking.
  - Begin CDN and DNS protection integration.
- **Day 11-12: Anomaly Detection Development:**
  - Software Engineer starts developing the anomaly detection system (e.g., using machine learning libraries).
  - Start collecting baseline traffic data.
- **Day 13-14: Initial Testing and Incident Response Planning:**
  - Security analyst starts creating basic attack simulations to test the implemented defenses.
  - Begin drafting the incident response plan.
  - Team Lead confirms threat intelligence feeds are working.

Week 3: Adaptive Mitigation and Monitoring (Software Engineer, Team Lead, Security Analyst)

- **Day 15-17: Adaptive Mitigation Development:**

  - Software Engineer implements automated response and dynamic threshold adjustments.
  - Integrate AI-driven mitigation components if possible.
- **Day 18-20: Monitoring and Reporting Development:**
  - Software Engineer develops real-time monitoring dashboards and alerting systems.
  - Security analyst works on SIEM integration and log analysis.
- **Day 21: Integration and Initial Testing:**
  - All team members work on integrating the different components.
  - Initial testing of the integrated system.

Week 4: Testing, Refinement, and Documentation (All Members)

- **Day 22-25: Comprehensive Testing and Vulnerability Assessment:**
  - Security Analyst conducts thorough testing, including simulated DDoS attacks.
  - Identify and address vulnerabilities.
  - Team lead monitors threat intellegence and confirms those feeds are being used correctly.
- **Day 26-27: Refinement and Optimization:**
  - Address any issues identified during testing.
  - Optimize performance and scalability.
- **Day 28: Documentation and Reporting:**
  - Complete documentation of the "Black Storm" protocol, including architecture, implementation details, and incident response procedures.
  - Prepare a final report summarizing the project.
- **Day 29: Final Testing and Review:**
  - Last round of testing.
  - Final code review.
- **Day 30: Presentation and Deployment planning.**
  - Prepare presentation.
  - Discuss deployment planning.