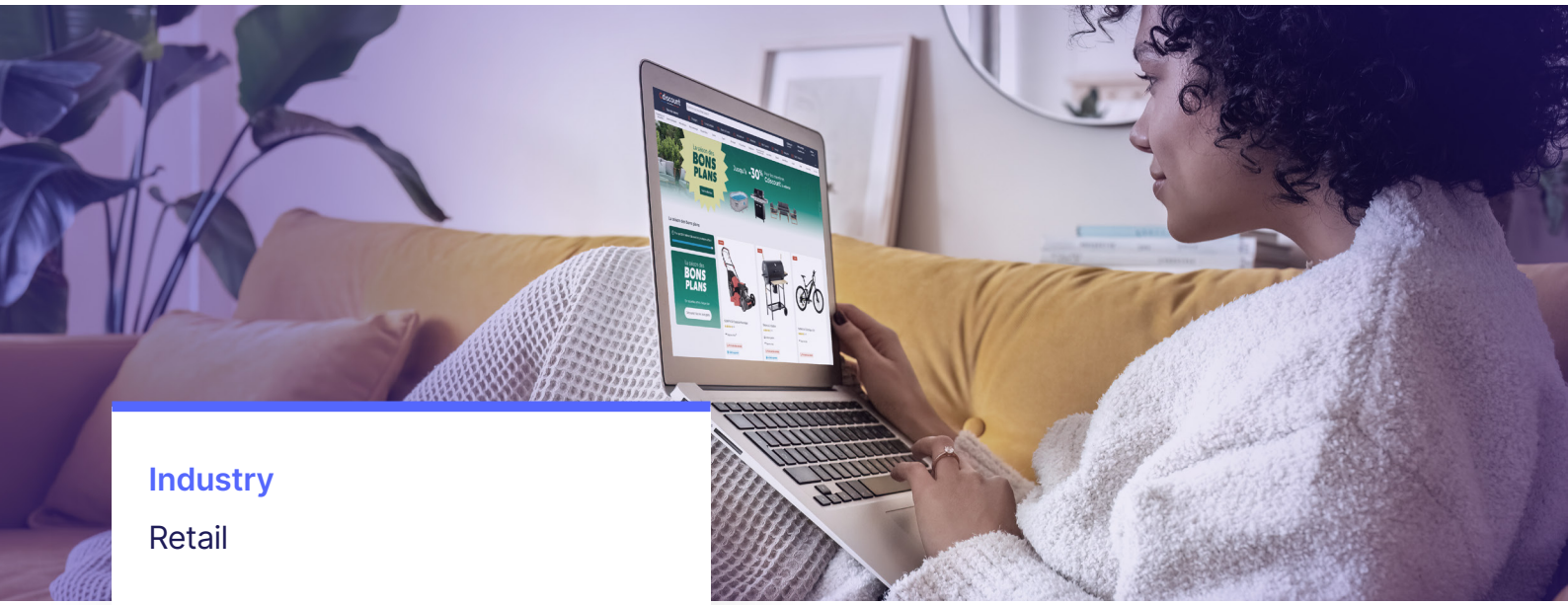
Checkmarx MAKE SHIFT HAPPEN Cdiscount

Case Study

Cdiscount Matures AppSec Program With Actionable Guidance From Checkmarx APMA



Industry

Retail

Location

Bordeaux, France

Checkmarx Solutions

- Static Application Security Testing
- Software Composition Analysis

Checkmarx Services

APMA

Key Takeaways

- Received a blueprint for AppSec maturity
- Maximized ROI
- Improved confidence in AppSec program

The Need

Turn AppSec scans into actionable intel

Founded in 1998 on the banks of the Garonne River in France, Cdiscount is one of the country's leading e-commerce companies selling everything from electronics to household goods and food. Over the past two decades, Cdiscount has expanded its customer base to more than 10 million and it's employing nearly 2,000 people.

Given its rapid growth, Cdiscount quickly realized that to remain competitive, it would need to continue innovating and creating new applications and processes. But more applications and modern development practices mean increased security risk.

