ROAR Third-Party Vendor Assessment Report

Vendor: GitHub
Assessor: Adam Richie-Halford, ROAR Information Security Officer

Overview

GitHub is a widely used platform for version control and collaboration in software development, known for its comprehensive security practices. This assessment evaluates GitHub's compliance with industry standards and certifications, verifying its suitability as a third-party vendor for managing ROAR's code and development workflow.

Certifications and Compliance

- **SOC 2 Type II**: GitHub complies with SOC 2 Type II, which validates its security, availability, confidentiality, and privacy controls. The certification ensures that GitHub maintains effective data protection measures and robust security controls.
- **ISO 27001**: GitHub is certified under ISO 27001, an international standard for information security management systems (ISMS). This certification demonstrates GitHub's commitment to systematically managing and protecting sensitive information.
- **Cloud Security Alliance (CSA)**: GitHub has undergone assessments under the CSA STAR certification, which evaluates the security of cloud service providers.

Compliance details and reports can be accessed through the GitHub Security Page.

Security Practices

It is important to note that GitHub's security compliance confers no security benefits to ROAR if ROAR developers do not follow security controls. I recommend that all ROAR developers adhere to the following security controls.

1. **Access Control** Access to GitHub is performed using two-factor authentication and is restricted to authorized personnel.
2. **Code Review** Code changes must be reviewed and approved in order to progress through the software development life cycle (SDLC) and deploy a version to production.
3. **Code Vulnerability Scanning**: Vulnerability scans for the source code are performed to identify security issues. High/critical issues are remediated in a timely manner.

4. **Automated Tests**: A successful test result is mandatory in order to continue with the SLDC and deploy a version to the production environment.
5. **Test Failure**: In case test failures are detected, a notification is sent to relevant stakeholders. Any code change with a failed test cannot be deployed into production.
6. **Change Approval**: All code changes need to be approved/authorized, prior to being deployed into production.

Conclusion

GitHub's compliance with SOC 2 Type II, ISO 27001, and its robust security practices make it a reliable platform for managing code and collaborating on development projects securely.