WhiteHat SECURITY

Customer Case Study

IT Recruiting Company Needs Complete AppSec Solution

Project Background

Driven by a passion to help companies win the war for talent, our customer offers best-to-market software solutions and tools to unify all aspects of talent acquisition. Their customers are companies who need to manage their entire talent acquisition lifecycle within a single SaaS application. Our customer focuses on user-friendly technology and a customer experience second-to-none making them one of the largest and fastest-growing providers in the industry.

They came to WhiteHat with the following agenda:

- Make sure each application in their talent acquisition software is performing as per the documented benchmarks
- Make sure their product is stable without having any security vulnerabilities
- Develop standardized processes around vulnerability management

Our customer is relatively mature in their overall security posture. They are an ISO 27001-certified company that deals with the confidential and personal information of their customers on a daily basis, following risk-based security management processes. Their goal is to continuously improve security maturity in order to meet or beat the security posture of our most conscientious customers.

The Use Case

Our customer had time to look around at the options. They examined Rapid7, Qualys, and Veracode before picking WhiteHat Security as their preferred application security vendor. Their information security manager says, "We needed to implement a standard vulnerability assessment process across our entire environment in order to reduce risk and provide a standard overview of our security posture. In addition, we wanted to provide best-of-breed vulnerability and penetration testing to address our customers' needs."

In the end, they purchased the full suite of Sentinel offerings: DAST, SAST, Mobile, and Computer-Based Training. All of the scanning results are available via Sentinel, providing a single-pane view of the application security posture. "Dashboards are used interdepartmentally to communicate our security posture and to ensure that appropriate actions are taken to address vulnerabilities," says the QA manager for their test labs.

WHITEHAT SAST KEY BENEFITS

- Assess code at any point in the development cycle – even partial code
- Scan source code from any repository on premises
- Time-saving by finding vulnerabilities in UAT instead of jusT production for high-risk applications
- Rule Packs identify and verify vulnerability defects
- Backed by Threat Research Center consultation and best-practice remediation

WHITEHAT DAST KEY BENEFITS

- Fully-managed platform, with near zero false positives
- Run scheduled assessments daily or on demand
- Advanced analytic capabilities to monitor trends and key statistics like remediation rate, time to fix vulnerabilities, and age of vulnerabilities
- Open XML API integration with bug tracking systems, SIEMs, GRC, and WAF products

For our customer, application security scanning is primarily used in the UAT phase, and then again in production. This allows them to reduce the time to fix – finding vulnerabilities in test with low false positives is cheaper than finding them in production. They find the detailed descriptions of the vulnerabilities, continuous scanning, and advice from the Threat Research Center to be the most valuable aspects of their program. WhiteHat's leading-edge SAST service scans the source code, identifies vulnerabilities, and then provides detailed descriptions of those vulnerabilities and their remediation advice as well as ready-to-implement solutions for each exposure. When combined with constant dynamic scanning on production web applications and mobile code reviews, the end-to-end application solution is complete.

The Result

The Information Security Manager says, "WhiteHat is an important layer in our vulnerability management process and has helped us by contributing strongly to improved security."

Continuous education of both management and development via the computer-based training is another aspect of this forward-thinking organization. Over time, improved knowledge and understanding of the OWASP Top-10 vulnerabilities and how to avoid them means that developers code in a secure way the first time, building security into the requirements and design phases of new applications.

For this customer, it's all about the multi-level approach: "WhiteHat scans our source code continuously and provides actionable information about source code vulnerabilities, which helps us improve the inherent security of our code. WhiteHat also scans our pre-production environment and is integrated within our quality assurance processes, which helps us remediate security threats prior to pushing our code to production. Finally, WhiteHat continuously monitors our production environments to ensure no new vulnerabilities are inadvertently introduced. This three-pronged attack against vulnerabilities has made development and deployment processes more efficient and actionable."

> **"WhiteHat is an important layer in our vulnerability management process and has helped us by contributing strongly to improved security."**

WHITEHAT MOBILE KEY BENEFITS

- Supports iOS and Android
- Options for developer-signed binaries, source code review, and manual assessments
- Analysis available for client-side applications, server-side, and API checks
- Identifies third-party libraries in code, as well as native library hooks
- Business Logic Assessments and use case analysis

WHITEHAT COMPUTER BASED TRAINING BENEFITS

- Developer education
- Learn at your own pace
- OWASP Top-10 vulnerabilities explained, and broken down with best practice advice
- Management-level training on concepts and prioritization

About WhiteHat Security

WhiteHat Security has been in the business of securing web applications for 15 years. Combining advanced technology with the expertise of its global Threat Research Center (TRC) team, WhiteHat delivers application security solutions that reduce risk, reduce cost and accelerate the deployment of secure applications and web sites. The company's flagship product, WhiteHat Sentinel, is a software-as-a-service platform providing dynamic application security testing (DAST), static application security testing (SAST), and mobile application security assessments. The company is headquartered in Santa Clara, Calif., with regional offices across the U.S. and Europe. For more information on WhiteHat Security, please visit www.whitehatsec.com, and follow us on Twitter, LinkedIn and Facebook.

WHITEHAT SECURITY, INC. 3970 Freedom Circle Santa Clara, CA 95054 • 1.408.343.8300 • www.whitehatsec.com