Proactive Security for a Leading Retailer: Bright Security's DAST Solution in Action

INTRODUCTION

In today's increasingly digital world, retail businesses must prioritize the security of their applications and APIs to protect sensitive customer data and maintain a competitive edge. This case study examines how a prominent California-based retail company utilized Bright Security's Dynamic Application Security Testing (DAST) solution to identify and remediate vulnerabilities before they reach production, ultimately securing their applications and APIs without compromising the speed and efficiency of their DevOps processes.

BACKGROUND

The retail company, a major player in the major global player, operates a large online presence and relies heavily on applications and APIs to power its e-commerce platform. Recognizing the potential risks associated with vulnerabilities in their software, the company sought a security solution that would enable them to detect and address issues early in the development process, without hindering the agility of their DevOps team.
SOLUTION

To achieve this goal, the retailer implemented Bright Security's DAST solution, a state-of-the-art security testing tool designed to identify both technical and business logic vulnerabilities in applications and APIs. By integrating the DAST solution into their DevOps pipeline, the company was able to proactively address security concerns without slowing down development or treating security as an afterthought. Bright Security's DAST solution is known for its ability to deliver highly accurate results with minimal false positives. This feature ensures that developers can focus on addressing genuine security issues without wasting time and resources on false alarms.

IMPLEMENTATION

The seamless integration of Bright Security's DAST solution into the retailer's existing DevOps processes allowed developers to test and remediate vulnerabilities as they arose, effectively shifting application security (AppSec) testing left. This approach reduced the likelihood of security issues making it to production and ensured that security concerns were addressed in tandem with ongoing development efforts.

RESULTS

Since implementing the DAST solution, the retail company has been able to detect and remediate significantly more vulnerabilities early in the SDLC resulting in a significantly marked improvement in the security of its applications and APIs. By enabling developers to identify and address vulnerabilities early in the development process, the company has significantly reduced the risk of security breaches and protected its valuable customer data. Furthermore, the adoption of Bright Security's DAST solution has allowed the company to maintain the agility and efficiency of its DevOps processes, demonstrating that security need not be a bottleneck or an afterthought in software development.

Integrating Bright Security's DAST solution into our DevOps pipeline has been a game-changer for our organization. By shifting AppSec testing left and empowering our developers to address vulnerabilities early in the development process, we've been able to maintain the speed and efficiency of our operations without sacrificing security. As a result, we can confidently provide our customers with a secure and reliable e-commerce platform, while ensuring that we remain agile and competitive in the rapidly-evolving retail landscape.

VP of Cybersecurity

CONCLUSION

This case study demonstrates the value of Bright Security's DAST solution for a leading global retail company. By embracing a proactive approach to security testing, the retailer has not only improved the security of its applications and APIs but has also maintained the agility and efficiency of its DevOps processes. With the support of Bright Security's DAST solution, the company can continue to innovate and succeed in the competitive retail market, while keeping customer data secure and maintaining customer trust.