Sentinel Source for Microservices

Application Security for Microservices

Implementing a microservices based architecture is the modern way of creating web and mobile applications. A microservices approach is perfectly suited to provide agility, scale services efficiently, and satisfy the reliability requirements of the critical applications that power your digital business. Microservices have sped up the process of building and releasing software, but in this race to get to market, the last thing you want is to overlook the security of these microservices.

Find and Fix Security Vulnerabilities in Your Microservices Code

Sentinel Source for Microservices, a service of the WhiteHat Application Security Platform, is the most accurate Static Applications Security Testing (SAST) offering that scans your source code, identifies vulnerabilities, and provides detailed vulnerability descriptions and remediation advice, as well as precise ready-to-implement Directed Remediation patches for certain vulnerabilities. All vulnerabilities are verified by the security engineers of our Threat Research Center to offer prioritized, actionable results with near zero false positives.

SENTINEL SOURCE FOR MICROSERVICES 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 application security to meet the needs of your organization with the WhiteHat Application Security Platform.

Software Composition Analysis

IDENTIFY OPEN SOURCE COMPONENTS IN YOUR CODE

Included SCA feature displays 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- Out of date libraries that may benefit from an upgrade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.

Securing your Microservices Software Development Life Cycle

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

AWS SUPPORT

Sentinel Source supports AWS or VMWare for VM Appliances

Comprehensive Integration with SDLC

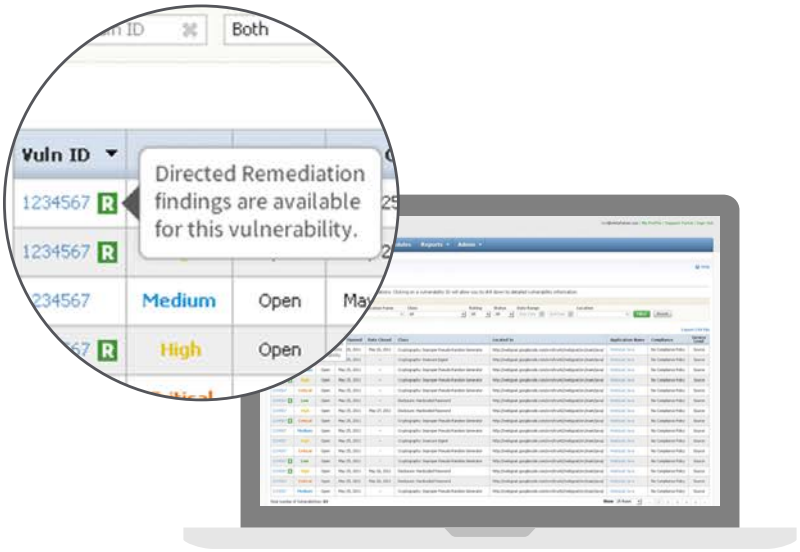
CATEGORY	INTEGRATIONS		BENEFITS
IDE Integrations	• Eclipse • Xcode	• Visual Studio • IntelliJ	Vulnerability details available right within the development environment
Bug Tracking Systems	• Atlassian Jira®		Automatically open or close tickets for bugs and defects found or fixed by Sentinel Source
Supported Repositories	• Git • SVN • Perforce	• CVS • TFS • 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*



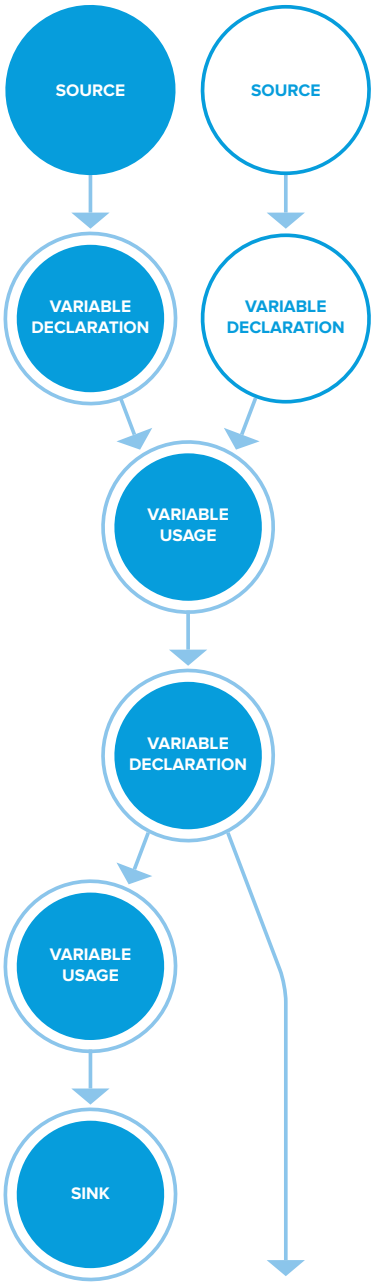
Data Analytics

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.



Sentinel Source for Microservices Benefits

Early visibility into Security Flaws

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.

Security Embedded into Your DevOps Processes

Comprehensive SDLC integrations with IDEs, CI/CD systems like Jenkins, Bug Tracking systems, and ALM tools allow you to work from within the tools of your choice – without impacting productivity.

Threat Research Center Expertise

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.

Direct contact with a Team of Security Engineers at no Additional Cost

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

Reduce 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. 1741 Technology Dr. #300, San Jose, CA 95110 • 1.408.343.8300 • www.whitehatsec.com