**GitHub Security Checklist**

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Feature** | **Checklist Item** | **Details** |
| **Code Scanning** | CodeQL Workflow | Ensure CodeQL analysis is enabled. | Verify that the CodeQL analysis workflow is configured for the repository. |
|  |  | Configure custom queries for CodeQL. | Add specific queries to address the organization's unique security requirements. |
|  |  | Schedule regular scans. | Define a schedule for CodeQL scans, e.g., after every commit or on a nightly basis. |
|  | CodeQL CLI | Verify CLI configuration. | Ensure that the CodeQL CLI is properly installed and configured for local use. |
|  |  | Authenticate the CLI with GitHub. | Confirm that authentication tokens are set up for the CLI to access GitHub repositories. |
|  | 3rd-party Code Scanning Tools | Integrate 3rd-party tools. | Configure additional code scanning tools for enhanced analysis. |
|  |  | Ensure compatibility with GitHub Advanced Security. | Verify that the 3rd-party tools are compatible and correctly integrated with GitHub workflows. |
| **Secret Scanning** | Push Protection for Secrets | Enable push protection. | Activate push protection for repositories to prevent secrets from being committed. |
|  |  | Define custom patterns for secrets. | Add organization-specific secret patterns for scanning. |
|  |  | Regularly update secret definitions. | Ensure that secret definitions are kept current with organizational changes. |
| **Dependency Management** | Dependency Graph | Enable dependency graph. | Confirm that the dependency graph is activated for the repository. |
|  | Dependabot Alerts | Enable Dependabot alerts. | Ensure that alerts are turned on to receive notifications about vulnerable dependencies. |
|  |  | Configure notification preferences. | Define how alerts are delivered, e.g., via email or GitHub notifications. |
|  | Dependabot Version Updates | Activate automatic version updates. | Enable Dependabot to automatically propose updates for outdated dependencies. |
|  | Dependabot Security Updates | Configure Dependabot for security updates. | Set up Dependabot to apply security patches automatically. |
|  | Dependency Review | Enable dependency review for pull requests. | Activate the feature to review changes to dependencies in PRs. |
|  |  | Provide guidance for dependency updates. | Include documentation or links to preferred practices for managing dependencies. |
| **General Governance** | Permissions Management | Restrict access to repositories. | Implement least privilege principles by restricting access to sensitive repositories. |
|  |  | Use granular permissions for tokens. | Ensure personal access tokens have the minimum required permissions. |
|  | Security Alerts Workflow | Define an alert triage process. | Document the steps for investigating and remediating security alerts. |
|  |  | Assign roles for alert management. | Designate specific individuals or teams to manage alerts and remediation. |
|  | Reporting and Metrics | Track security metrics. | Establish metrics for tracking issues such as resolved vulnerabilities, open alerts, and scan coverage. |
|  |  | Generate periodic reports. | Create weekly or monthly summaries of security activity for stakeholders. |