The Power of Shift Left: How a Major Software Company Empowered Developers To detect and remediate vulnerabilities Early in the SDLC

INTRODUCTION

In the rapidly-evolving world of software development, ensuring a high level of security is a critical priority for businesses. As hackers and cyber criminals continue to develop more sophisticated methods of attack, companies must be proactive in their efforts to identify and address vulnerabilities in their software. This case study explores how a leading US-based software company successfully implemented Bright Security’s Dynamic Application Security Testing (DAST) solution to detect and address vulnerabilities early in the development process, saving time and money while improving overall security.

BACKGROUND

The company in question, a major player in the US software industry, provides various software solutions Across the Cybersecurity sector. With a strong commitment to security, the company recognized the need for a more efficient and effective way to identify vulnerabilities in their software before it reached production. By implementing a security solution that could detect and enables to remediate vulnerabilities early in the development process, the company aimed to reduce the potential for costly security breaches and improve the overall quality of their software, while aligning their development and Appsec teams.
SOLUTION

To achieve these goals, the company chose to deploy Bright Security's DAST solution, a cutting-edge tool designed to identify and address potential security vulnerabilities in real-time. Bright Security’s DAST solution utilizes purpose built scanning technology to detect vulnerabilities as early as the unit testing phase, enabling developers to address issues before they reach production. This proactive approach to security testing has been proven to save both time and money, while as significantly reducing the risk of security breaches.

IMPLEMENTATION

The implementation of Bright Security's DAST solution involved a seamless integration with the company's existing software development processes. By incorporating the DAST solution into their development workflow, the company empowered their developers to identify and remediate vulnerabilities as they arose, minimizing the risk of introducing insecure code into the production environment.

One of the key features of Bright Security's DAST solution is its ability to produce highly accurate results with minimal false positives. This enables developers to focus their efforts on addressing genuine security vulnerabilities, without the need to waste valuable time and resources on investigating false alarms.

RESULTS

Since implementing Bright Security’s DAST solution, the software company has been able to detect and remediate a much higher number of risks early in the SDLC resulting in a significant reduction in the security vulnerabilities that make it to the production environment. This has not only resulted in a more secure software offering for their customers but has also led to substantial cost savings and increased efficiency in the development process.

By enabling developers to identify and remediate vulnerabilities during the unit testing phase, the company has reduced the time spent on addressing security issues later in the development cycle. This has led to a more streamlined development process, with developers able to focus on delivering high-quality, secure software solutions for their clients.

“Thanks to Bright Security's DAST solution, our team can now scan for vulnerabilities much earlier in the development process. This has allowed us to remediate issues more efficiently, based on the comprehensive guidelines provided by the tool. By empowering our developers to address security concerns at the unit testing phase, we've significantly reduced the number of vulnerabilities that reach production, saving both time and money.”

Head of security engineering

CONCLUSION

This case study demonstrates the value of Bright Security's DAST solution for a leading US-based software company. By adopting this advanced security testing tool, the company has been able to significantly improve its overall security posture, save time and money, and deliver a higher-quality, more secure product to its customers.