Checkmarx Software Composition Analysis (CxSCA) Helps DAZN Secure their Open Source Libraries

Why Securing Open Source is Essential

DAZN is a ground-breaking, live and on-demand sports streaming service soon to be available in over 200 countries. With millions of sports fans to cater to, DAZN has secure applications high on its agenda. Security comes from the top (their c-suite) and rolls down to their software developers who understand the value of a secure application. Application Security Testing (AST) solutions are imperative to DAZN, so they deliver highly secure applications to their expansive customer base.

One of the influencing forces behind DAZN's development organization is that they give developers professional freedom and flexibility in their software development practices. For example, DAZN's developers often use open source libraries within their proprietary code so that they don't need to "re-invent the wheel" with each software iteration. This makes Software Composition Analysis (SCA) an essential part of the software development lifecycle (SDLC) per DAZN:

> The business case for SCA is proven: If you are going to use open source libraries, then you have to use an SCA solution to be able to give a competent estimation of the risks associated with your project. You need the data.
>
> **Dr. George Perkins,** Application Security Specialist at DAZN Group.

Key Benefits of Checkmarx SCA

DAZN developers and security teams have already been using and benefiting from Checkmarx SAST and Codebashing solutions for some time to secure their proprietary code. Therefore, Checkmarx SCA (CxSCA) was the logical next step to ensure their open source usage was just as secure.

CxSCA's top 3 features and functionalities according to DAZN:

- The ability to audit the parts of the library that are actually being used: If you use a library that has some known vulnerabilities, but you don't use those particular parts of it in your code base, you can warn the developers as to the sensitive parts to avoid.
- Managing risk across all of the source code: With CxSAST and CxSCA combined, you can look "up" to management and the business side of things: "They talk risk, so we have to talk risk to them as well, and CxSCA is a vital source of data for us to get a feeling and to compute the risk for our source code. SCA gives you the data to back up your case." (Dr. Perkins).
- Leveraging CxSAST technology with CxSCA's "Exploitable Path" approach: Indicating whether an open source library's vulnerability is exploitable in the software: "You can actually show the path that was used. This demonstrates if the library is vulnerable. Once you show practical information, the developers tend to appreciate that. It makes the abstract, concrete." (Dr. Perkins).

CxSCA and DevSecOps

DAZN is a leader when it comes to implementing and practicing advanced software development: They use microservices architectures, have fast release cycles, and automate where applicable. This meant CxSCA had to fit right into their work models without delaying delivery:

Scan During Peer Review: When you talk about DevOps, you talk about delivery pipelines, and a minute or two is the norm. I can't add many minutes' worth of scanning to a 2-minute process. So, we looked at where the best time was in the actual process and the time was during peer review.

Save time with automation: As long as you don't impede developers' work, they are happy to embrace security tools. In GitHub, a pull request automatically triggers a CxSAST and CxSCA scan when using CxFlow as an orchestration engine. This saves valuable time and overhead for the developers.

Leverage your security champions: We have one security champion per team, which gives us the focus on the different DevSecOps tools we put in the SDLC. The champion pitches security to the team. They are essential since we (security teams) can't be everywhere at once.

Dr. George Perkins, Application Security Specialist at DAZN Group.

Secure SDLC, End to End

By using a combination of CxSAST and CxSCA, DAZN developers and security teams are able to prioritize which open source vulnerabilities matter most, save time, and improve their overall application security testing approach. Checkmarx's end-to-end integration for DevSecOps allows automating the process of application security testing by integrating with source repositories, CI and build servers, and bug tracking solutions.

CxSCA builds on Checkmarx's years of AST experience, empowering its customers to enjoy the benefits of a single vendor and one unified management layer for full DevOps security coverage.

Software = Security

About Checkmarx

Checkmarx is the global leader in software security solutions for modern enterprise software development. Checkmarx delivers the industry's most comprehensive Software Security Platform that unifies with DevOps and provides static and interactive application security testing, software composition analysis, and developer AppSec awareness and training programs to reduce and remediate risk from software vulnerabilities. Checkmarx is trusted by more than 40 of the Fortune 100 companies and half of the Fortune 50, including leading organizations such as SAP, Samsung, and Salesforce.com. Learn more at Checkmarx.com.