SYNOPSYS®

Eliminating Vulnerabilities Early in the SDLC for Société Française du Radiotelephone

Company Overview

Altice Europe is a leading player in the convergence between telecom and media in France, serving 23 million customers through its SFR division—Société française du radiotelephone—providing voice, video, data, internet telecommunications and professional services to consumers and businesses.

The challenge: Putting code security at the center of development

With more than 23 million customers, the business-to-consumer (B2C) IT division of SFR deploys dozens of major projects each year, including web, front-end, and office applications. The B2C IT Division wanted to increase its cyber security strategy and to complete its tools with a dynamic scanner capable of dealing with security in a dynamic mode, meaning within the framework of code execution and dialogue between several applications or between a front- or back-end, in order to ensure code security at the early stage of development.

Specifically, SFR wanted a solution that would:

- Enable developers to get involved and updated on cyber security issues.
- Reduce the volume of vulnerabilities during the production stage of projects.
- Reduce potential impacts on customers as well as risks of financial penalties from legal authorities.
- Enable developers/testers to fix bugs early in the SDLC.
- Enable automated security testing and instant vulnerability detection as part of the CI/CD workflow.
- Get contextual information to easily reproduce and fix vulnerabilities in real time.
- Obtain instant results for quick remediation.
- Improve accuracy of findings compared to SAST scanners.
- Improve cross-functional collaboration.

"SFR chose Seeker to help prevent code vulnerabilities of web applications and obtain real-time results for quick remediation."

Robert Cohen,
Validation & Security Director at SFR

The solution: Enterprise-scale IAST to identify vulnerabilities early in the SDLC

Synopsys' Seeker IAST solution is designed to help find high-risk security weaknesses while fostering collaboration between development and security teams. Seeker detects web application vulnerabilities and ties them directly to business impact, providing a clear explanation of risks. Seeker's seamless integration into CI/CD workflows enables automated application security testing without slowing down the release cycle.

Seeker saves valuable time, resources, and costs by enabling developers to fix critical security flaws early in the SDLC. Seeker reduces risk by securing apps before they go to production.

By automatically verifying findings in real time, Seeker helps reduce false positives that are common in other application security testing tools, making it easy to triage and prioritize on critical vulnerabilities that matter most.

Seeker also provides developers with the exact location of vulnerabilities in the code, remediation suggestions, and code execution flow to help them quickly remediate vulnerabilities.

The results: Putting developers at the heart of security testing

SFR is at the implementation stage with Seeker, but eventually the IAST solution will be used daily for every code review. The B2C IT Division is currently testing approximately a dozen of on-premises applications daily, and eventually will increase that number to several dozen applications. Less false-positive results and a substantial increase in productivity is expected when the solution is fully deployed.

Even at this early stage, SFR has already seen benefits from Seeker, including:

- Improvement of detection compared to other software like classic SAST.
- The ability to put back developers at the heart of security challenges and empower them on security norms conformity while they work on deliverables.

Seeker's ability to identify vulnerabilities during code execution; its informative reports; its ability to identify code lines to ease the correction process for the development teams; and its remedial suggestions are cited by Zine-Eddine Yahoui, Senior Manager of Cyber Security for the business-to-consumer (B2C) IT division of SFR, as three of the solution's features they like the most.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com