





Git Security Posture

Measure and Evaluate Git Security Posture
Powered by the Open SSF Framework



Securing software development workflows is critical for protecting intellectual property, sensitive data, and production systems. Git repositories, as the cornerstone of modern software development, must be monitored and safeguarded against vulnerabilities, misconfigurations, and threats. OpsMx Delivery Shield provides a robust framework for assessing and improving the security posture of your Git repositories.

Why Measure Git Security Posture?




-  **Prevent Unauthorized Access:** Protect source code from malicious actors by ensuring robust access controls.
-  **Maintain Integrity:** Identify and mitigate risks such as accidental secrets exposure, code tampering, and configuration errors.
-  **Comply with Standards:** Meet industry security standards and regulations for software development.
-  **Enable Continuous Improvement:** Leverage data-driven insights to enhance security practices iteratively.

OpsMx Delivery Shield Git Security Posture

OpsMx Delivery Shield measures and evaluates Git security posture as part of its comprehensive application security solution. OpsMx Git Security Posture is built on the OpenSSF framework to offer guidelines, tools, and practices to systematically assess and improve the security of software and repositories. Key components include:




- **Scorecards:** Automated security health checks for Git repositories.
- **Best Practices:** Encourages adherence to security and operational best practices.
- **Criticality Score:** Identifies high-priority repositories requiring attention.
- **Securing Critical Projects:** Tailored guidance for mission-critical software.

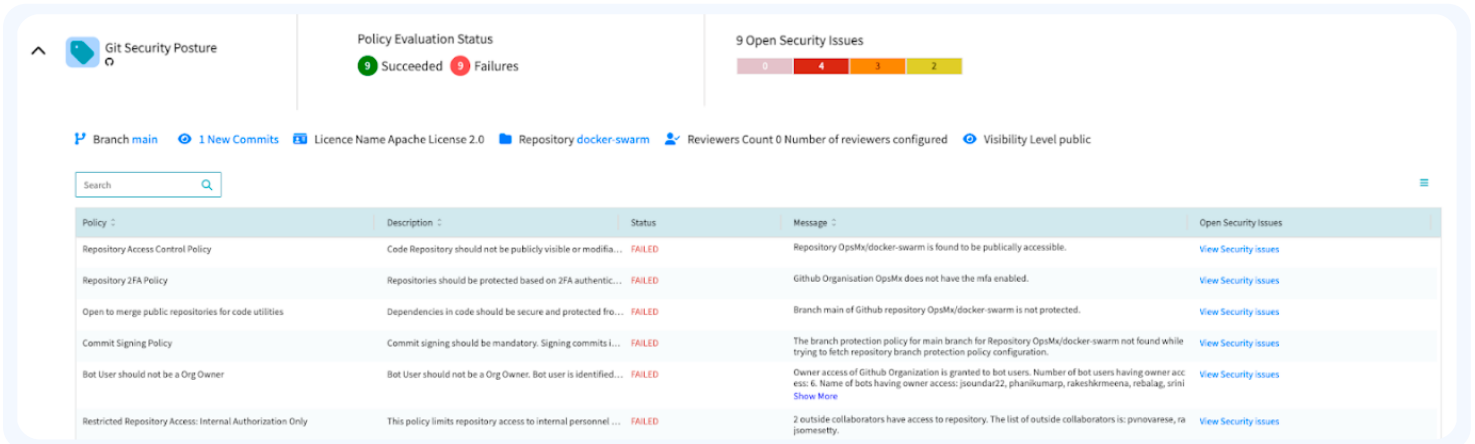
Measuring Git Security Posture

-  **Conduct Automated Assessments**
 - **Run Git Security Assessment:** Use the tool to analyze your repository across metrics like branch protection, dependency updates, and code review practices.
 - **Assess Dependency Management:** Identify vulnerabilities in third-party libraries.
-  **Enforce Secure Configurations**
 - **Implement Branch Protections:** Require reviews and signed commits for changes.
 - **Enable Two-Factor Authentication (2FA):** Ensure contributors use 2FA for their accounts.
 - **Secrets Scanning:** Identify and remediate exposed secrets.
-  **Track and Report Progress**
 - **Establish a Baseline:** Record the initial security posture.
 - **Monitor Metrics:** Regularly update the security posture results and compare them against your baseline.
 - **Communicate Findings:** Share reports with stakeholders to highlight improvements and areas needing focus.



Benefits of Using the OpsMx Delivery Shield Git Posture Framework

-  **Comprehensive Insight:** Gain a clear understanding of your repository's security strengths and weaknesses.
-  **Enhanced Collaboration:** Foster a security-first culture among developers.
-  **Scalable Solutions:** Address risks in both small and large repositories efficiently.



