Case Study: Cutting Security Remediation Time by 85%

Overview

Fletch helps small and mid-sized businesses cut through security alert noise by putting threat intelligence into context. Its platform prioritizes vulnerabilities so teams can focus on what matters most. With a lean, R&D-driven team, Fletch needed a way to streamline security workflows without slowing down developers.

Darien Kindlund
VP of Technology, Fletch Security

The Challenge

Fletch wanted to speed up remediations from its developers—while avoiding situations where multiple senior devs had to coach juniors on the right way to fix a problem in Fletch's specific environment.

"There's a lot of institutional knowledge you have to convey to someone just trying to do a fix. When a junior asks why you do it this way, it's a problem where you have to bring up months of context and pain and issues. They end up having to go back on their own time to see why we do it this way, which doesn't always happen."
—Darien Kindlund, VP of Technology at Fletch

Without enough time in the ---[day to understand the "why" behind remediation guidance, developers continued to make similar errors that left their code vulnerable. Many tools on the market that claimed to remediate simply offered an auto pull request, "but these tools don't take into account the context behind actual additional factors you have to take into account in your environment."

Fletch hoped to find a solution that not only automated remediation, but did so contextually and iteratively, in a way that could improve developers' secure coding practices.

The Solution

Fletch chose Amplify Security due to its context-aware, smart solution. Integrating directly into Fletch's existing workflow, Amplify offers remediation suggestions directly within its existing CI/CD pipeline. Amplify's intelligent remediation guidance, which rapidly learns an environment and its context, ensures that proposed fixes are both clear and tailored to the specific needs of the team.

"Amplify looks at any commit that is about to be merged into the master branch and analyzes it using a number of source code vulnerability scanning tools—they look at what was changed in the code, with a focus on any new vulnerabilities being introduced,"

"The internal tool highlights a specific line number and why it ended up being a problem—then Amplify uses that context to explain the issue and the fix. Then it offers guidance and further context if they want to learn more about the category of issues. It's all in the merge request, so our devs can keep using their tools."

zero
NEW VULNS IN THE FIRST 30 DAYS

85%
REDUCTION IN TIME TO RESOLUTION

BOOSTED SOC2 AND HIPAA COMPLIANCE

Amplify X Fletch: Cutting Security Remediation Time by 85%

Results

Fletch has seen an 85% reduction in resolution time for security issues overall.

85% REDUCTION IN RESOLUTION TIME FOR SECURITY ISSUES

"That's even greater in many cases. What once took a full week to resolve now only takes 24 hours, and that's good because our engineers wear a lot of hats."

Kindlund said that automated remediation often saved multiple developers time on the same commit:

"Teams no longer have to tie three people up dealing with a single security issue. The original dev can solve it on their own with Amplify, to the satisfaction of the rest of the team, which is a huge savings for the entire team."

zero NEW VULNS IN THE FIRST 30 DAYS

In addition to accelerating remediation at Fletch, Amplify rapidly reduced security technical debt and improved secure coding practices with its contextual guidance.

Amplify's business value became even clearer when Fletch sought compliance certifications, including SOC2 and HIPAA.

BOOSTED SOC2 AND HIPAA COMPLIANCE PROCESSES

"You need to be able to provide the auditor with evidence of how you're achieving best practices, and part of that evidence is showing the interactions around the code commit. We were able to achieve compliance certifications much faster with the evidence Amplify provides us."

Why Amplify?

Kindlund says Amplify stands out from the pack because of its capabilities for learning and iterative guidance.

"Other security tools can be tone-deaf—they identify a problem in a clinical sense, but they don't take into account the context, it's all boilerplate."

Amplify is different:

"What's helpful is that Amplify acts as a companion to the developers that doesn't get annoyed or overwhelmed by all these contextual issues, which is great because it is a tool that actively learns and helps devs get up to speed with not just how to fix, but how to fix it in a way that works in our environment, based on knowledge of past fixes. They can work independently on issues and discover the historical reasons a fix happened, without adding drag to senior devs."

Kindlund also praises Amplify for its level of adaptability to developers' workflows and knowledge base:

"There are very few security products on the market that have a level of interactivity that meets both security teams and development teams where they're at in terms of skill level. Amplify is designed to mold to the needs of our devs, rather than forcing devs to constantly look up and research additional context to solve the problem effectively."

Book a Demo