WhiteHat Sentinel Source

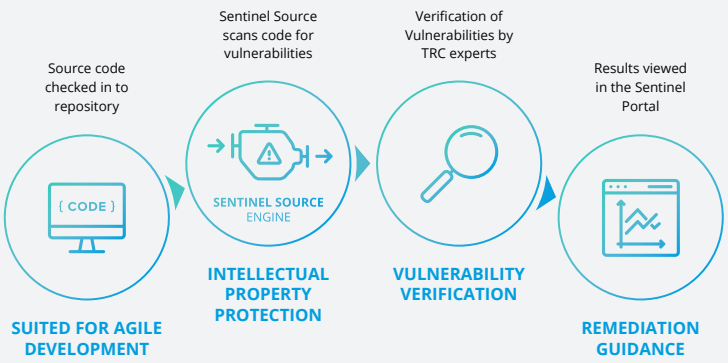
Build Security into the Software Development Life Cycle

Rapid development schedules – especially in Agile environments – require developers to crank out code at breakneck speeds. It is very easy for developers to lose sight of the security best practices in these scenarios. In today's environments, high profile attacks are becoming a pervasive problem. Even the most highly regarded companies have suffered loss of customer data resulting in damage to their reputations as well as their bottom lines. It is essential that security be top of mind and built into the applications, rather than "bolted on" after-the-fact.

Quickly Identify and Fix the Latest Vulnerabilities in Your Code

Sentinel Source, WhiteHat's Static Applications Security Testing (SAST) offering, scans your entire source code, identifies vulnerabilities and provides detailed vulnerability descriptions and remediation advice, as well as precise ready-to-implement remediation solutions for certain vulnerabilities. Sentinel Source enables you to:

- Assess code at any point in the development cycle – even partial code.
- Run scheduled assessment daily or on demand.
- Preserve your intellectual property – source code can be scanned within your premises
- Stay up-to-date on the latest attacks with Rule Packs that identify and verify vulnerability defects.
- Scale security to meet the needs of your organization with automated, always-on cloud based platforms.
- Easily discover and assess the size (in lines of code or MB) of your apps with supported files types using WhiteHat's Count Lines of Code (WHLOC) tool



HOW SENTINEL SOURCE WORKS

The Sentinel Source engine is very accurate and fast at finding security defects. Our scanning technology is optimized for each source code language and we can scale at unprecedented levels.

Threat Research Center

The WhiteHat Security Threat Research Center (TRC) is a dedicated team of security engineers who discover and validate new and complex defects before they reach production. TRC engineers prioritize and validate every potential vulnerability – to provide you with actionable results and help you determine where best to allocate resources based on severity and threat value. Vulnerability details include:

- Exact code snippet, line number and file name
- Description of the vulnerability and remediation advice
- Access to the security engineers via the built-in "Ask a Question" feature

Technical Features

SUPPORTED VULNERABILITIES

Sentinel Source supports over 50 vulnerabilities, including:

- Application Misconfiguration
- Credential/Session Prediction
- Directory Indexing
- Insufficient Authorization/Authentication
- Automatic Reference Counting
- Cross Site Request Forgery
- Information Leakage
- Insufficient Transport Layer Protection
- Insufficient Binary Protection
- Cross Site Scripting
- Injection Attacks
- Interprocess Communication
- OS Commanding
- Insecure Cryptography
- SQL Injection
- Cryptographic Related Attacks

SUPPORTED LANGUAGES

Sentinel Source supports a variety of coding languages for web application, web services, desktop applications, and mobile applications, including:

SOURCE CODE

- Java
- C# (.NET)
- ASP.NET
- PHP
- JavaScript
- Node.js
- Objective-C (iOS)
- Android
- HTML5

BINARIES

- Java
- C# (.NET)

SENTINEL SOURCE DELIVERY

Each organization has different needs and Sentinel Source offers a variety of delivery models. Whatever your current infrastructure, our delivery methods adapt to you. Options include:

- On-Premise VM appliance
- Cloud VM

Comprehensive Integration with SDLC

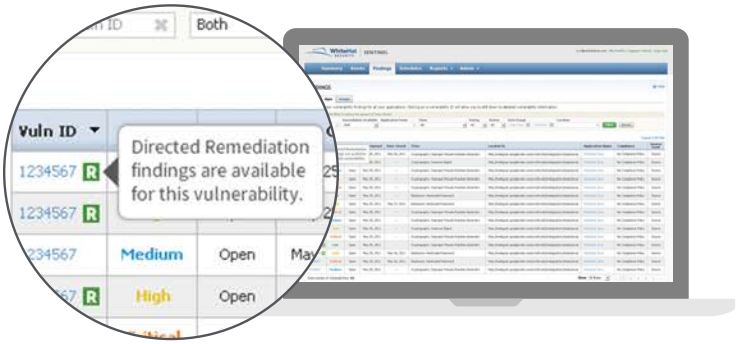
CATEGORY	INTEGRATIONS	BENEFITS
IDE Integrations	Eclipse, Xcode, Visual Studio, IntelliJ	Vulnerability details available right within the development environment
Bug Tracking Systems	Atlassian Jira®	Automatically open or close tickets for bugs and defects found or fixed by Sentinel Source
Supported Repositories	Git, SVN, Perforce, CVS, TFS, or files accessible via HTTP/S, SFTP	Scan source code from any supported repository or source code archive accessible by Sentinel Source appliance.
Miscellaneous	Jenkins (CI Server Plugin), Nuget, Maven, Gradle	Resolve code dependencies using popular Continuous Integration Servers and Dependency Management Systems
ALM/Bug Tracking Systems using WhiteHat Integration Server (WIS)	Atlassian Jira®, Borland StarTeam (Dev Services Required), HP ALM, HP Quality Center, IBM Rational Team Concert (Rational Quality Manager), IBM Rational Requirements Composer, Microsoft Team Foundation Server, ThoughtWorks Mingle, Rally, VersionOne, Bugzilla, Serena Business Manager, ServiceNow (Deployment Services may be required)	Integrate to best-of-breed ALM tools with WhiteHat Integration Server (WIS) which provides bi-directional integration between Sentinel artifacts and ALM tools

