

AppDetectivePro™ 7.2

What's New



The leading database scanning and vulnerability assessment solution for global auditors and IT advisors offers new work plan management enhancements to help streamline database compliance audits. In addition, version 7.2 includes new checks and support for Massachusetts 201 data privacy requirements.

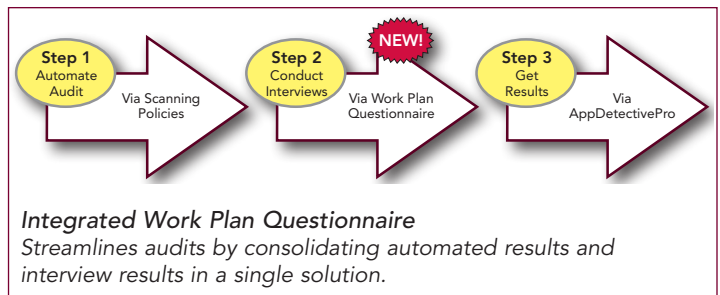
NEW WORK PLAN MANAGEMENT ENHANCEMENTS

Extending Beyond Automated Results to Streamline Database Auditing

The new work plan capabilities bring together both the automated and manual processes of a database audit within a single framework.

Historically, organizations have used AppDetectivePro's compliance policies to automate the scanning component of a database audit (password checks, privileged escalation investigation, misconfigurations, etc.). The recording of interview results and notes around findings, data processes and compliance exceptions was a separate manual effort.

This new functionality simplifies audits and reduces the time to compliance by automating a complete database audit work plan process. External and internal IT audit teams can use AppDetectivePro to facilitate work plan automation by leveraging its Work Plan Manager to create a consistent framework for managing all control objectives. Audit scan results are now instantly transformed into audit finding evidence to support your answers.



SUPPORT FOR DISA STIG AND OTHER REQUIREMENTS

The built-in audit work plan for DISA STIG streamlines database audits following the DISA STIG checklists. This feature provides organizations with the ability to eliminate the manual process of running SRRs (Security Readiness Review) scripts and to solely utilize AppDetectivePro for DIACAP compliance.

The work plan manager also supports the use broader-based general IT audit control requirements, such as CoBIT, COSO, and ISO 27002.

Customize Questionnaire

Document interview results

Match against scan results

AppDetectivePro - Interview

Interview status: In Progress | IP address: 192.168.2.60 | Start date: 9/10/2010 12:30:19 PM | Last update date: 9/10/2010 12:31:29 PM

Application: Microsoft SQL Server 2000 | Port: 2000

Work plan: SRR DB Checklist V8R1.6 for SQL Server 2000 | Audit policy: DISA-STIG Database Security - Audit (Built-in)

Questionnaire: Microsoft SQL Server 2000 DB Checklist V8R1.6 - KB v4.0 | Questionnaire type: DISA-STIG

Question

Name: DDL permissions should be granted only to authorized accounts.

Description: Database Administrator

References:

Type	Value
STIG ID	DM1760
CAT	DDL permissions should be granted only to authorized accounts.
IA Control	ECLP-1 Least Privilege
VX	V0002453

Response

Answer: Not a Finding Open Finding Not Applicable Not Reviewed

The DDL permissions discovered are valid for these authorized accounts.

Checks results

Audit: 9/8/2010 11:16:53 PM

Check Name, Status and Vulnerability Details

Statement permission granted

Check Status: Executed (Violation Found)

Vulnerability details:

- (Granted By=dbol)(Permission=CREATE PROCEDURE)(Database=publ)(Granted To=public)(State=GRANT)(Object Name=)
- (Granted By=dbol)(Permission=CREATE TABLE)(Database=publ)(Granted To=guest)(State=GRANT)(Object Name=)

Questions: 17 | Answered (default response is modified): 1 | Unanswered (has default response): 16

Buttons: Previous, Next, Finish Interview, Clear Response, Continue Later

AppDetectivePro 7

What's New

New Feature Highlights:

- **Work Plan Editor** – Allows users to pair business risk context with database scans. The questionnaire editor allows users to map control objectives to specific checks within their scan policies.
- **Audit Findings Report** – Delivers a comprehensive database audit report, providing consolidated results for a complete audit that includes manual interview answers and scan results.
- **SHATTER Knowledgebase Update** – Built upon the most comprehensive knowledgebase in the industry, AppDetectivePro provides built-in knowledgebase updates of vulnerability and configuration checks from TeamSHATTER, the industry's preeminent database security research team.

New Compliance Audit Policy for Massachusetts 201 CMR 17

Effective March 1, 2010, the new Massachusetts 201 CMR 17 data privacy regulation applies to any organization that does business in Massachusetts or handles information about Massachusetts residents. Non-compliance can result in possible penalties of up to \$50,000 for each instance depending on the infraction.

AppDetectivePro 7 includes new policies that enable enterprises to scan for all the security configuration standards set forth by the new law.

Get all the latest news and best practices on Mass 201 CMR 17 at: <http://www.appsecinc.com/solutions/mass201/index.shtml>

ADDITIONAL VULNERABILITY KNOWLEDGEBASE CHECKS

AppDetectivePro 7 adds over thirty new and updated checks, including coverage for the Oracle July 2010 CPU and the Oracle Litchfield Zero Day vulnerability (DBMS Java Packages) as well as for SQL Server and Sybase.

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

Application Security, Inc. (AppSec) is the leading provider of cross platform database security, risk and compliance solutions for the enterprise. Application Security, Inc.'s products – DbProtect and AppDetectivePro – deliver the industry's most comprehensive database security solution and are used in the most demanding environments around the world. With over 2,500 customers, AppSec was named to Inc. Magazine's 2007 (Inc. 500) and 2009 list of America's Fastest Growing Companies, and was also named to the 2009 Deloitte Technology Fast 50. For more information, please visit www.appsecinc.com or follow AppSec on Twitter at www.twitter.com/appsecinc.

**APPLICATION
SECURITY, INC.®**

www.appsecinc.com

ABOUT TEAMSHATTER

TeamSHATTER is AppSec's world-renowned research team, specializing in application vulnerability assessment and mitigation. The team conducts ongoing research into threats and vulnerabilities, identifying and reporting on security alerts. This intense focus and effort has resulted in the industry's premier knowledgebase of vulnerabilities, patches, and remediation best practices. AppSec provides frequent product updates for the purpose of ensuring that DbProtect customers are able to proactively secure their systems against the latest database vulnerabilities and threats using ASAP Updates. All of the security alerts and checks developed by TeamSHATTER are integrated into our security solutions. Follow TeamSHATTER on Twitter at www.twitter.com/teamshatter.