# goblin.tools

- [ ] Create DevSecOps Platform
  - [ ] Define the requirements and objectives for the platform
    - [ ] Identify the purpose of the platform
    - [ ] Determine the target audience
    - [ ] Research the competition
    - [ ] Analyze user needs and preferences
    - [ ] Set measurable goals for the platform
    - [ ] Define the scope of the project
    - [ ] Document the requirements and objectives in a clear and concise manner.
  - [ ] Identify the necessary tools and technologies to be incorporated
    - [ ] Analyze the requirements and objectives for the project
    - [ ] Consider the scope of the project and the type of work to be done
    - [ ] Research the latest tools and technologies relevant to the project
    - [ ] Evaluate the compatibility of the tools and technologies with the existing infrastructure
    - [ ] Determine the budget available for acquiring the necessary tools and technologies
    - [ ] Consult with experts or industry professionals for recommendations
    - [ ] Review and finalize the list of necessary tools and technologies to be incorporated.

- [ ] Set up the development, security, and operation teams for collaboration and integration
  - [ ] Determine the roles and responsibilities of each team
  - [ ] Define the communication and collaboration channels
  - [ ] Establish the tools and technologies needed for integration
  - [ ] Assign team members to work on joint projects
  - [ ] Develop metrics to track progress and effectiveness
  - [ ] Agree on processes and procedures
  - [ ] Implement security measures
  - [ ] Train all teams on collaboration and integration practices
  - [ ] Continuously assess and improve collaboration efforts.
- [ ] Establish workflows and protocols for continuous integration and delivery (CI/CD)
  - [ ] Research established best practices for CI/CD
  - [ ] Evaluate current development processes and identify areas for improvement
  - [ ] Identify tools and technologies that will support CI/CD workflows and protocols
  - [ ] Define the steps necessary for continuous integration and delivery, from code commit to deployment
  - [ ] Develop guidelines and documentation for consistent use of the CI/CD workflows and protocols by the development team
  - [ ] Train the development team on the new workflows and protocols
  - [ ] Implement and monitor the new CI/CD workflows and protocols to ensure they are functioning as intended.

- [ ] Implement security measures throughout the software development lifecycle (SDLC)
  - [ ] Analyze potential risks and threats to software
  - [ ] Design security into every phase of the SDLC
  - [ ] Implement security controls, such as firewalls and encryption
  - [ ] Continuously monitor and test the security measures in place
  - [ ] Remediate any vulnerabilities discovered during testing
  - [ ] Educate all members of the software development team on security best practices
  - [ ] Keep up to date on current security issues and adjust security measures accordingly
  - [ ] Regularly review and update security policies and procedures for the SDLC.

- [ ] Automate testing and monitoring processes
  - [ ] Identify the systems or applications that require testing and monitoring
  - [ ] Determine the tools and technologies that will be used for automated testing and monitoring
  - [ ] Develop test cases and scripts that will simulate different scenarios and events
  - [ ] Integrate testing and monitoring into the software development lifecycle
  - [ ] Execute automated tests to identify any bugs, errors, or vulnerabilities
  - [ ] Set up notifications and alerts for when certain thresholds are reached or events occur
  - [ ] Continuously monitor and improve testing and monitoring processes to ensure optimal performance and accuracy.

- [ ] Provide training and support to all stakeholders involved in the platform
  - [ ] Identify all stakeholders involved in the platform
  - [ ] Develop a training and support plan
  - [ ] Communicate the plan to stakeholders
  - [ ] Schedule training sessions
  - [ ] Facilitate training sessions
  - [ ] Provide ongoing support to stakeholders as needed
  - [ ] Evaluate effectiveness of training and support efforts
  - [ ] Adjust training and support plan as necessary
- [ ] Continually assess and improve the platform based on feedback and metrics
  - [ ] Review feedback from platform users
  - [ ] Analyze metrics related to platform performance
  - [ ] Identify specific areas for improvement
  - [ ] Develop a plan for implementing improvements
  - [ ] Implement changes to the platform
  - [ ] Monitor and measure the impact of changes made
  - [ ] Continue to gather feedback and adjust as needed.