BLACK DUCK SECURITY GITHUB APP

The Black Duck Security app streamlines the onboarding and continuous synchronization of GitHub repositories with Black Duck Polaris™ Platform, Black Duck® SCA, and Coverity® Static Analysis. This enables development and security teams to easily configure and automate static application security testing (SAST) and software composition analysis (SCA) scans of your development projects at scale.

IMPROVE SECURITY WHILE MAINTAINING DEVELOPER PRODUCTIVITY

Scans can be triggered by code commits and pull requests, with automated fix pull requests and scan results available as PR comments. This improves application security and accelerates developer productivity by providing actionable feedback within their preferred GitHub workflows.

The ability to onboard repositories in bulk improves your security posture by enabling policy-driven code scans to be run across your full portfolio of applications. Policy enforcement is automated, with the ability to break builds and flag violations when they occur.

Key capabilities include

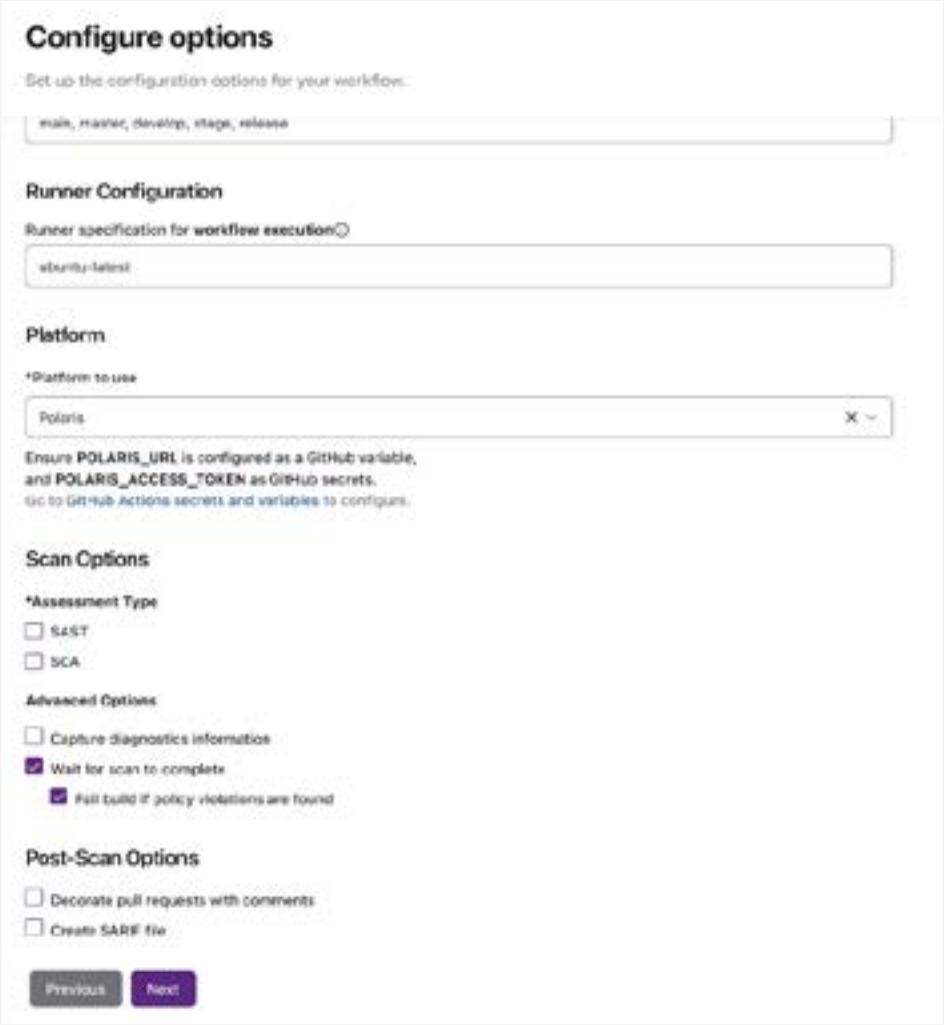
- Bulk onboarding and configuration of GitHub repositories at scale
- Automated SAST and SCA scans triggered by code commits and pull requests
- Scan results added as pull request comments for discovered issues
- Automated fix pull requests for vulnerable open source dependencies
- Customizable policy enforcement with the ability to fail builds if violations exist
- SARIF reports integrated into GitHub Advanced Security dashboards

For more information, please visit https://github.com/marketplace/black-duck-security

HOW TO USE THE BLACK DUCK SECURITY APP

To use the Black Duck Security app

1. Access the app from the GitHub Marketplace.
2. Install the app to one or more organizations.
3. Select the organization and repositories to onboard.
4. Choose the Black Duck product you want to integrate.
   - Polaris
   - Black Duck SCA
   - Coverity
5. Configure the options for the selected Black Duck product. *Configure scan options for your repositories by choosing the affected branches, which events will trigger scans, and which Black Duck products to integrate with.*
6. Review the workflow file. Users can configure advanced options, if necessary.
7. Click Submit to add the workflow into the selected repositories.



About Black Duck

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.