GitHub and Government

DevSecOps for government agencies, the GitHub way

The key to the government's ability to innovate at speed is access to secure, high-quality software. But the path to production, including strict compliance standards for security, governance, and accreditation, can add months—or years—to delivery cycles. Even after moving to the cloud, these delays can slow down innovation and pose a risk to your organization's critical goals and needs. Instead, successful digital transformation depends on implementing security earlier in your DevOps pipeline—the process of "shifting security left" also known as DevSecOps.

With event auditing, compliance tooling, governance engines, enforced workflows, and constant transparency, GitHub is an important part of any government organization's digital transformation. Government agencies can quickly innovate using modern software development workflows, while decreasing time to delivery and improving security. And by implementing a DevSecOps process that includes cloud provisioning and orchestration, developers can build without added input from operations teams. Whether you're at the federal or local level, a cloud deployment model with GitHub will help you support your constituents and deliver the digital experiences they rely on.

Building more secure software, faster

As many government agencies know, one of the biggest challenges to security and compliance is obtaining an authority to operate (ATO). GitHub simplifies and accelerates this process by allowing security professionals to standardize how applications are built, and adopt automated—not manual—controls. GitHub also helps teams provide and enforce known secure baselines and settings, plus secure code and practices. Organizations can create and map transparent audit logs to known NIST 800-53 controls and evidence. This allows security professionals to understand the impact of development activities in real time and better manage risk.

By streamlining and automating the tasks above, GitHub allows teams and projects to adopt a continuous accreditation posture. Instead of waiting

for final code review, teams can perform some of these security tasks earlier in the development process, keeping friction low to speed up compliance and innovation. GitHub supports an organization's ability to "shift left"—finding and preventing defects as they arise in the software delivery process. This allows teams to capitalize on DevSecOps and the innovative, modern software development practices provided by commercial cloud environments.

Building your DevSecOps workflow

Shifting left increases collaboration, creates better code, and maintains security and compliance—but requires technology that can keep up. From automated workflows to built-in code review, GitHub helps your organization detect security vulnerabilities sooner and prevent them in the first place.

Secure development environment

The systems you build are only as secure as the systems you build them on, so having an end-to-end, Impact Level 5 (IL5) environment confirms that all activity is secure from the start. Deployed in your IL5 of choice, GitHub brings a secure developer application environment built on top of the cloud platform's already-proven security and infrastructure.

Full event traceability and auditing

GitHub's audit log tracks all software development and user events that happen in the system. You can use these events and processes to verify that you're meeting specific security controls, then automatically create and manage security artifacts by translating raw security data into the format that works for you.

GitHub Actions

GitHub Actions is a task scheduling, automation, and integration framework that serves as the foundation for taking software from concept to a secure, compliant production solution. By

automating your tasks, you'll depend less on manual controls and processes and create a more repeatable and reliable authorization process. Actions also integrates with GitHub's policy enforcement, allowing you to enforce required workflows, processes, and tools automatically.

Peer code review

Code review enforces processes and two-person rules that reduce errors and promote best practices, like requiring two sets of approval before changes are merged or deployed. Using GitHub's built-in policy controls, you can be certain that no code makes it into production without proper checks and validations.

Rich integration platform

Thanks to a diverse API surface, GitHub not only supports collaboration with developers and security experts, but with tools and automation as well. This allows you to bring the newest development and security tools to your software development life cycle, while letting you keep and rely on many of the tools that are part of your secure systems today.

Policy and user enforcement

GitHub includes a full-featured, RBAC-backed authentication and authorization layer, so you can manage specific permissions and access. GitHub's policy enforcement framework ensures that the entire software development lifecycle—including code revisions, change management, build tools, and testing—happens in just the way regulations require.

Pre-approved templates

Building off your defined cloud governance implementation, GitHub lets you define pre-configured assets, workflows, and environments to accelerate the accreditation process. These templates, workflows, and scripts all help you to create, build, and deploy regulated workloads, making the acceptance of pre-audited type accreditation possible.

Governance as code

Governance as code simplifies and standardizes deployed assets in the same way as managing infrastructure as code does for the cloud. You can

define your project configurations, workflows, and even policy as code, building an audit trail to guarantee compliance. These items of governance, along with rich audit details, give you a 360-degree view into your product's development compliance.

Supply chain vulnerability awareness

GitHub provides tools to manage the code that your team writes and the code that it relies on to support your mission. This code may come from large, established software vendors or from top developers working on open source projects. Regardless of its source, GitHub works closely with security experts at Mitre and elsewhere in the public and private sector to help you understand the code in your software supply chain and make sure you're protected from undue risk.

GitHub uses the data from your software supply chain, the results of your workflows and builds, and your policy, governance, and implementations to create a software bill of materials or OSCAL document. You can then use the document GitHub creates to communicate your product's compliance and security posture.

Best of breed secure code analysis

For organizations who need an additional level of code security, GitHub offers GitHub Advanced Security: a state-of-the-art, first-class code scanning solution. Capable of finding novel, unique, and ever-changing software vulnerabilities, Advanced Security uses the world's most powerful code analysis engine, CodeQL, to help your security team and developers work together to protect your code.

Additional components, including secret scanning, software composition analysis, and dynamic application testing verify that your code and mission stay secure.

Shipping software that's more secure doesn't mean sacrificing speed or innovation. Developers and security teams can build safer applications by making security part of the development lifecycle from step one. Combined with GitHub and the deployment capabilities found in leading cloud platforms, your team can create a DevSecOps pipeline that meets government standards without compromise.

Questions about DevSecOps? We're here to help.

SALES@GITHUB.COM
GITHUB.COM/ENTERPRISE

GitHub and Government