How KPMG helps clients reduce risk and accelerate software delivery with GitHub Security Campaigns

Leveraging GitHub Copilot Autofix to achieve remediation at scale

What are GitHub Security Campaigns?

A Security Campaign is a targeted effort to remediate identified vulnerabilities at scale using AI. Security Campaigns can be created for specific alerts generated by CodeQL and are launched for a defined period to simplify how teams tackle security debt.

Improved security posture

- Copilot Autofix automates remediation at scale, **reducing the time vulnerabilities are left unaddressed** and offers a more **reliable** and **consistent** approach to security patches.

Increased developer productivity

- By automating remediation and integrating directly with pre-existing workflows, our data shows a potential **69% reduction in time** spent on manual security-tasks with Copilot Autofix, allowing developers to spend more time on other essential development activities.

Tech debt reduction

- With AI-powered remediation at scale with CoPilot Autofix, Security Campaigns help to **reduce resource demands and pay down security debt** by accelerating the remediation process through automated PRs with security fixes at the time of detection.

Copilot code explanation

Provides explanations of identified security vulnerability, the code generated to address it, and steps to remediate the vulnerability

Copilot Autofix

Automatically suggests code to fix the security alert generated with static code analysis powered by CodeQL

Campaigns progress dashboard

View key metrics around your Security Campaign, including completion rate, average remediation time, percent of Autofix PRs merged, and time remaining

Developing a tailored strategy for remediation at scale

What level of support do you need from KPMG?

The KPMG approach enables a thorough adoption strategy and implementation plan for Security Campaigns. Whether your organization is looking for assistance with getting started by launching the first Security Campaign or is seeking hands-on support to leverage Copilot's Autofix capabilities at scale, KPMG offers varying levels of support to meet your needs.

	Tech Stack & Ecosystem Analysis	Security Campaign Set Up & Launch	Security Fixes with Autofix PRs	KPI Development & Tracking
High	In-depth analysis of application portfolio and organization security posture to target applications for current and future Security Campaigns	Full ownership of the Security Campaign lies with KPMG from start to finish	PRs generated by Autofix will be reviewed and merged by KPMG	KPIs will be developed and tracked by KPMG, and reports will be generated for upward communication
Medium	Identification of target applications through a comprehensive review of application portfolio and security vulnerabilities	Some hands-on guidance is provided around Security Campaign target and duration, but organization is responsible for managing day-to-day tasks	Detailed guidance and occasional hands-on assistance will be provided around PRs generated by Autofix	Tailored KPIs will be developed, and a system for tracking and reporting will be setup
Low	Identification of a low-risk, low-priority application	Basic guidelines and recommendations will be provided, but the organization is responsible for Security Campaign configuration and launch	Recommendations will be provided around merging PRs generated by Autofix, but the organization is responsible for the merge	High-level KPIs will be developed leveraging those already built-in to Security Campaigns

KPMG uses Security Campaigns to scale vulnerability remediation and let developers focus on features

Feature	Description
Static Code Analysis	Analyzing source code for security vulnerabilities and coding errors.
	Generating alerts of varying severities for security vulnerabilities detected.
Security Fix Generation	Auto-generating security fixes for common security vulnerabilities.
	Auto-generating security fixes for alerts generated from custom analysis.
Documentation	Breaking down complex security fixes into simpler steps.
	Explaining security fixes in plain language for easier understanding.
End-to-End Remediation	Automatically fix new alerts in pull requests generated.
	Automatically fix alerts in pull requests that are in the backlog.
Remediation Optimization	Tracking progress towards a defined goal and deadline.
	Generating key metrics around remediation and auto-fix efficiency.
Scalability & Adaptability	Translating to multiple ecosystems within an organization.
	Adapting to vulnerability type and amount present.
Compliance & Governance	Monitoring and tracking of organization and repository-specific security posture.
	Maintaining an audit trail and version history of security-related activities.
Workflow Integration	Providing support for multiple languages and frameworks already in use.
	Integrating with existing developer workflows and processes.

Why KPMG?

KPMG has an experienced team who will bring a unique approach in helping your organization leverage GitHub Security Campaigns. With our deep experience and understanding of GitHub Advanced Security (GHAS) capabilities, we can help you unlock the potential of GHAS, customized to your needs and objectives. Our subject matter professionals guide you through each phase of the journey and go beyond the technology to support robust and sustainable security management with the implementation of GHAS.

GitHub certified resources

The KPMG team boasts over 200 GitHub certified professionals and is among the system integrators with one of the highest number of certified resources, providing a highly-skilled and diverse pool of talents equipped to deliver GHAS work.

Intimate GitHub strategy experience

KPMG assisted GitHub in creation of its Well Architected Framework, an opinionated guide to smart adoption of the GitHub platform.

Broad range of clients

The KPMG team has worked with clients across various industries to deliver GHAS work, bringing insights and leading practices from all industries to best suit your organization.

Typical Scope of services:

Adoption Enablement: Increase understanding of GHAS capabilities across organizations and empower developers to leverage the tool directly in the development pipeline

Tool Integration: Provide detailed step-by-step guides and leading practices for tool rollout throughout organizations, starting with the tools easiest to implement that are designed to reduce the most risk

Long-Term Support: Develop customized documentation and an adoption roadmap to empower organizations to use GHAS even after real-time support has ended

Contact us

Caleb Queern
Managing Director, Advisory
Cyber Security Services
cqueern@kpmg.com

Shahn Alware
Managing Director, Advisory
CIO Advisory
salware@kpmg.com

Jackie Mak
Director, Advisory
Cyber Security Services
jackiemak@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related. entities

Learn about us: in **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.