Enhancing Security and Building Customer Confidence:

Deployment of Bright's DAST Solution in a Prominent U.S. Healthcare Organization

INTRODUCTION

The healthcare sector is a treasure trove of confidential client data, including medical records and insurance specifics. Given the rising incidence of cyber threats and the potential fallout of data breaches, it’s essential to secure and maintain the privacy of this sensitive data. This case study examines the adoption of Bright's Dynamic Application Security Testing (DAST) solution by a premier U.S. healthcare organization committed to providing exceptional services while safeguarding its clients' data.

BACKGROUND

The challenge of protecting sensitive client data is a constant stressor in the healthcare industry, which has unfortunately become a prime target for cybercriminals seeking to exploit valuable data. To counter these threats, the healthcare organization made significant investments in enhancing its application security. Recognizing the inadequacies of traditional DAST solutions in fulfilling the increasing security demands, the organization sought a more robust solution. The goal was to find a system capable of maintaining a competitive edge in the security landscape while ensuring robust protection against evolving cyber threats.
**SOLUTION**

To fulfill its security objectives, the organization chose to deploy Bright's DAST solution to scan web applications as well as APIs early in the development process. The capabilities of the solution for scalability and customization has been particularly of importance for this large healthcare organization with a diverse range of applications and security needs. The solution can be tailored to align with the organization's specific application landscape and integrated seamlessly with its existing security frameworks. This means the organization can maintain a consistent and holistic security approach across its entire infrastructure.

**IMPLEMENTATION**

The deployment of Bright's solution started in August 2022, beginning with a detailed evaluation of the organization's existing security infrastructure, vulnerabilities, and regulatory compliance needs. With the help of dedicated Bright representatives, the healthcare organization tailored the DAST solution to their specific requirements. This included configuring the solution to suit their application environment, integrating it smoothly with existing security frameworks, and ensuring compatibility with their development and testing procedures.

**RESULTS**

Post-deployment of Bright's DAST solution, the organization has experienced the remarkable benefit of early vulnerability detection throughout the software development lifecycle. This proactive strategy allows them to identify and address vulnerabilities before they can be exploited, safeguarding client data. By staying one step ahead of potential threats, the organization can retain their clients' trust and uphold the highest data protection standards.

"The deployment of Bright's DAST solution has been an enormous success. The tool has significantly improved our vulnerability detection process, enabling early identification and mitigation of potential security risks. The continuous support from the Bright team has been invaluable, facilitating a smooth deployment process and providing assistance whenever required. We are pleased with the results and reassured about the heightened security and protection of our applications."

**Director of Application Security**

**CONCLUSION**

The integration of Bright's DAST solution has been a game-changer for the healthcare organization, enhancing their security framework. The process facilitated seamless integration of the solution with their existing system, tailoring it to their unique needs. This proactive measure has strengthened their ability to shield client data from potential threats and maintain customer confidence. By prioritizing security and adopting Bright's DAST solution, the healthcare organization has underscored their commitment to maintaining top-tier data protection standards in an increasingly challenging digital environment.