COMPLIANCE AND CONTINUOUS ATO

Uniting Security and Development with GitLab and Anchore

GitLab

*"Security is the core of the **DoD DevSecOps Initiative** and Platform One. Because both Anchore and GitLab have been approved as hardened containers in **Iron Bank**, organizations using these tools can obtain Certificate to Field (CtF) and Continuous Authority to Operate (cATO) authorization to go live with their applications faster. Developers have the ability to push validated code into production on an ongoing basis, resulting in shorter development cycles, less debugging, and more rapid feature development,"* said Rob Slaughter, Director of DoD Platform One.

Deploy Containers With Confidence

With the increase of high-profile breaches, it is becoming more clear that being in compliance does not necessarily equal being secure. And while most dev teams want a secure software development lifecycle, the increasing pressure to get to market faster means checking the boxes—and no more. With the easy-to-use Anchore and GitLab integration, you'll be able to speed up compliance—whether you're looking to meet DoD cATO or FedRAMP compliance.

DevOps Power

Enterprises across the public sector rely on GitLab's source code management and CI/CD capabilities to deliver software rapidly.

Uniquely Suited for Government Agencies

Anchore's approach to container security and compliance is a perfect fit for federal agencies implementing modern DevSecOps practices—and has become the de facto standard in DoD reference implementation.

Better Together

Combining these tools provides a seamless management of your risk profile in one place through GitLab's Risk Management Framework (RMF)—reducing the friction of typical software security scanning.

Key Capabilities

Centralized Risk Management Framework provides you with easy access to your security issues that are automatically populated and generated within your GitLab user interface.

Automated security makes a developer's life easier by having quick access to review and perform any necessary audits.

Easy-to-use security tools provide security scanning for those who have been reluctant to integrate before—ensuring critical steps are not bypassed.

Out-of-the-box policy enforcement developed for the public sector unites your security and development teams—keeping everything in compliance.

Faster time to compliance for public sector agencies looking to meet DoD regulations or FedRAMP ATO.

Adding Anchore Scanning to GitLab—As Easy as 1-2-3!

1

In your GitLab project repository, ensure that the following variables are set in Settings > CI/CD > Variables:

- ANCHORE_CLI_URL
- ANCHORE_CLI_USER
- ANCHORE_CLI_PASS

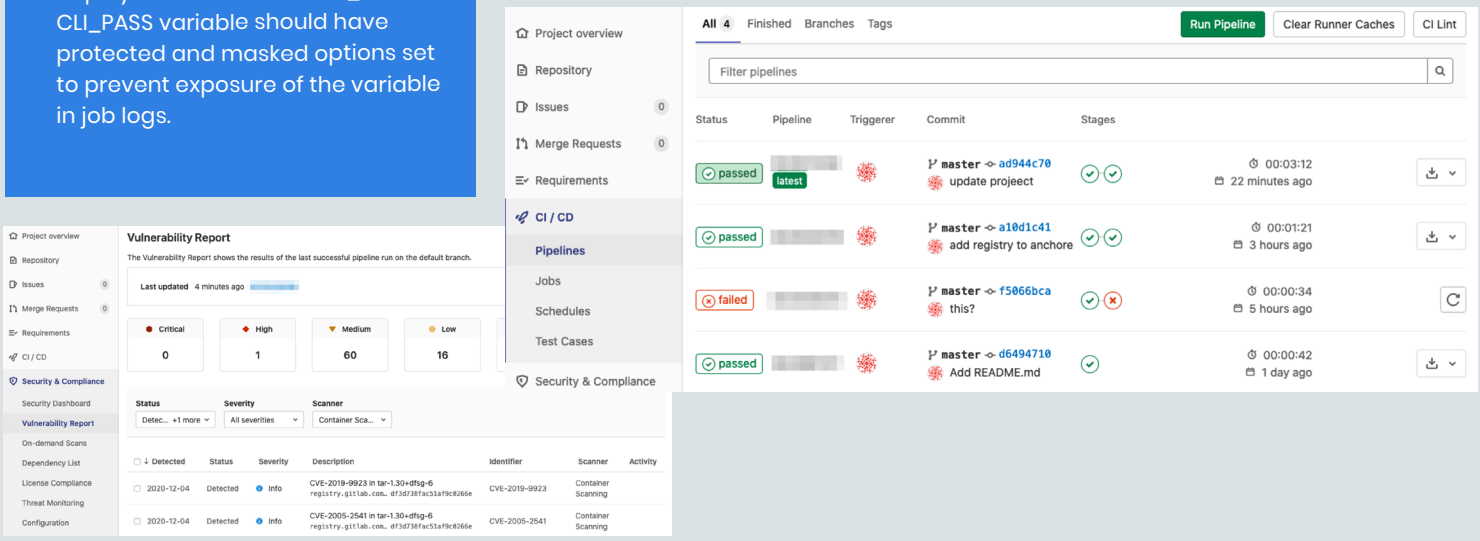
This allows the integration to access your Anchore Enterprise deployment. The ANCHORE_CLI_PASS variable should have protected and masked options set to prevent exposure of the variable in job logs.

2

In your project's .gitlab-ci.yml, include the code snippet anywhere in your CI flow after your target container image has been built and pushed to the GitLab Container Registry that you have made accessible from your Anchore Enterprise deployment. Visit docs.anchore.com to get the code.

3

After a successful scan, results will be available for review and management using GitLab's native security features. Navigate to your project's Security & Compliance > Vulnerability Report UI to review any discovered vulnerabilities in your container image.



Anchore enables organizations to speed digital transformation and reduce risks by streamlining the development of secure and compliant cloud-native applications. Anchore's solutions integrate with the DevOps toolchain to automate security and compliance checks throughout the software development lifecycle. Organizations can reduce costs and accelerate time to market by remediating security and compliance issues early and continuously. Headquartered in California with offices in Virginia and the UK, Anchore's customers include large enterprises and government agencies that require secure and compliant cloud-native applications. To learn more about Anchore's solutions, visit www.Anchore.com.

anchore.com/enterprise info@anchore.com

anchore