



WhiteHat Sentinel Integration with Snort

WhiteHat & Snort Integration Delivers Increased Control Over Application Threats

benefits

Introducing the first-of-its-kind website security integration with Snort®, the leader in open source intrusion prevention systems (IPS). Now, WhiteHat Sentinel customers can use Sentinel vulnerability data to create ultra-targeted Snort rules, expanding the capability of an IPS to reliably detect application layer attacks. This new level of intelligence enables security professionals to increase their visibility into verified real-time threats. With Snort deployed at 80 percent of Fortune 100 companies and 42 percent of the Global 500, this advancement will have a significant impact on enterprise website security.

Laser-Focused Snort Rules: Cut Through the Noise

WhiteHat Sentinel is the first website vulnerability management solution to integrate verified website vulnerability data with Snort, thereby extending IPS from the network space to include websites, the foremost target for the enterprising hacker. The WhiteHat Snort Integration is easy to configure, allowing companies to quickly begin generating Snort rules for specific vulnerabilities.

WhiteHat Sentinel delivers the most complete and accurate vulnerability information available, which is the foundation of a comprehensive website risk management program. Snort integration enables security teams to monitor more effectively, fix problems, and precisely prioritize risk in their environment.

As a result, users can fine-tune Snort alerts and correlate findings to reduce noise and allow security teams to focus on real issues. Prior to the WhiteHat Sentinel / Snort integration, security professionals were forced to sift through reams of Web server logs to retrieve the same information now seamlessly generated and validated by WhiteHat. Now false positives are eliminated, so security teams can be confident that an alert signifies a real problem.

Extend Your Existing IPS Infrastructure

Security professionals can now leverage their deployed IPS infrastructure to be alerted to custom Web application attacks in real-time. This feature delivers the previously impossible ability to detect and block website attacks without having to deploy additional devices.

WhiteHat Sentinel integration with Snort also allows for the efficient prioritization of actual website vulnerabilities, based on what is being attacked and by whom. Using Sentinel's highly precise Snort rules offers the unique ability to deploy the IPS in block mode to prevent attacks.

- Increase visibility into real-time threats
- Fine-tune Snort alerts and correlate findings to reduce noise
- Increase control over application threats
- Leverage deployed IPS infrastructure to be alerted to custom Web application attacks in real-time
- Extends IPS from the network space to include Web applications
- Simple deployment via WhiteHat's open XML API

"We are excited by the enhancement of Snort rules with WhiteHat Sentinel's targeted website vulnerability data. Verified and accurate vulnerability information from the running Web application makes it easy to generate a list of Snort rules in IPS mode in order to stop attackers from taking advantage of these vulnerabilities, while simultaneously fixing the problems."

Marty Roesch
founder and chief technology officer
Sourcefire and creator of Snort

How it Works

The Sentinel / Snort integration is implemented as a script which when executed, will securely connect to the Sentinel open API to extract a website's vulnerability details. The script will then translate the downloaded vulnerability information into Snort alert rules. Users may then apply these rules to a Snort IPS to alert on or block attacks against vulnerable websites.

The script may be scheduled to regularly pull vulnerability information from Sentinel.

Simple Deployment

The WhiteHat Sentinel open XML API for Snort is available immediately, free of charge, to all Sentinel customers. To begin using this feature, login into the WhiteHat Customer Support portal and click on the FAQ section. Search for the article titled, "Where do I find more information on Snort integration? This contains a downloadable .zip file. Open the file, read the release notes and after a simple configuration of your IPS, you're ready to go.

In addition to Snort, the WhiteHat Sentinel open XML API enables data exchange with Web application firewalls (WAF), bug tracking systems and security information and event management systems (SIEM) to provide complete website risk management.

To Learn More

To learn more about WhiteHat Sentinel and the Snort integration, please visit www.whitehatsec.com, contact the WhiteHat sales office at (408) 343-8300, or email sales@whitehatsec.com.

About WhiteHat Security, Inc.

Headquartered in Santa Clara, California, WhiteHat Security is the leading provider of website risk management solutions that protect critical data, ensure compliance and narrow the window of risk. WhiteHat Sentinel, the company's flagship product family, is the most accurate, complete and cost-effective website vulnerability management solution available. It delivers the visibility, flexibility and manageability that organizations need to take control of website security and prevent Web attacks. Furthermore, WhiteHat Sentinel enables automated mitigation of website vulnerabilities via integration with Web application firewalls and IPS's. To learn more about WhiteHat Security, please visit our website at www.whitehatsec.com.



WhiteHat Security, Inc. | 3003 Bunker Hill Lane | Santa Clara, CA 95054
408.343.8300 | www.whitehatsec.com

Copyright © 2009 WhiteHat Security, Inc. | Product names or brands used in this publication are for identification purposes only and may be trademarks of their respective companies.

Snort is a registered trademark of Sourcefire, Inc.

100809