

GH-100T00: GitHub fundamentals - Administration basics and product features

Course Outline

1) GitHub fundamentals Administration basics and product features Part 1 of 2

- Introduction to GitHub
 - Identify the fundamental features of GitHub
 - Learn about repository management
 - Gain an understanding of the GitHub flow, which includes branches, commits, and pull requests
 - Explore the collaborative features of GitHub by reviewing issues and discussions
 - Recognize how to manage your GitHub notifications and subscriptions
 - Lab: A guided tour of GitHub
- Introduction to GitHub administration
 - Summarize the organizational structures and permission levels that GitHub administrators can use to organize members in order to control access and security
 - Identify the various technologies that enable a secure authentication strategy allowing administrators to centrally manage repository access
 - Describe the technologies required to centrally manage teams and members using existing directory information services
 - Describe how you can use GitHub itself as an identity provider for authentication and authorization
- Introduction to GitHub's products
 - Define the difference between the different types of GitHub accounts: Personal, Organization, and Enterprise
 - Explain each GitHub plan: GitHub Free for personal accounts and organizations, GitHub Pro for personal accounts, GitHub Team, and GitHub Enterprise
 - Distinguish the features associated with accessing GitHub on GitHub Mobile and GitHub Desktop
 - Describe a brief overview of GitHub billing and payments
- Maintain a secure repository by using GitHub best practices
 - Identify the tools and GitHub features to establish a secure development strategy
 - Enable vulnerable dependency detection for private repositories
 - Detect and fix outdated dependencies with security vulnerabilities
 - Automate the detection of vulnerable dependencies with Dependabot
 - Add a security policy with a SECURITY.md file
 - Remove a commit exposing sensitive data in a pull request
 - Remove historical commits exposing sensitive data deep in your repository
 - Lab: Secure your repository's supply chain

2) GitHub fundamentals Administration basics and product features Part 2 of 2

- Manage sensitive data and security policies within GitHub
 - Create documentation that details security guidelines and useful information for collaborators
 - Set permissions and other rules
 - Automate processes that prevent security breaches
 - Respond to security breaches
- Authenticate and authorize user identities on GitHub
 - Be able to describe the Authentication and Authorization Model
 - Understand how to manage user access to your GitHub organization through Authorization and Authentication tools
 - Identify the supported identity providers and technologies that support secure repository access
 - Understand the implications of enabling SAML SSO
 - Identify the authorization and authentication options available, and understand the administrator's role in enforcement of a secure access strategy for a GitHub enterprise
 - Describe how users access private information in a GitHub organization
 - Evaluate the benefits of enabling Team Synchronization to manage team membership
- GitHub administration for enterprise support and adoption
 - Set up authentication with Security Assertion Markup Language (SAML) single sign-on and a connection between Enterprise Server and Enterprise Cloud with GitHub Connect
 - Automate security and version updates for your project's dependencies, as well as administrative duties and user interactions with GitHub
 - Identify when to open a ticket with GitHub Enterprise Support to resolve issues
 - Recognize the capabilities of centrally managing your GitHub enterprise members through GitHub Enterprise Managed User accounts (EMUs)
- Manage GitHub Actions in the enterprise
 - Identify the different tools you can use at enterprise and organization levels to manage your actions and workflows
 - Evaluate what the appropriate runners are for your enterprise instance
 - Discover the different configurations available for self-hosted runners and customize them according to your enterprise use case
 - Understand what encrypted secrets are and how to use them in your actions and workflows
 - Lab: Use a repository secret in a GitHub Actions workflow
- Leverage GitHub Actions to publish to GitHub Packages
 - Understand what a Package Repository is and when to use it
 - Set up a Continuous Integration (CI) workflow with GitHub Actions to publish to GitHub Packages
 - Validate your knowledge with an exercise that checks your ability to publish to a GitHub Packages registry
 - Identify how to authenticate, install, and manage GitHub Packages
 - Lab: Publish to a GitHub Packages registry