WhiteHat SECURITY

Integrating Security Across the Software Development Lifecycle (SDLC)

ReachLocal®

Security is a top priority

Businesses like ReachLocal recognize that security is an important part of a web application SDLC

This case study is about ReachLocal, a company that is a leader in powering local online marketing. Its mission is to help businesses all over the world reach more local customers online. Headquartered in Woodland Hills, Calif., ReachLocal has over 68 locations throughout the United States, Canada, Australia, the United Kingdom, Germany, the Netherlands, Japan, and Brazil.

When ReachLocal began, the Internet was already integral to our everyday lives. You could go online to do anything you needed – read the news on websites like CNN.com, research businesses on directories like Citysearch, and of course, use search engines like Google to look for local products and services. In fact, consumers already had thousands of choices to find information about businesses in their area. But if you were a local business owner, it became much more difficult to reach these digital consumers, which meant getting fewer customers. As a result, ReachLocal was the first company dedicated to helping local businesses get customers online.

Security is a top priority for ReachLocal customers who may be new to the digital space or unaccustomed to the growing presence of the online commercial space. To ensure that their security needs are met, ReachLocal has partnered with WhiteHat Security, a leader in application security testing. WhiteHat Security offers Sentinel Services, a SaaS Web application security offering, which allows ReachLocal to not only identify and remediate web application vulnerabilities but to make security an integral part of their software development lifecycle (SDLC).

Software development lifecycle and security

Web application security is a critical issue facing modern businesses today. As attacks increase and websites become more complex, it's not enough to find and identify vulnerabilities. Security needs to be a part of the development process. To understand how the integration works we must first understand the SDLC.

In its most basic definition, the SDLC comprise four parts of a web application: Requirements and Design, Development, Quality Assurance, and Production. Web application security needs to be a part of each stage of the SDLC.

- Requirements and Design – Training and education on security to build better applications with security in mind. Includes computer-based training (CBT) for secure coding.
- Development – Identifying vulnerabilities in the source code and having the ability to integrate security into the early development process. Includes computer-based training (CBT) for secure coding.
- Quality Assurance – Ensuring that security is a part of the QA process to have code ready to roll out into production.
- Production – Identifying any remaining vulnerabilities, including key business logic vulnerabilities, and accurately prioritizing them for remediation.

Businesses like ReachLocal recognize that security is an important part of a web application SDLC. This is why Mikhael Felker, director of regulatory and compliance at ReachLocal, chose WhiteHat Security to secure key web applications.

"We are dedicated to working with customers like ReachLocal," said John Haniotis, vice president of product management at WhiteHat Security. "Security is a critical part of the SDLC and security leaders like Mikhael understand its significance. That's why he has integrated Sentinel into his company's development process."

Sentinel factors into KPIs

Integrating security into each stage of the SDLC is important; however, developers, QA, and management must be aware of their organization's security needs as well as prioritize it. Businesses are accustomed to using Key Performance Indicators (KPIs) to measure and track results. KPIs are created to represent a desirable outcomes such as revenue growth, reliability, incidents closed within 24 hours, and more. Because there is so much focus on KPIs, executives, management, and employees all rally to "make the numbers." The goal of ReachLocal's information security and compliance team was to leverage KPIs with the goal of reducing web application security vulnerabilities and ultimately making more secure products.

ReachLocal created a security KPI, referenced as a security score. The KPI score incorporates three components:

- Existing vulnerabilities (backlog items) and prioritizing based on severity
- New vulnerabilities introduced within the past month
- Closed vulnerabilities in the past month

An urgent open vulnerability would decrease the KPI score more than a major one. The security score is primarily computed with WhiteHat Sentinel vulnerability data. The vulnerability data include severity and threat levels, across major web properties.

This process helps product development teams prioritize addressing different web application vulnerabilities.

"WhiteHat provides Proof-of-Concept code for vulnerabilities, so developers will trust vulnerability data and take action," said Curt Jeppson, senior security engineer for ReachLocal.

Tickets for those vulnerabilities are created within the web application's JIRA project using the JIRA plugin for Sentinel and are incorporated in the backlog using the same Agile SDLC as any product feature or bugfix.

In order to make the security score KPI more visible and impactful, it was incorporated into the overall software quality score as 20 percent of the quality measurement. The software quality score KPI is a very visible company metric, shown to all of the product and technology groups at ReachLocal on a monthly basis. Product managers heavily guard and work hard to push their software quality score, or "Q score" as close to maximum value as possible. Since security is now one-fifth of the overall score, product managers and their development teams are less likely to introduce vulnerabilities and more likely to correct any existing vulnerabilities in a consistent timeframe.

"We were able to develop a process that integrated WhiteHat Sentinel's scoring system and prioritized vulnerabilities into our own security KPI scores to inject security as a part of the SDLC," said Mikhael Felker, director of regulatory and compliance at ReachLocal.

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 ReachLocal

ReachLocal, Inc. (NASDAQ: RLOC) develops online marketing and transaction solutions that power local commerce for SMBs, from lead generation and lead conversion to booking and buying. Our global distribution network includes local Internet marketing consultants and service professionals, along with select third-party agencies and resellers throughout Australia, Austria, Belgium, Brazil, Canada, Czech Republic, Germany, Japan, the Netherlands, New Zealand, Poland, Russia, Singapore, Slovakia, the United Kingdom and the United States. ReachLocal is headquartered in Woodland Hills, Calif. For nearly a decade, ReachLocal has helped local businesses acquire customers online, delivering more than 110 million leads to customers in 16 countries. Currently, the company has over 24,600 customers across five core verticals: healthcare, automotive, home services, professional services and specialty services.

WhiteHat SECURITY

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

010314