



FOR IMMEDIATE RELEASE

Contact:

Dawn van Hoegaerden
WhiteHat Security
408-492-1817 ext.14
dawn@whitehatsec.com

Rachel Miller
SHIFT Communications
617-681-1256
rmiller@shiftcomm.com

WhiteHat Security Debuts Sentinel 3.0, the Next Evolution of the Industry's On-Demand Vulnerability Assessment for Web Applications

- WhiteHat Sentinel 3.0 Provides Comprehensive, On-Going and Easy-To-Manage Vulnerability Assessment of Web Applications -

SANTA CLARA, CA.—October 23, 2006—WhiteHat Security, Inc., a leading provider of Web application security services, today announced WhiteHat Sentinel 3.0, the industry's only continuous vulnerability assessment and management service for Web sites. Sentinel 3.0 reduces the burden of securing Web applications with an on-going service that provides up-to-date, and comprehensive identification of the vulnerabilities that are putting online customer and corporate data at risk. It is the only solution that can assess for all 24 classes of vulnerabilities identified by the Web Application Security Consortium's (WASC) threat classification.

Web application security is inherently complex because the vast majority of e-commerce and interactive sites are created with custom code. Often, these sites change on a weekly or even daily basis, unlike commercial software products. WhiteHat Sentinel 3.0 enables assessment each time a Web site is changed or updated, and ensures the identification of existing and new vulnerabilities. This is accomplished through a three-step process - scanning, verification and custom testing. As part of this process, WhiteHat integrates expert analysis with proprietary scanning technology which delivers more in-depth results than scanning alone, since many of the most dangerous vulnerabilities can only be detected by this combined process. WhiteHat security engineers review all scanner findings to ensure accuracy and eliminate false positives.

Some of the key elements of Sentinel 3.0 include:

- One-click vulnerability retesting, for fast and easy confirmation of vulnerability remediation;

- Customized threat levels which streamline the remediation process by allowing customers to prioritize vulnerability repair;
- "Inspector," (patent-pending) which enables WhiteHat to build a knowledgebase to look at defect patterns and immediately apply new discoveries on one site across the entire customer base;
- Web services API to directly integrate Sentinel vulnerability data with bug tracking systems or SIMs, and allow end-users to remain within their established framework system; and,
- Mapping to Payment Card Industry (PCI) vulnerability severity levels for simplified customer reporting.

WhiteHat Sentinel is a powerful platform based on a service-oriented architecture (SOA) that was built to assess hundreds, even thousands of the largest and most complex websites simultaneously. This scalability of both the methodology and the technology enable WhiteHat to streamline the process of Web application vulnerability assessment for customers. In addition, Sentinel 3.0's unique Web-based customer interface provides real-time reporting for current vulnerability status at any time.

"Companies need to comprehensively assess their websites every time they change, and Sentinel 3.0 is the only solution that provides this capability," said Stephanie Fohn, chief executive officer, WhiteHat Security. "In addition, Sentinel 3.0 makes the entire process of managing website security much easier for the customer, by providing all the information necessary to quickly and efficiently remediate vulnerabilities."

Industry Analysts Highlight Great Need to Mitigate Web Application Vulnerabilities.

"Given that applications, especially Web applications, are becoming a prime target of attackers, it is becoming imperative for enterprises to invest in vulnerability assessment solutions that identify and address the serious web application weaknesses. The critical Web application vulnerabilities need to be intelligently prioritized so they can be fixed," said Charles Kolodgy, research director for Security Products at IDC. "Large e-commerce, financial services and healthcare organizations, increasingly at risk to Web application attacks, should strongly consider evaluating security service offerings to address managing and mitigating Web application vulnerabilities."

With Sentinel 3.0, WhiteHat has enhanced its customer interface to provide users with easier access to information and greater control. To ensure customers are getting the most out of the service, WhiteHat has implemented an "Ask a Question" feature as part of the interface where users can submit questions regarding specific vulnerabilities. WhiteHat support can respond to and answer these customized questions, and also store them in a centralized repository for future access.

"Increasing amounts of data exposed via Web sites, combined with rapidly changing application code, necessitate continuous application assessment

services,” said Bill Pennington, vice president of services, WhiteHat. “In addition to all of the new features and functionality of Sentinel 3.0, WhiteHat’s scalable technology and process enable us to provide on-going service to customers, regardless of whether they have one site or thousands.”

WhiteHat Sentinel 3.0 is currently available for an annual subscription fee with tiered pricing based on the number of Web applications. Contact the WhiteHat sales office at (408) 492-1817 for more information.

About WhiteHat Security, Inc.

Headquartered in Santa Clara, California, WhiteHat Security is a leading provider of web application security services. WhiteHat delivers turnkey solutions that enable companies to secure valuable customer data, comply with industry standards and maintain brand integrity. WhiteHat Sentinel, the company’s flagship service, provides continuous vulnerability assessment and management for web applications. For more information about WhiteHat Security, please visit our website, www.whitehatsec.com.

###