

MAXIMIZING GITHUB'S POTENTIAL

GITHUB SECURITY ASSESSMENT

GitHub **security starts at the organizational level**, as attacks on source code within the software development lifecycle can occur from various GitHub misconfigurations. Within GitHub, there are a plethora of features available to ensure your environment is locked down. Our GitHub review focuses on:



Identity



Organizational configuration



Developer collaboration



Security coding best practices



OWASP top 10 CI/CD Security risks

Together with the security features of Github and third-party tooling, an assessment of the environment will be made, analyzed, and presented to the customer. We adhere to organization **best practices** which include assigning multiple owners, and using Teams for managing access and sending notifications. For GitHub Enterprise users, the implementation of policies becomes an essential tool in enforcing and making organization settings and features readily available.

GITHUB SECURITY FEATURES

Private Repositories	Multi-Factor Authentication	Required Reviews	Secret Scanning	Dependency graph	Dependency review in PR
✓	✓	✓	✓	✓	✓

✓ included

✓ Github Advanced Security needed