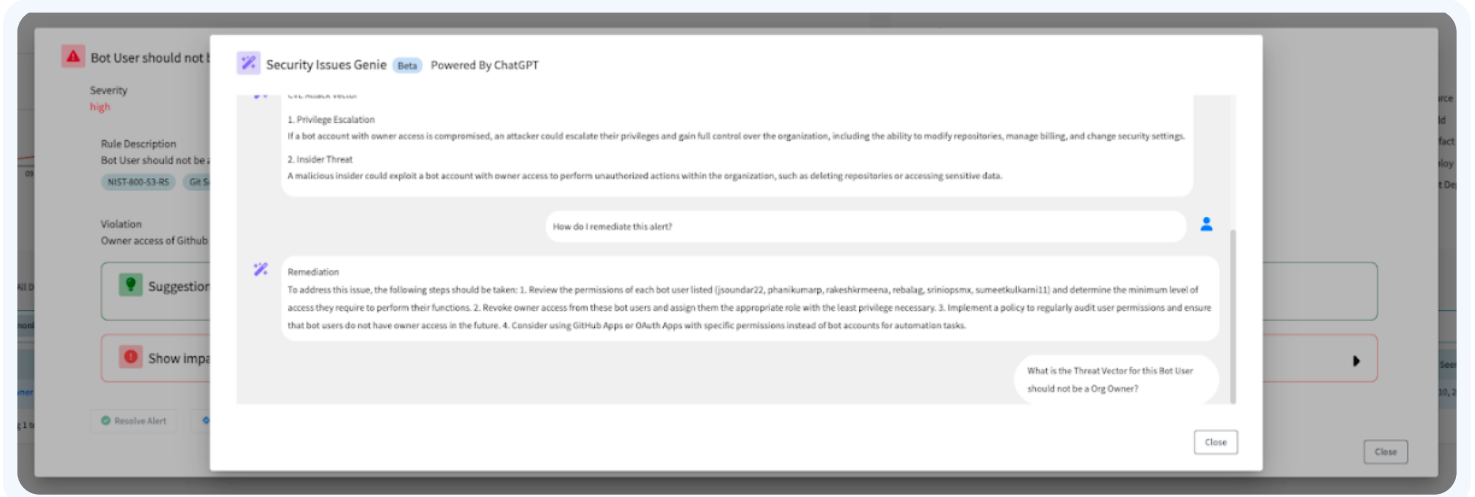
Git Security Posture

Policy Evaluation Status: 9 Succeeded, 9 Failures

9 Open Security Issues

Branch: main | 1 New Commit | Licence Name: Apache License 2.0 | Repository: docker-swarm | Reviewers Count: 0 | Visibility Level: public

Policy	Description	Status	Message	Open Security Issues
Repository Access Control Policy	Code Repository should not be publicly visible or modifi...	FAILED	Repository OpsMx/docker-swarm is found to be publicly accessible.	View Security issues
Repository 2FA Policy	Repositories should be protected based on 2FA authentic...	FAILED	Github Organisation OpsMx does not have the mfa enabled.	View Security issues
Open to merge public repositories for code utilities	Dependencies in code should be secure and protected fro...	FAILED	Branch main of Github repository OpsMx/docker-swarm is not protected.	View Security issues
Commit Signing Policy	Commit signing should be mandatory. Signing commits i...	FAILED	The branch protection policy for main branch for Repository OpsMx/docker-swarm not found while trying to fetch repository branch protection policy configuration.	View Security issues
Bot User should not be a Org Owner	Bot User should not be a Org Owner. Bot user is identifi...	FAILED	Owner access of Github Organization is granted to bot users. Number of bot users having owner access: 6. Name of bots having owner access: jsoundar22, phanikumarp, rakeshkrmeena, rebalag, srini Show More	View Security issues
Restricted Repository Access: Internal Authorization Only	This policy limits repository access to internal personnel ...	FAILED	2 outside collaborators have access to repository. The list of outside collaborators is: pxnovarese, rajmesetty.	View Security issues



Bot User should not be an Org Owner
Severity: High

Rule Description: Bot User should not be an Org Owner (NIST-800-53-R5, Git S...)

Violation: Owner access of Github...

Security Issues Genie (Beta) Powered By ChatGPT

Threat Vector

- Privilege Escalation**
If a bot account with owner access is compromised, an attacker could escalate their privileges and gain full control over the organization, including the ability to modify repositories, manage billing, and change security settings.
- Insider Threat**
A malicious insider could exploit a bot account with owner access to perform unauthorized actions within the organization, such as deleting repositories or accessing sensitive data.

How do I remediate this alert?

Remediation
To address this issue, the following steps should be taken: 1. Review the permissions of each bot user listed (jsoundar22, phanikumarp, rakeshkrmeena, rebalag, sriniopsmx, sumeetkulkarni11) and determine the minimum level of access they require to perform their functions. 2. Revoke owner access from these bot users and assign them the appropriate role with the least privilege necessary. 3. Implement a policy to regularly audit user permissions and ensure that bot users do not have owner access in the future. 4. Consider using Github Apps or OAuth Apps with specific permissions instead of bot accounts for automation tasks.

What is the Threat Vector for this Bot User should not be a Org Owner?

Close

ABOUT US

OpsMx secures and intelligently automates software delivery from developer to deployment, building on an Open Software Delivery architecture and AI/ML-powered DevSecOps. OpsMx products and services enable hundreds of thousands of developers at Google, Cisco, Western Union, and other leading global enterprises to ship better software faster.

FOR MORE INFORMATION, CONTACT US:

OPSMX, INC | 350 OAKMEAD PKWY, SUNNYVALE, CA 94085 | INFO@OPSMX.COM
WWW.OPSMX.COM/SECURE SOFTWARE DELIVERY