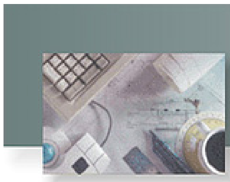

Product Component

DEFINITION

Name	WatchFire® AppScan®
Description	WatchFire AppScan is security vulnerability scanning and reporting tool for web development.
Rationale	AppScan provides a comprehensive list of tasks needed to fix the security issues found by the vulnerability scan. It has automated capabilities for penetration testing and advanced testing utilities that complement manual testing, offering penetration testers more power, automation, and efficiency.
Benefits	• Increases the development team's productivity by identifying vulnerabilities prior to deployment • Reviews applications that have been deployed to identify new threats • Allows tester to select specific tests

ASSOCIATED TECHNOLOGY AREA

List the name of the associated Technology Area	Security Testing

KEYWORDS

List all Keywords	HTML, XML NET, IPS, IDS, detection, security, compliance, anomalies, attacks, vulnerabilities, development, audit.

VENDOR INFORMATION

Vendor Name	WatchFire	*Website*	www.watchfire.com
Contact Information			

POTENTIAL COMPLIANCEORGANIZATIONS/GOVERNMENT BODIES

Standard Organizations

Name	PCI Data Security Standard, ISO 17799, ISO 27001	*Website*	
Contact Information			

Government Bodies

Name		*Website*	
Contact Information			

COMPONENT REVIEW **Platform Information**	
Hardware Platform Support	Minimum Requirements Hardware: Pentium 4 2.4 GHz Resolution 1024x768 Memory: 256 MB Network: 1 NIC 10/100 MBPS
Operating System Support	Operating System: Windows XP, Windows 2000, Windows 2003 Required Software: .Net Framework 1.1, JRE 1.5
Review Aspects	
List Desirable aspects	1. The AppScan product suite consists of: a. Development tools b. Auditing tools c. Security tools 2. Each suite component provides the following: a. Interaction with several major development environments, such as JBuilder, Websphere, MS Visual Studio.Net, and Eclipse b. Intelligent fix recommendations c. Unit testing of web applications can be performed within major development environments 3. In addition, AppScan for Auditors is: a. Used to conduct on-going web application security audits to validate security and compliance against regulatory and organizational initiatives in the live environment b. Equipped with expanded testing functions for auditors 4. Licensing deployment and usage options a. AppScan Enterprise Reporting Server: i. Uploads AppScan results for enterprise-wide reporting, management and controls who has access to information and generate summary reports with high-level metrics b. AppScan Enterprise Full Server: i. Central server for automated scanning and reporting across the enterprise ii. Allows auditors or administrators to monitor and manage vulnerabilities, see the security status of applications and schedule security scans based on organizational needs. 5. Utilities that are used in conjunction with the suite tools:

a. HTTP Proxy - An HTTP intercepting proxy that allows users to stop, edit, and submit requests and responses between the client and the server. It includes the ability to write automated scripts in JavaScript using the utility API. This enables users to manipulate requests and responses on the fly. HTTP Proxy also includes logging facilities for debugging of HTTP communications.

b. Connection Test - An HTTP pinging utility that helps website developers and auditors to test the connection between a client and a web server. Unlike the command PING, which uses the ICMP protocol (that is sometimes blocked by firewalls); Connection Test uses the HTTP protocol to communicate with the website.

c. HTTP Request Editor - HTTP Request Editor enables users to create specific HTTP requests and send them to a website. The editing will perform either on the raw request, or by viewing the request in a "parsed" mode. The response to the request can be viewed either raw, or in an embedded browser.

d. Expression Test - A tool for testing regular expression patterns on a given text.

e. Encode/Decode - A utility that transforms text strings into several encoding methods, such as URL Encoding, Base64, 3DES, MD5, SHA1, HTML entities, Overlong UTF-8 and more.

f. Application Coverage - Scans web applications looking for security vulnerabilities, and includes integrated Web Services scanning and JavaScript Execution and Parsing

6. AppScan generates regulatory compliance templates and reports including for 34 out-of-the box regulations. The most common are:

   - PCI Data Security Standard
   - ISO 17799
   - ISO 27001
   - COPPA
   - Data Protection Act
   - DCID -- Director of Central Intelligence Directive 6/3
   - EU Safe Harbor
   - FISMA
   - GLBA
   - HIPAA
   - NERC -- Security Guidelines for the Electricity Sector
   - OCC Web-Linking Guidelines
   - Privacy and Electronic Communications Regulations
   - Security Breach Information Act (SB 1386)
   - Section 207
   - Section 208
   - Section 508
   - Visa CISP

List Undesirable aspects	- Proprietary system - Professional training required

ASSOCIATED COMPLIANCE COMPONENTS

Product

List the Product-specific Compliance Component Names	Security Testing

Configuration Links

List the Configuration-specific Compliance Component Names	

COMPONENT CLASSIFICATION

Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*

COMPONENT SUB-CLASSIFICATION

Sub-Classification	Date	Additional Sub-Classification Information
Technology Watch		
Variance		
Conditional Use		

RATIONALE FOR COMPONENT CLASSIFICATION

Document the Rationale for Component Classification	

MIGRATION STRATEGY

Document the Migration Strategy	

IMPACT POSITION STATEMENT

Document the Position Statement on Impact	

AGENCIES

List the Agencies Currently Utilizing this Product	DOLIR, OA, DSS, DMH, DOI, DHSS, OSCA, DED, DPS

CURRENT STATUS

Provide the Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*

AUDIT TRAIL

Creation Date	11/03/2006	*Date Accepted / Rejected*	11/28/2006
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			