To stay ahead of risk, Cdiscount needed an efficient application security (AppSec) program that enabled its software development team to quickly deliver applications that complied with the company's security requirements. That meant finding AppSec solutions that could be easily integrated and automated into its developer's existing tools and processes. It also meant finding solutions with the ability to set policy requirements around must-fix flaws.

After careful consideration and proof of concepts, Cdiscount initially chose two core Checkmarx products: Static Application Security Testing (SAST) for source code analysis and Software Composition Analysis (SCA) to track, assess, and remediate open source vulnerabilities. Both products uncovered numerous vulnerabilities, but the challenge then became how to prioritize vulnerabilities and how to remediate them without slowing time to market and impacting the customer experience.

> **The APMA methodology elevated the discussion to the overall spectrum of an AppSec program and zoomed out from the day-to-day discussion that usually is driven by a tactical or operational issue to fix.**
>
> **Christophe Piquet**
> AppSec Manager at Cdiscount

The Solution

APMA assessment to inform best practices and next steps

To find ways to mature its AppSec program, Cdiscount elected to participate in the Checkmarx AppSec Program Methodology & Assessment (APMA) framework. Checkmarx APMA is designed to assess the current state of an enterprise AppSec program and provide specific, actionable steps needed to advance the program. The assessment begins with a one-hour interview that covers five key dimensions:

- **Strategy & governance**
  Focuses on high-level goals and objectives, policies and KPIs
- **Security testing — tactical**
  Focuses on the processes of an AppSec program
- **Security testing — operational**
  Focuses on technology, such as the AppSec tools and how to use them, including procedures and guidelines
- **Security testing — architecture & scale**
  Focuses on the infrastructure required to perform security testing
- **Planning**
  Focuses on breaking down the work into work packages, creating a timeline, and how to provision or train resources

After Christophe Piquet, AppSec Manager at Cdiscount, participated in the interview, Checkmarx produced an in-depth APMA report for Cdiscount detailing the AppSec program's existing state of maturity and the desired state. That led to a gap analysis and outlined best-practices designed to help Cdiscount attain the desired state specified.

To help Cdiscount reach its AppSec goals without overwhelming its developers, Checkmarx recommended an agile sprint approach focused on implementing two to three recommendations at a time. This allowed Cdiscount to break the project into smaller tasks, observe progress, and constantly adjust priorities after each sprint.

The Results

+ Received a blueprint for AppSec maturity

Cdiscount immediately benefited from the APMA interview itself, which required Piquet to look inward at the AppSec tools and processes in place and the efficiency of the development and AppSec teams. "It was very constructive to understand the magnitude of our current AppSec program and the role that everyone plays in its execution," Piquet said. Reviewing the maturity level of the different components of the APMA methodology helped them draft the blueprint of what a good AppSec program at Cdiscount would look like. "The APMA methodology elevated the discussion to the overall spectrum of an AppSec program and zoomed out from the day-to-day discussion that usually is driven by a tactical or operational issue to fix," Piquet said. "Having a well-thought-out interview process really helped focus our efforts."

+ Maximized ROI and increased confidence in AppSec

The gap analysis, which identified the steps needed to move from the current state to the desired state of maturity, allowed Cdiscount to understand how to optimize the implementation of the recommendations advised by the APMA team. This led to two main benefits. First, it helped Cdiscount improve its AppSec program by optimizing its ***SAST*** and ***SCA*** security testing tools to speed scan and fix times, further prioritize the most critical vulnerabilities, and — ultimately — maximize its return on investment. Second, by achieving its desired state of AppSec maturity, Cdiscount gained added confidence that it's providing the safest and highest quality services to its customers.

Checkmarx

Checkmarx is the leading application security provider, offering the industry's most comprehensive cloud-native platform, Checkmarx One™. Our products and services enable enterprises to shift everywhere in order to secure every phase of development for every application while simultaneously balancing the dynamic needs of CISOs, security teams, and development teams. We are honored to serve more than 1,800 customers, including 60 percent of Fortune 100 organizations, and are committed to moving forward with an unwavering dedication to the safety and security of our customers and the applications that power our day-to-day lives.

MAKE SHIFT HAPPEN