WhiteHat SECURITY

SPOTLIGHT: SENTINEL SOURCE

Threat Research Center

An extension of your Application Security Team

WhiteHat Security's Threat Research Center (TRC) is an elite team of the industry's top security experts, who are a critical and integral component of the WhiteHat Sentinel Product Family. All vulnerabilities reported by the Sentinel platform are verified by security experts in the TRC using cutting edge vulnerability tests and proprietary algorithms to ensure that you get actionable, confirmed results and near zero false positives.

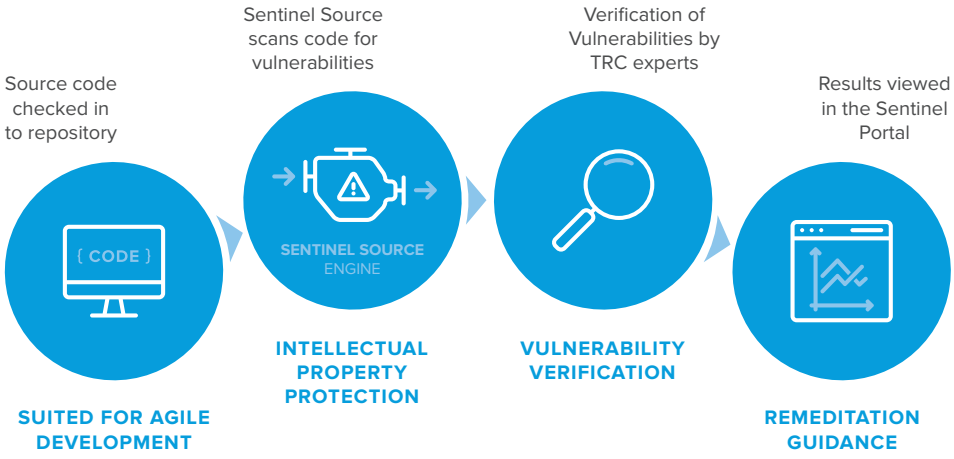
Sentinel Source

Sentinel Source, WhiteHat's static analysis offering, scans your entire source code for application vulnerabilities.

A VM appliance drives the Sentinel Source engine.

It retrieves application code from a repository and uses the scanning engine to assess the code for vulnerabilities.

The scanning engine compiles the source code to an abstract syntax tree to aid in finding data flow vulnerabilities.



TRC engineers work with the client to choose scan settings to ensure that:

- The appliance has access to the repository
- All of the correct code is being scanned, and no extra code
- The code is broken up into applications appropriately
- The code can be processed and assessed by the scanning engine

Delivering customized configuration, scanning and assessments

Rulepacks defined by the TRC decide the conditions under which vulnerabilities should be flagged by the scanning engine. Any code that is not included in the repository, for example a library that is being used, benefits from having rules written to describe the behavior of that code to the engine. TRC engineers are updating these rules on a weekly basis and the appliance calls home to WhiteHat servers to get these updates.

The rules written mostly fall into three categories:

- **Support Rules** provide the engine with the ability to parse and assess code for a given language, framework, or library.
- **Data Flow Rules** identify conditions where untrusted or "tainted" data may end up where it can cause damage.
- **Semantic Rules** test for specific vulnerabilities in a single file, usually configuration issues.

Unmatched vulnerability verification virtually eliminates false positives

TRC engineers confirm vulnerabilities found by the scanning engine. Only code snippets related to the vulnerability are sent back to the TRC for verification and the majority of the source code remains onsite. TRC engineers confirm the exploitability of the vulnerability via proprietary, state-of-the-art algorithms and methods before it is reported in the Sentinel interface. Descriptions and solutions for the issues are adjusted and remediation advice is offered where applicable.

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

About WhiteHat Security

Founded in 2001 and headquartered in Santa Clara, California, WhiteHat Security is the leader in application security, enabling businesses to protect critical data, ensure compliance, and manage risk. WhiteHat is different because we approach application security through the eyes of the attacker. Through a combination of technology, more than a decade of intelligence metrics, and the judgment of real people, WhiteHat Security provides complete web security at a scale and accuracy unmatched in the industry. WhiteHat Sentinel, the company's flagship product line, currently manages tens of thousands of websites – including sites in highly regulated industries, such as top e-commerce, financial services, and healthcare companies. For more information on WhiteHat Security, please visit www.whitehatsec.com.

WhiteHat SECURITY

WhiteHat Security, Inc. | 3970 Freedom Circle | Santa Clara, CA 95054 | 1.408.343.8300 | www.whitehatsec.com