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, NTT Application Security’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 assessments 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 NTT Application Security’s Count Lines of Code 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.
NTT Application Security Experts

Our dedicated team of security engineers discover and validate new and complex code defects before they reach production. By prioritizing and validating every potential vulnerability you get actionable results that help to 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
» C# .NET Core
» PHP
» JavaScript
» Python

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

LANGUAGES:
• Java
• C# .NET
• JavaScript
• PHP
• C# .NET Core
• Python

CODE REPOS:

BUG TRACKERS / ALM TOOLS:

✓ Additional 25+ ALM tools via the NTT Application Security Integration Server
**Sentinel Source Directed Remediation**

Directed Remediation is a 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 NTT Application Security’s secure libraries to protect your applications.
- Establish security best practices for the development teams by emulating NTT Application 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.
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
NTT Application Security experts validate 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 NTT Application Security engineers to ask questions about specific vulnerabilities.

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