

WhiteHat Sentinel – Selection Guidelines

WhiteHat Security is pleased to offer two versions of the WhiteHat Sentinel Service, the Standard Edition (SE) and the Premium Edition (PE). Below is an easy-to-use chart which highlights Sentinel SE and PE’s common and unique features and benefits.

WhiteHat Sentinel Standard Edition (SE) is designed for smaller, less complex, lower-risk attack target websites, where code changes are relatively infrequent. SE is an appropriate solution for companies with ten to hundreds of websites that have best practice or PCI 6.6 compliance requirements. Sentinel SE replaces scanners that are ineffective, generate an inordinate amount of false positives and aren’t scalable. WhiteHat Sentinel SE also offers an easy migration path to the Sentinel Premium Edition.

WhiteHat Sentinel Premium Edition (PE) is ideal for larger, more complex, mission critical, publicly-facing websites that are high-risk attack targets. These websites normally require frequent code updates, increasing the likelihood of introducing new vulnerabilities.

The key differentiator between Sentinel SE and Sentinel PE is the inclusion of custom testing by the WhiteHat Security Operations Team to manually identify business logic flaws. Uncovering these types of vulnerabilities requires manual review of a website by security experts who are capable of understanding things like account structures and the contextual logic in Web applications.

The Sentinel PE testing methodology uses the WASC (Web Application Security Consortium) 24 classes of attacks as a measuring stick against which all testing is performed. The WASC 24 has been adopted as a global standard and is used as a benchmark to ensure comprehensive Web application vulnerability assessments.

WhiteHat Sentinel Service Selection Guidelines		
Type of Service	Sentinel SE (Standard Edition)	Sentinel PE (Premium Edition)
Website Type(s)	<ul style="list-style-type: none"> • Less complex, smaller in size • Lower-valued assets • Lower-risk attack targets • Less frequent code changes • Less vital business logic 	<ul style="list-style-type: none"> • Complex, larger in size • Mission critical • High-risk attack targets • Frequent code changes • Contains critical business logic • Must meet rigorous compliance standards
Unique Features		
Business Logic Testing	No	Yes
Proof of Concept Vulnerability Examples	No	Yes
WASC 24	Tests for 13 (see back page)	Tests for 24 + 2* (see back page)
Common Features		
Subscription based	Unlimited number of assessments/year	
Accurate	<ul style="list-style-type: none"> • Virtually eliminates false positives • All vulnerabilities discovered are verified for accuracy 	
Scalable	Scales to meet needs of the largest enterprise-class environments	
Turnkey	Easy to set up and use	
PCI 6.6 Compliant	Yes	
Price	Annual subscription, tiered pricing	
API Access	Yes	
Accounts	Unlimited	
Support		
Support	Email	Email + Phone
Support hours	8:30-5:30 PM PT M-F	8:30-5:30 PM PT M-F

Sentinel SE Assesses for the 13 Classes of Technical Vulnerabilities

Technical Vulnerabilities

Command Execution

- Buffer Overflow
- Format String Attack
- LDAP Injection
- OS Commanding
- SQL Injection
- SSI Injection
- XPath Injection

Information Disclosure

- Directory Indexing
- Information Leakage
- Path Traversal
- Predictable Resource Location

Client-Side

- Content Spoofing
- Cross-site Scripting (XSS)

Business Logic

N/A

Sentinel PE Assesses for the 24 + 2* Classes of Vulnerabilities:

Technical Vulnerabilities

Command Execution

- Buffer Overflow
- Format String Attack
- LDAP Injection
- OS Commanding
- SQL Injection
- SSI Injection
- XPath Injection

Information Disclosure

- Directory Indexing
- Information Leakage
- Path Traversal
- Predictable Resource Location

Client-Side

- Content Spoofing
- Cross-site Scripting (XSS)
- HTTP Response Splitting*

Business Logic

Authentication

- Brute Force
- Insufficient Authentication
- Weak Password Recovery
- Validation
- Cross-Site Request Forgery*

Authorization

- Credential/Session Prediction
- Insufficient Authorization
- Insufficient Session Expiration
- Session Fixation

Logical Attacks

- Abuse of Functionality
- Denial of Service
- Insufficient Anti-automation
- Insufficient Process Validation

