WhiteHat Remediation Services

Effectively Remediate Vulnerabilities

A comprehensive web application security program not only involves accurate vulnerability findings, but also efficient and timely remediation for identified vulnerabilities. With this information in hand, security and development teams can more accurately demonstrate risk reduction to all stakeholders.

WhiteHat Security has partnered with AsTech Consulting to create WhiteHat Remediation Services. This service provides a way to rapidly improve remediation and demonstrate the results through custom WhiteHat Sentinel remediation performance reporting.

The service starts with an initial review of vulnerabilities and trend information provided through reports available in WhiteHat Sentinel. AsTech remediation experts then leverage this information and conduct an initial scoping call to define a two-week engagement that delivers remediation results and maps out an improvement plan to increase remediation efficiency. Each engagement involves up to four distinct work streams depending on the situation:

Services Overview

Remediation Outsourcing
Clients with short-term needs, typically on legacy applications, can engage AsTech remediation resources to simply reduce the number of security vulnerabilities. These resources can be integrated into existing software processes to reduce risk without impacting existing project delivery schedules.

In some cases, allocation and use of existing resources (both people and technology) is not optimized for efficient remediation. AsTech remediation experts will conduct a thorough review of resources and technology integration and provide recommendations for improvement.

Directed Redevelopment
Directed redevelopment delivers remediation of specific vulnerabilities and trains developers on the proper methods to efficiently remediate vulnerabilities and how to avoid them by working “shoulder-to-shoulder” with AsTech remediation experts.

Effectively incorporating WhiteHat Sentinel results into existing development, build and QA processes are critical to improving code security. AsTech remediation experts will evaluate and re-engineer existing processes in the Scan/Triage/Mitigation/Reporting cycle and recommend improvements to areas where the process tends to breakdown.

Engagement process

Pre-engagement

- Define which development organization/application is going to be the focus of the program
- Discussion and analysis on current remediation program challenges and structure
- Run initial remediation scorecard
- Define engagement - which workflows are most likely to achieve the greatest improvement in remediation performance

Engagement Week 1

In the first week (on-site) the AsTech team will accomplish the following:

- "On the ground" situational analysis of the current status of remediation program
- Refinement of engagement model – determine which of the workflows are going to be the focus of the engagement
- Workflow engagement – including remediation of vulnerabilities, assess current process

Engagement Week 2

Second week may be a combination of on/off-site work depending on the identified requirements. Deliverables may include:

- List, description, and findings regarding specific remediated vulnerabilities
- Summary engagement document that identifies areas of improvement and recommendations for remediation program
- Conference call to review findings

Post-Engagement

Three months after initial engagement, the team will re-engage to determine performance of revised remediation program and processes. Actions during post-engagement may include:

- Re-run of remediation score card report
- Conference call and final remediation score card review
- Other recommended actions to improve remediation performance

About WhiteHat Security

Founded in 2001 and headquartered in Santa Clara, California, WhiteHat Security provides end-to-end solutions for application security. The company's cloud website vulnerability management platform and leading security engineers turn verified security intelligence into actionable insights for customers. Through a combination of core products and strategic partnerships, WhiteHat security provides complete application security at a scale and accuracy unmatched in the industry. WhiteHat Sentinel, the company's flagship product line, currently manages thousands of websites - including sites in highly regulated industries such as e-commerce, financial services and healthcare companies. For more information, visit www.whitehatsec.com.

About AsTech

AsTech software security engineers have an average of more than 15 years of enterprise application development experience coupled with extensive security expertise. We draw from this wealth of experience to offer strategic, agile, and robust solutions to develop secure applications and to address the vulnerabilities already found in existing applications. We work closely with software development teams to help them succeed in continuously improving the security of critical Internet applications.

WhiteHat SECURITY

WhiteHat Security, Inc. | 3970 Freedom Circle | Santa Clara, CA 95054 | 1.408.343.8300 | www.whitehatsec.com