COALFIRE

DATA SHEET

Secure code review

The roots of remediation are often found at the source

To create resilient software, secure-coding decisions must take place long before any code is developed. While no single approach can eliminate or identify all risk, a secure code review leverages the power of humans to go beyond static and dynamic testing and generate powerful insight that can prevent issues. That's why independent code reviews should be incorporated at critical audit checkpoints within the software development lifecycle (SDLC).

Our secure code review approach

We logically break down your application in a manner that allows for a thoughtful review of the most security-critical features and functionality, resulting in actionable, development-level remediation strategies for all issues identified – from hard-coded credentials to flaws surrounding encryption implementation.

Conduct manual review: Application code is manually reviewed to evaluate the approach taken for third-party and open source dependency usage, data validation, session management, authentication, and authorization logic validation. We also help minimize the attack surface and organizational risk exposure by validating adherence to secure-coding best practices.

Utilize automated tools: To ensure a comprehensive code review, we augment manual code reviews, where applicable, with automated static analysis via commercial, custom-built, and open-source tools. We also examine your design for weaknesses and flaws, like legacy interoperability and insecure architectural dependencies, which may result in security compromises.

Report and debrief: Your team will receive an executive summary and technical details that contain a unique description of each vulnerability, supporting screenshots and evidence, severity and impact, and remediation recommendations.

Promote prevention to avoid reaction

Maintaining the highest level of quality to the source code your organization creates helps promote stability and maintainability of the application's architecture and individual code modules. Including regular code reviews as part of an SDLC should reduce the overall cost of development and result in fundamental net gains, such as:

- Increased developer skills for writing architecturally sound and secure code
- Code that results in fewer bugs as found by quality assurance

Why Coalfire

- Our AppSec consultants have experience in both software engineering and security consulting, which means we're able to deliver modern, actionable guidance on all aspects of application security.
- We conduct more than 1,000 complex projects each year for clients in the technology, healthcare, financial, manufacturing, energy, and retail industries.
- Our team comprises experienced testers of the world's largest cloud service providers, including Amazon, Google, IBM, Microsoft, Oracle, and Salesforce.
- For the past 10 years, we have trained and educated security professionals at Black Hat in the advanced tradecraft we developed.

Get proactive insight to prevent production-based reactions.

Learn more about Coalfire's secure code reviews.

Coalfire.com | 877-224-8077

COALFIRE.

About Coalfire

The world's leading organizations – including the top five cloud service providers and leaders in financial services, healthcare, and retail – trust Coalfire to elevate their cyber programs and secure the future of their business. Number one in compliance, FedRAMP®, and cloud penetration testing, Coalfire is the world's largest firm dedicated to cybersecurity services, providing unparalleled technology-enabled professional and managed services. To learn more, visit **Coalfire.com**.