|  |  |
| --- | --- |
| Week | Work Description |
| **1-2** | **Project Kickoff and Initial Assessment**   * Assemble project team * Initial security posture assessment |
| **3-4** | **Planning and Strategy Development**   * Define zero-trust architecture transition plan * Develop threat hunting and incident response protocols |
| **5-6** | **Tool Selection and Procurement**   * Select and procure Crowdstrike’s EDR technology * Begin vulnerability scanning |
| **7-10** | **Infrastructure Setup and EDR Implementation**   * Set up servers and network infrastructure * Initial EDR system implementation and configuration |
| **11-14** | **EDR Development and Testing**   * Develop custom EDR components * Begin continuous vulnerability testing with red team |
| **15-18** | **Deployment and Staff Training**   * Deploy EDR solution across the network * Conduct staff training sessions on the new system |
| **19-22** | **Optimization and Fine-Tuning**   * Optimize EDR configurations based on red team feedback * Fine-tune threat hunting and incident response procedures |
| **23-26** | **Monitoring and Continuous Improvement**   * Initiate continuous monitoring phase * Regularly review and update the security measures |
| **27-28** | **Project Review and Closure**   * Conduct final project review * Document lessons learned and close the project |