Sentinel Source Directed Remediation

Directed Remediation is a WhiteHat Sentinel Source feature that offers targeted and customized remediation fixes for a growing list of vulnerabilities*, significantly reducing the burden on the development team. This enables you to:

- Easily fix the vulnerabilities in the source code by utilizing precise code patches that are immediately ready to implement.
- Utilize WhiteHat's secure libraries to protect your applications.
- Establish security best practices for the development teams by emulating WhiteHat's security fixes in other development areas.

**We are continually expanding the types of vulnerabilities and languages supported by Directed Remediation*



Software Composition Analysis

This feature leverages Maven, Nuget and Gradle to display a list of third party libraries being used in the source code. This provides a per app breakdown of every library being used and identifies:

- Licenses for each library being used
- Out of date libraries that may benefit from an upgrade
- Vulnerabilities in those libraries and security risks associated with them

With Software Composition Analysis, you can accelerate the time-to-market for your applications, by safely and confidently utilizing open source code, without introducing unnecessary risk.

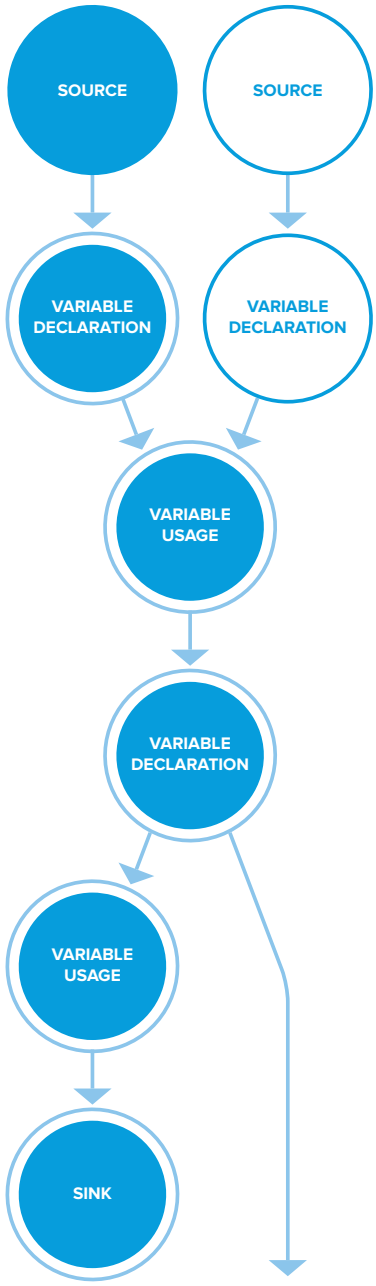
Data Analytics

With various reporting formats tailored to users at any level in the organization, you can gain deep visibility into your risk exposure with data analytics.

- Role-based dashboards and data intelligence enable you to measure threat, governance and compliance risks.
- Advanced analytic capabilities allow you to monitor trends and key statistics such as remediation rate, time to fix vulnerabilities and age of vulnerabilities
- Compliance (PCI) reports can be run at any time

SENTINEL SOURCE DATA FLOW DIAGRAMS

Visual representation of data flows and multiple traces simultaneously enable you to navigate code snippets related to vulnerability, identify common code snippets for multiple vectors of attack providing you insight into where more advanced security controls could be introduced.



Why Enterprises Select Sentinel Source?

It's suited for agile development

Sentinel Source allows you to assess code at any point in the development process, making it easy for your development teams to catch critical vulnerabilities earlier in the software development lifecycle. We integrate with Jenkins, IDEs and the best-of-breed application lifecycle management (ALM) tools. This provides the ability to work from within the tools of your choice, without impacting productivity. There is no need to compile code – Sentinel Source scans the source code from repositories, without requiring any extra work.

Your intellectual property stays onsite

Sentinel Source tests your source code within your own environment. No need to upload source code or binaries to a new location.

You get real, verified, actionable results with near zero false positives

WhiteHat's Threat Research Center (TRC) validates every potential vulnerability, groups them to avoid over reporting duplicates, and enables you to focus your remediation efforts on verified actual bugs and defects, saving you from wasting time and money.

You have direct contact with a team of Security Engineers at no additional cost

Via the "Ask a Question" feature in the Sentinel Portal and within IDEs and Jira®, you have direct access to the TRC Security engineers to ask questions about specific vulnerabilities.

You can reduce the time-to-fix for your security issues

WhiteHat's security experts provide remediation guidance to help you determine where to best allocate resources based on severity and threat value. Built in features such as "Ask a Question" and "Directed Remediation" accelerate the time-to-fix for your security issues.

WhiteHat SECURITY

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